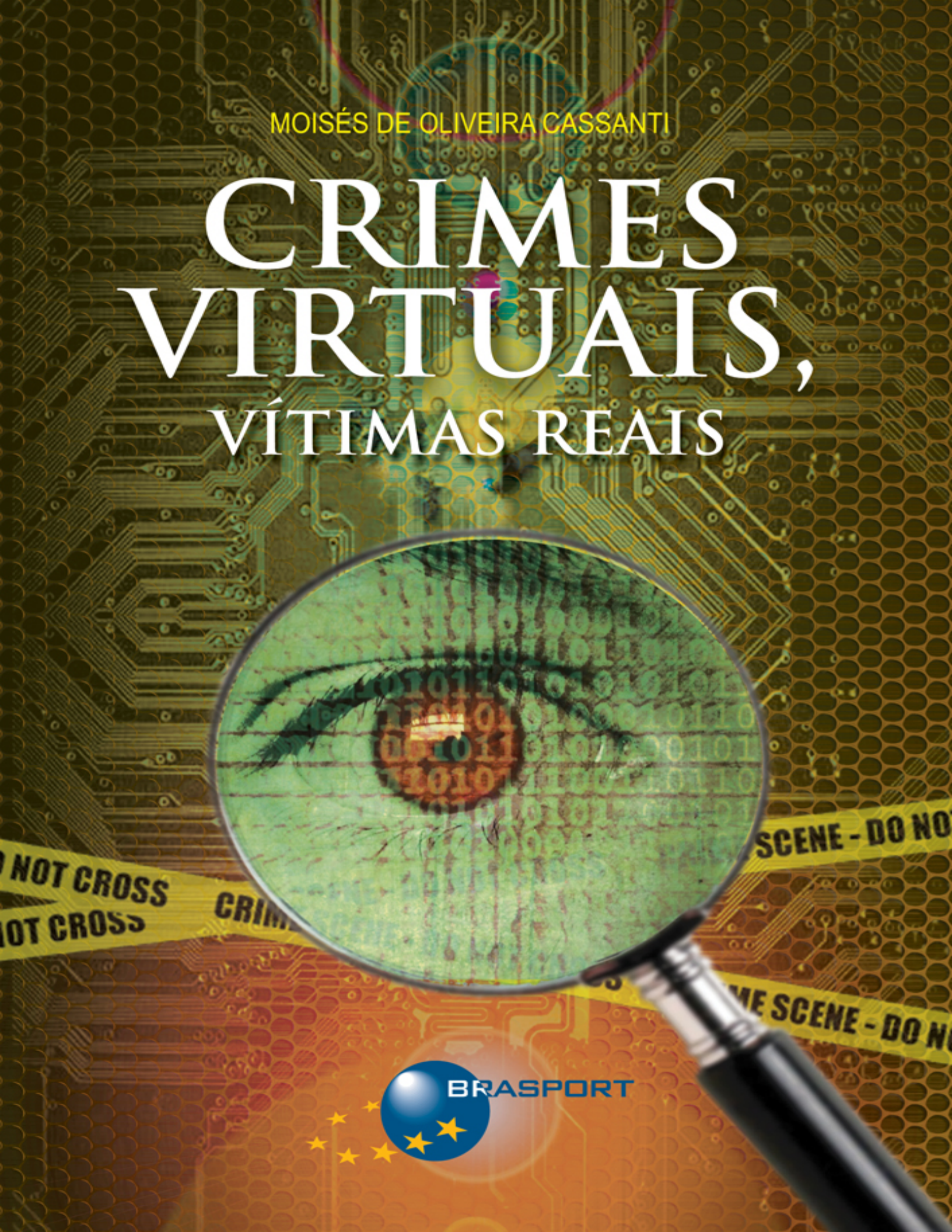
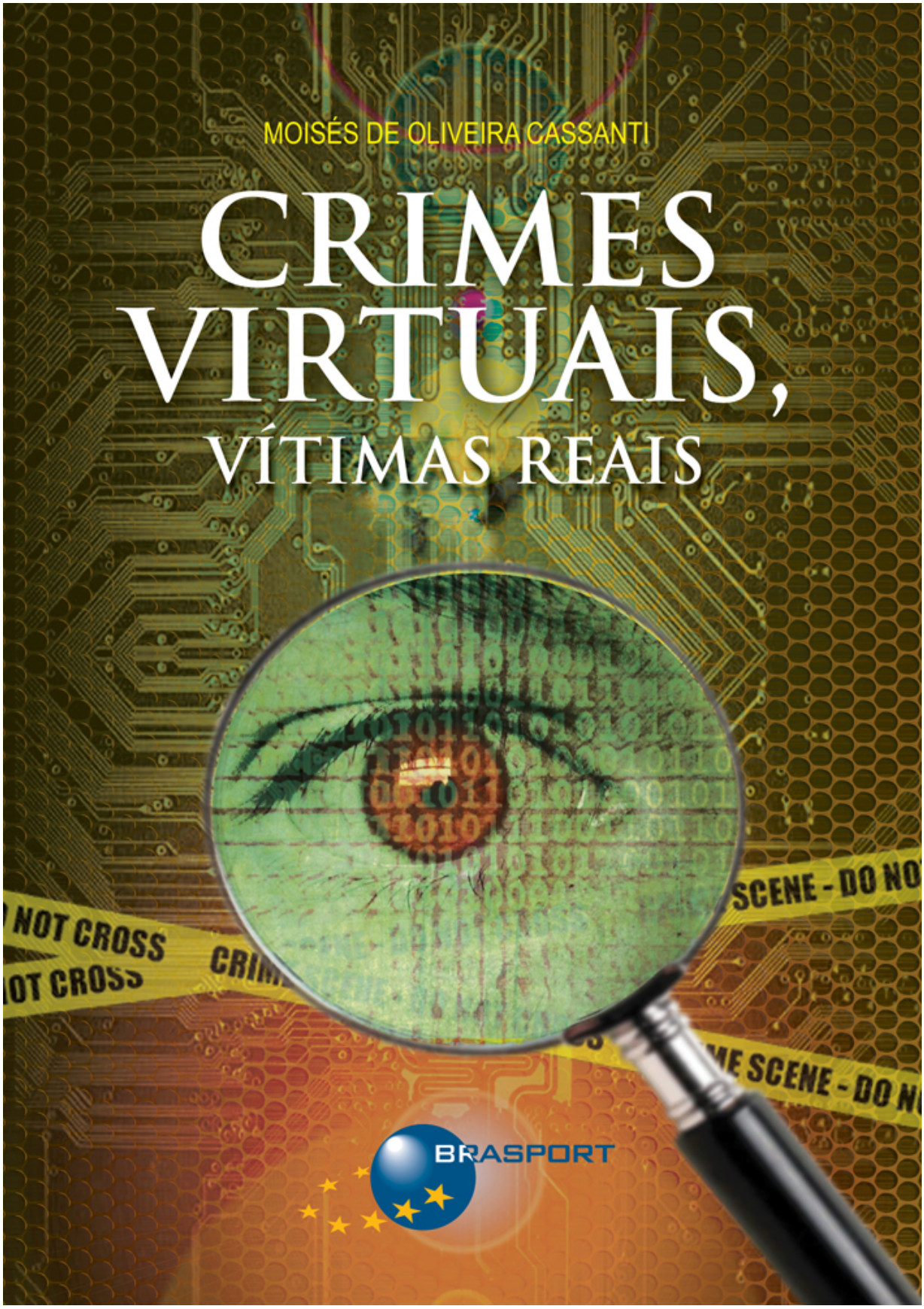
MOISÉS DE OLIVEIRA CASSANTI

CRIMES VIRTUAIS, VÍTIMAS REAIS



BRASPORT


MOISÉS DE OLIVEIRA CASSANTI
CRIMES VIRTUAIS,
VÍTIMAS REAIS
NOT CROSS
SCENE - DO NO
BRASPORT

CRIMES VIRTUAIS, VÍTIMAS REAIS

MOISÉS DE OLIVEIRA CASSANTI

CRIMES VIRTUAIS,
VÍTIMAS REAIS

BRASPORT

Copyright© 2014 por Brasport Livros e Multimídia Ltda.

Todos os direitos reservados. Nenhuma parte deste livro poderá ser reproduzida, sob qualquer meio, especialmente em fotocópia (xerox), sem a permissão, por escrito, da Editora.

Editor: Sergio Martins de Oliveira Diretora: Rosa Maria Oliveira de Queiroz Gerente de Produção Editorial: Marina dos Anjos Martins de Oliveira Revisão de Texto: Maria Helena A. M. Oliveira Editoração Eletrônica: Michelle Paula Capa: Paulo Vermelho Produção de ebook: S2 Books Técnica e muita atenção foram empregadas na produção deste livro. Porém, erros de digitação e/ou impressão podem ocorrer. Qualquer dúvida, inclusive de conceito, solicitamos enviar mensagem para editorial@brasport.com.br, para que nossa equipe, juntamente com o autor, possa esclarecer. A Brasport e o(s) autor(es) não assumem qualquer responsabilidade por eventuais danos ou perdas a pessoas ou bens, originados do uso deste livro.

BRASPORT Livros e Multimídia Ltda.
Rua Pardal Mallet, 23 – Tijuca 20270-280 Rio de Janeiro-RJ
Tels. Fax: (21) 2568.1415/2568.1507
e-mails: marketing@brasport.com.brvendas@brasport.com.br
editorial@brasport.com.br

site: www.brasport.com.br

Filial SP
Av. Paulista, 807 – conj. 915
01311-100 São Paulo-SP
Tel. Fax (11): 3287.1752
e-mail: filialsp@brasport.com.br

Dedicatória

Dedico este livro à minha companheira que divide comigo os momentos bons e principalmente os ruins. Já me acostumei com a sua voz dizendo que vai dar tudo certo e agradeço por nunca me ter deixado desistir.

Aos meus pais, nos quais me espelho para criar meus filhos.

Aos meus filhos que me ensinaram a importância de se viver. Sem vocês nada teria sentido.

Aos meus irmãos e amigos.

Em especial ao "Mané": sua inocência me inspira, sua força me incentiva e sua lealdade me protege.

Muito obrigado.

Sabe o que eu mais quero agora, meu amor?
Morar no interior do meu interior
Prá entender por que se agridem
Se empurram pro abismo
Se debatem, se combatem sem saber
Vander Lee

Agradecimentos

A Deus, que, tenho certeza absoluta, sempre ouviu minhas orações.

Ao apoio da minha família em todos os meus projetos.

À Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP, pelo carinhoso acolhimento e em especial ao seu presidente Dr. Coriolano Almeida Camargo, que vem conduzindo de forma brilhante esta comissão.

Prefácio

A informação é um dos bens mais preciosos da humanidade; aquele que a detém também detém o poder. Dessa forma, os homens sempre irão à busca das informações, infelizmente perdendo, em muitos casos, o escrúpulo e a ética para consegui-las.

Ao longo da história, podemos observar que, em todos os tempos, um grande desafio foi unir os povos, independentemente da distância, religião, cultura, etnia, entre outros aspectos. A internet conseguiu! Ela criou a possibilidade da união. Entretanto, o que temos visto é que, ao mesmo tempo em que ela permitiu que as pessoas pudessem se comunicar sem nenhuma barreira, deixou-as vulneráveis a diversos tipos de ataques.

Todos estão vulneráveis, por meio da engenharia social (práticas utilizadas para obter informações sigilosas ou importantes de empresas e sistemas, enganando e explorando a confiança das pessoas) ou por fraudes eletrônicas, sequestros de dados e outros crimes no meio eletrônico que passaram a fazer parte do cotidiano dos usuários domésticos e até das grandes empresas.

Quanto vale o conhecimento? Quanto vale o capital intelectual? Como proteger as informações de uma pessoa ou de uma empresa?

Várias empresas, preocupadas com o vazamento de informações, têm criado regras nos contratos de trabalhos

de seus funcionários que permitem o acesso à caixa de e-mail e o rastreamento de outros dispositivos. Segundo declarações daqueles que fazem consultorias e implementam softwares para rastrear o uso das informações pertinente às empresas, esse mercado no ano de 2013 cresceu três vezes em relação ao ano anterior.

Recentemente, no mês de junho de 2013, o mundo cobrou do presidente dos Estados Unidos da América, Sr. Barack Obama, uma postura mais ética após ele ter declarado que os grandes provedores liberam as informações dos seus usuários para o governo americano investigar. A chanceler da Alemanha, Sra. Angela Merkel, declarou nas mídias que liderará um movimento na Comunidade Europeia para cobrar dos Estados Unidos um esclarecimento do acontecido. De quem são as informações? A que tipo de informações o governo americano tem acesso? Qual a finalidade destas informações?

Quem é você, leitor, no meio desses processos? Uma possível vítima? Todos nós estamos, mais ou menos, vulneráveis! "Crimes Virtuais, Vítimas Reais" trata esse assunto de uma maneira simples e clara, facilitando ao leitor o uso de uma internet mais segura. Boa leitura e aplicação dos novos conhecimentos.

Prof. Dr. Valdéres Fernandes Pinheiro

Diretor Acadêmico e Coordenador do curso de graduação em Sistemas de Informação da Faculdade Impacta de Tecnologia, Diretor e Coordenador do Intercambio Brazil/USA International Cyber Security Law Program FIT/CCC&TI, Sócio-Diretor da GBR Group Brasil, Diretor Executivo da FP Solutions, Diretor Financeiro da Anarnet, Membro Consultor da Comissão de Crimes de Alta Tecnologia da OAB-SP, Membro Avaliador do Congresso Internacional PMI-SP, com participações e publicações em diversos congressos nacionais e internacionais. É autor de

capítulo no livro “Competitividade e Negócios Eletrônicos - estudos de casos”.

Sobre o Livro

A internet revolucionou o comportamento humano, mudando fortemente sua rotina, modificando padrões de conduta e de relacionamentos estabelecidos há milhares de anos. As pessoas estão cada vez mais conectadas e essa nova realidade social que nos cerca, por um lado, trouxe, sem dúvidas, muitas facilidades e progressos, E por outro, nos deixou mais vulneráveis a riscos inerentes da tecnologia da informação, criando uma nova modalidade de crimes, os chamados crimes virtuais.

Pode ser que você imagine que não corre riscos, pois utiliza o computador[1] apenas para fins domésticos como: fazer trabalhos escolares, acessar redes sociais, ler e-mail e, de vez em quando, se comunicar com algum familiar distante. Mas saiba que os alvos dos atacantes geralmente são os computadores domésticos, pois eles sabem que a maioria das famílias guarda seus recursos digitais e arquivos pessoais como fotos, currículos, informações financeiras (como imposto de renda) e outros documentos importantes em seus computadores e nem sempre mantêm proteção adequada. Isso faz de você um alvo fácil e lucrativo. Além de acessarem suas informações pessoais como: ver seus arquivos, ler seus emails, ver todas as suas senhas ou apagar seus arquivos, os atacantes podem utilizar o seu computador para promover ataques a outros computadores transferindo assim a responsabilidade de sua conduta

criminosa para você, sem que você saiba ao menos que existe alguém infiltrado em seu equipamento.

Mesmo que você conheça e utilize métodos eficazes de proteção para o seu computador e se sinta seguro contra invasões, não se esqueça de que nem assim você está livre de ser vítima de crimes contra a honra como o de calúnia, cometido através das redes sociais, ou de ameaças por e-mails, golpes em sites de compras, furto de identidade, perfis falsos, uso indevido da sua imagem, *cyberbulling* e tantos outros.

Mas o que fazer diante de uma dessas situações? Existem leis que o protegem? A quem procurar?

Este livro aborda todos esses temas, começando pelos meios e métodos por que um atacante invade o seu computador, passando a discutir cada um dos crimes virtuais e, por fim, como se proteger e agir caso tenha sido vítima.

Boa Leitura!

Moisés de Oliveira Cassanti

Sumário

Capítulo 1. Entendendo Melhor a Internet
- Vocabulário tecnológico
- Hackers X crackers
- Cibercrime
- Dispositivos móveis

Capítulo 2. Meios Utilizados por Atacantes para Ter Acesso ao Computador do Usuário
- E-mail
- Mensageiro instantâneo
- Redes sociais
- Sistemas de compartilhamento de arquivos (P2P)
- Sites fakes (páginas falsas)
- Arquivos PDF

Capítulo 3. Principais Ameaças
- Malware
- Vírus de computador
  - Tipos de vírus
- Cavalos de troia ou trojan
- Ransomware
- Rootkit
- Worms
- Engenharia social
  - Phishing
- Spywares
- Adwares

Capítulo 4. O Que Um Atacante Faz Quando Invade Um Computador?
- Fraude eletrônica
- Sequestros de dados
- Ataques DDoS
- Ataques por botnet
- Ataques por spyware

Capítulo 5. Crimes Virtuais
- Principais delitos
- Furto de identidade
- Crimes virtuais nas redes sociais
  - Pornografia infantil (pedofilia)
  - Apologia a crime ou a criminoso
  - Sequestradores escolhem vítimas pela internet
  - Cyberbullying
  - Crimes contra a honra
  - Perfis falsos
  - Xenofobia e bairrismo
  - Casos de polícia

Capítulo 6. Como se Proteger de Ataques e Crimes Virtuais
- Mantenha o seu computador protegido
  - Sistemas operacionais e demais programas
  - Antivírus e anti-spyware
  - Firewall
- Navegue com segurança
- Crie senhas difíceis e mude-as periodicamente
- Cuidado ao fazer compras pela internet
  - Proteja-se dos golpes
- Realize operações bancárias com segurança
- Cuidado com downloads
- Cuidado com e-mails
- Cuidado com salas de bate-papo (chat)
- Cuidado ao fazer cadastros

- Tenha bom senso

Capítulo 7. Como Agir em Caso de Crimes Virtuais
- Colete e preserve as evidências
- Atribua validade jurídica às provas obtidas
  - O que é uma ata notarial?
  - Para que serve?
  - Como utilizar nos casos de internet?
  - Preciso de advogado?
- Faça um boletim de ocorrência
  - Como registrar ocorrência dos crimes contra a honra e ameaça
  - Como registrar ocorrência de ameaças por e-mails
- Como fazer denúncia de crimes contra os direitos humanos na internet?
  - Através da SaferNet
  - Através do Ministério Público Federal (MPF)
- Como solicitar a remoção do conteúdo ilegal e/ou ofensivo diretamente ao provedor de serviço
  - Carta modelo
  - Decisão
- Como denunciar estelionato na internet
- Como denunciar extorsão pela internet
  - Casos concretos
- Fraudes com cartões de crédito
  - Como proceder nos casos de fraudes com cartões
- Como denunciar lojas virtuais que não entregam os produtos
  - Como posso ter certeza de que o site é confiável ou de que está registrado
- Como denunciar perfis roubados ou clonados
  - No Facebook
  - No Twitter
- Como denunciar vídeos impróprios no YouTube
- Outros canais importantes para denúncias

Como investigar e apurar judicialmente a autoria de crimes digitais
Capítulo 8. Endereços Úteis
Endereços dos principais provedores de serviços
Provedores de acesso
Como rastrear um IP utilizando a geolocalização
O que o endereço IP revela sobre você
Capítulo 9. Novas Leis Reforçam a Luta Contra Crimes Virtuais
Leis de Crimes Informáticos
O Marco Civil da Internet
Quais são os direitos e garantias estabelecidos pelo Marco Civil?
Decreto Federal 7.962/13
Capítulo 10. Estudos de Casos
Golpes
Empréstimo fácil
Ofertas de emprego
Troca de mercadorias
Phishing
Perfil falso
Furto de identidade
Crimes contra a honra
Retirada de conteúdo
“O par perfeito”
Compras pela internet
Ameaças
Outras dúvidas

Capítulo 1. Entendendo Melhor a Internet

A internet é uma grande praça pública, o maior espaço coletivo do planeta. Estima-se que no final de 2013 cerca de 2,7 bilhões de pessoas em todo o mundo estarão conectadas.[2] No Brasil a internet está atingindo um número crescente de usuários; somos 105 milhões[3] de internautas que estão cada vez mais conectados e passando mais tempo on-line.

A internet é um conjunto de redes de comunicações em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de comunicação TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que, como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores.

Vocabulário tecnológico

A TI (Tecnologia da Informação) possui um linguajar próprio, sendo seu vocabulário geralmente composto por palavras de idioma estrangeiro com as quais nem todas as pessoas que utilizam o computador se familiarizam. Entender este linguajar ajuda o usuário na melhor compreensão do que acontece ao seu redor.

Para entendermos como é feita a invasão de um computador, primeiro vamos definir a nomenclatura que vamos adotar. Evitando termos muito técnicos, trataremos o responsável pela realização de um ataque por "**atacante**" e a vítima, ou quem utiliza o computador, de "**usuário**".

Hackers X crackers

"Brasil é campeão em atividade hacker na América Latina"[4]

"Site da Sepror é atacado por crackers em Manaus"[5]

Esses são exemplos de alguns títulos de notícias sobre cibercrimes que circulam na internet. Sempre que entram na pauta jornalística casos envolvendo **cibercriminosos** surge a dúvida sobre como chamá-los: **hackers** ou **crackers**? Mas afinal qual é a diferença?

Ambos são *experts* em computadores, dedicam boa parte do tempo para estudar sistemas e programações e contam com habilidades avançadas. A principal diferença está na forma como cada um utiliza este conhecimento.

Apesar do termo ***hacker*** sempre aparecer associado a roubo de dados e invasão de sistemas, no entendimento de especialistas em computação, os verdadeiros criminosos são designados como ***crackers***. A palavra deriva do verbo em inglês "to crack", que significa quebrar. Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos.

O termo ***hacker***, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é aplicada pela própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou

adaptar as antigas.

Existem subdivisões que definem outras habilidades dos *crackers*, sendo as mais conhecidas as seguintes: ➢

Carder: especialista em roubar informações bancárias como números de cartões de crédito, cartões de conta corrente ou poupança, ou contas em sites de movimentações bancárias, para compras on-line, saques em caixas eletrônicos, transferência para contas de laranjas entre outros atos ilícitos.

□

Defacer: especialista em pichar sites normalmente deixando mensagens de protesto contra o próprio site.

□

Spammer: dissemina e-mails com correntes e vírus que podem danificar e roubar informações dos usuários, como senhas bancárias.

□

Phisher: especializado em aplicar golpes diversos. Eles são profundos conhecedores das falhas de um sistema.

□

Phreaker: especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos.

Cibercrime

Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como

cibercrime. Outros termos que se referem a essa atividade são: **crime informático**, **crimes eletrônicos**, **crime virtual** ou **crime digital**.

Dispositivos móveis

A partir do segundo semestre do ano de 2011 acompanhamos um aumento muito expressivo dos chamados dispositivos móveis como celulares, *smartphones* e *tablets*. Com isso, os ataques virtuais que antes eram restritos aos computadores estão migrando para as plataformas móveis.

Assim como os computadores, os dispositivos móveis podem ser usados para a propagação de códigos maliciosos, furto de dados, envio de spam, além de poder fazer parte de *botnets* e serem usados para disparar ataques na Internet.

O acesso à internet, e-mails, aplicativos e principalmente às redes sociais a partir de qualquer lugar são algumas das facilidades oferecidas por esses dispositivos.

Algumas características próprias que os dispositivos móveis possuem os tornam mais atraentes para atacantes e pessoas mal-
intencionadas como:

- Grande quantidade de informações pessoais armazenadas.
- Maior possibilidade de perda e furto.
- Grande quantidade de aplicações desenvolvidas por

terceiros.

-

Rapidez de substituição dos modelos.

De forma geral, os cuidados que você deve tomar para proteger seus dispositivos móveis são os mesmos a serem tomados com seu computador pessoal, como mantê-los sempre atualizados e utilizar mecanismos de segurança. Por isso é muito importante que você siga as dicas apresentadas no **Capítulo 6 - Como se proteger de ataques e crimes virtuais**.

Capítulo 2. Meios Utilizados por Atacantes para Ter Acesso ao Computador do Usuário

Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais se quem pretender vencê-lo primeiramente não puder entendê-lo.

Muitos não sabem, mas para o usuário ser atacado, ele precisa permitir que isso aconteça de forma direta ou indireta. Na forma indireta, o atacante, para "entrar" na máquina, explora as vulnerabilidades, tanto por falhas nos softwares ou por configurações incorretas do computador, ou de segurança proporcionadas pelo *firewall*. Da forma direta, o atacante se utiliza de um dos meios listados a seguir para implantar um **programa malicioso** (*malware*) no computador do usuário e assim prosseguir com o ataque.

E-mail

Atualmente, o e-mail tornou-se um meio de comunicação indispensável, mas, por outro lado, ainda é um dos meios mais eficazes para que um atacante invada um computador. Spam, vírus, golpes de roubo de identidade e e-mails fraudulentos são apenas algumas das ameaças. O usuário recebe um e-mail fazendo despertar sua curiosidade e acaba clicando em um link, permitindo assim que o atacante alcance o seu objetivo.

Mensageiro instantâneo

São programas para enviar e receber mensagens simultaneamente. A comunicação é feita em tempo real por meio de textos, voz ou vídeo. As conversas podem ser feitas entre duas ou mais pessoas em ambinte privado.

Hoje muitos são os programas que executam esta tarefa, a exemplo do Skype, ICQ, Yahoo Messenger, Google Talk, dentre outros. Apesar de alguns detalhes variarem de um programa para outro, os passos básicos são os mesmos para qualquer utilitário de mensagens instantâneas disponíveis.

Em programas de mensagens instantâneas o mais comum é o atacante mandar um link através de uma pessoa conhecida. Se o usuário clica, a ameaça se instala no computador. Outro problema é que estes programas abrem portas que permitem ao atacante capturar o IP da máquina.

Redes sociais

A Wikipédia define uma rede social como "uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns".

Alguns dos níveis da rede social mais conhecido são, sem dúvidas, os sites de relacionamentos (Facebook, Orkut, Myspace, Twitter e muitos outros). Estes sites facilitam o encontro de pessoas que por algum motivo estavam afastadas e permitem fazer novas amizades por comunidades semelhantes. Mas o preço para quem se insere nessas redes é a sua privacidade, que estará aberta a todos os usuários da internet, ou seja, todos passam a obter informações sobre rotina, identidades e estilos de vidas dos participantes daquela comunidade.

Não existem ferramentas de segurança voltadas para proteger as pessoas de si mesmas; sabendo disso, as redes

sociais estão sempre na mira dos atacantes, pois é muito fácil enganar usuários desavisados.

Uma recente pesquisa realizada pela Kaspersky Lab apontou que 21% dos links maliciosos presentes na internet estão hospedados em **redes sociais**, contra 14% que estão disponibilizados em sites de conteúdo adulto. Segundo o estudo, sites como **Facebook**, **Twitter** e **Google+** tornaram-se uma arma em potencial para os atacantes, pois, quanto mais popular, maior a possibilidade da criação de links maliciosos para serem propagados pela rede.

O vencedor de maior disseminação de malware é o **YouTube**, que abriga atualmente 31% dos links maliciosos. Os serviços de busca, como o Google, ficam em segundo lugar, com 22%, onde é realizada manipulação de resultados para o redirecionamento a links maliciosos.

Sistemas de compartilhamento de arquivos (P2P)

Esses programas servem para compartilhar e localizar arquivos. Com eles você pode encontrar e fazer download de músicas MP3, vídeos AVI, MPEG e muitos outros formatos de arquivos, até mesmo programas. Entre os mais utilizados estão: o Ares, LimeWire, eMule *etc.* e todos disponibilizam milhares de arquivos, mas nem todos são confiáveis.

Sites fakes (páginas falsas)

Usam técnicas de redirecionamento em que eventualmente o usuário pode ser direcionado para um site falso, idêntico ao original, que lhe solicitará senha. Caso o usuário não desconfie, além do site lhe roubar alguma senha, poderá instalar algum tipo de programa malicioso.

Arquivos PDF

O formato PDF hoje em dia é um dos maiores vetores de

ataques para instalações de códigos maliciosos, isso porque ele permite a execução de Javascript e flash object embarcados no arquivo. Podem carregar *exploits* para o Adobe Reader e, quando a pessoa abre o arquivo, se instala o trojan. A dica de segurança para o PDF é utilizar leitores alternativos ao Adobe Reader, como o Foxit, por exemplo.

Capítulo 3. Principais Ameaças

Dizemos que um computador é vulnerável quando este apresenta varias deficiências de segurança. Antivírus desatualizado, sistemas operacionais piratas (que não podem receber atualizações), firewall desativado ou configurações incorretas da rede e ainda falhas nos softwares. Os atacantes exploram essas vulnerabilidades, resultando em possíveis ataques e danos para o computador ou seus dados pessoais.

Malware

O termo malware é a contração de "malicious software" (programa malicioso) e identifica qualquer programa desenvolvido com o propósito de causar dano a um computador, sistema ou redes de computadores. É um dos dois tipos de intrusos que podem invadir o seu computador (o outro é o próprio atacante). Os mais comuns são os vírus, *worms* e cavalos de troia. Geralmente se utilizam de ferramentas de comunicação conhecidas para se espalharem – como, por exemplo, *worms* enviados por e-mail e mensagens instantâneas, cavalos de troia provenientes de websites e arquivos infectados com vírus obtidos por download de conexões ponto-a-ponto. O malware também tenta explorar as vulnerabilidades existentes nos sistemas, tornando sua entrada discreta e fácil.

Vírus de computador

Os vírus são pequenos programas capazes de produzir cópias de si mesmo, porém não podem se autoexecutarem; para começar a agir, precisam que alguém ou algo os execute.

O termo vírus foi usado pela primeira vez pelo pesquisador Frederick Cohen, que chamou os programas de códigos nocivos de vírus. Foi Cohen que programou o primeiro vírus. “Fiz algo muito controlado e dentro de um laboratório. Não faria isso novamente hoje”, diz Fred Cohen, atual professor de Postura de Segurança da Universidade de New Haven (Connecticut), afirmando que produziu o arquivo malicioso com propósito científico. Sugere ainda a reformulação do sistema de punição aos criadores de vírus. “Não são mais estudantes que fazem isso, por isso acredito que necessitamos de uma lei para brecar essa tendência na internet.”[6]

No início os vírus eram transmitidos principalmente por meio de disquetes, sendo atividades de programadores que queriam demonstrar suas habilidades e virar celebridades no mundo dos hackers sem que isso necessariamente implicasse em prejuízos a suas vítimas. Diferentes dos vírus atuais, que se tornaram atividades criminosas com grupos organizados por fraudadores e profissionais com algum tipo de intenção maliciosa, como roubar dados ou danificar os sistemas de outros usuários.

Como já foi citado, os vírus não podem se autoexecutar para burlar esta deficiência; é preciso que um programa previamente infectado seja executado. Assim, se um programa contaminado for salvo em um HD, isso não vai proporcionar o ataque do vírus; enquanto o evento que ativa o vírus não for acionado pelo usuário, o vírus ficará “adormecido”. Outro mito que deve ser desfeito é de que os vírus podem danificar o hardware do computador. Os vírus são softwares, portanto não há como eles queimarem ou

quebrarem dispositivos do computador; o que pode ocorrer é de um vírus contaminar o BIOS de uma placa-mãe fazendo-a parar de funcionar, dando a impressão de que foi quebrada, mas existem laboratórios que recuperam o BIOS eliminando o vírus nele contido.

Tipos de vírus

a) **Vírus de arquivo:** anexa ou associa seu código a um arquivo de programa normal, costuma infectar arquivos executáveis, principalmente arquivos .COM e .EXE, e só tem efeito se os arquivos contaminados forem executados.

b) **Vírus de boot:** infecta a área de inicialização dos discos rígidos onde se encontram arquivos essenciais ao sistema. Costumam ter alto poder de destruição, impedindo, inclusive, que o sistema operacional seja executado.

c) **Vírus de macro:** são pequenos programas escritos na linguagem de macro de um aplicativo (por exemplo, o Word e o Excel do Microsoft Office) que, em geral, só se propagam em documentos desse aplicativo. Por causa disso, eles também são chamados de vírus de documentos. Para se tornarem ativos, eles precisam que aplicativos correspondentes sejam ativados e que uma das macros infectadas seja executada. Diferentemente dos vírus "normais", os vírus de macro não atacam arquivos executáveis, mas comprometem as configurações dos componentes do programa. A macro modifica o modelo global, fazendo operações inesperadas ou se recusando a realizar outras, causando infecção a todos os arquivos subsequentemente editados no mesmo programa.

d) **Vírus polimorfos** (palavra que provém do grego e que significa "que pode assumir várias formas"): são verdadeiros mestres do disfarce. Como um camaleão,

ele se transforma a cada infecção, modificando sua assinatura e por isso é muito difícil de ser detectado por programas antivírus.

e) **Vírus de e-mails:** enviam-se a si mesmos para todos na lista de correspondência do programa de e-mail do usuário, espalhando-se rapidamente. O vírus se propaga assim que ativado, bastando a exibição do texto da mensagem no painel de visualização (não precisa abrir o anexo) para ocorrer a contaminação. Como resultado, enquanto os vírus costumavam levar meses ou anos para se propagar, estes agora fazem isso em horas. Isso torna muito difícil para o antivírus responder antes que um grande dano seja causado.[7]

Cavalos de troia ou trojan

A engenharia social sempre existiu: conta a mitologia que o "Cavalo de Troia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia. Daí surgiram os termos "presente de grego" e "cavalo de troia"

No mundo virtual a ideia é a mesma: um cavalo de troia é um arquivo aparentemente inocente entregue pela porta da frente, mas que contém um elemento malicioso escondido em algum lugar dentro dele. Os cavalos de troia não podem se multiplicar, o que os diferencia dos vírus e *worms*: eles se alastram quando as pessoas são seduzidas a abrir o programa por pensar que vem de uma fonte legítima.

A maioria dos cavalos de troia são realmente programas funcionais, de modo que o usuário nunca se torna consciente do problema (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.), já que o elemento funcional no programa executa muito bem as funções para

as quais foi projetado, enquanto o elemento malicioso trabalha por trás do usuário para promover os interesses do atacante.

Algumas das funções maliciosas que podem ser executadas por um cavalo de troia são: ➢

Instalação de *Keyloggers* (histórico de teclas): esta ferramenta é muito usada por atacantes cuja finalidade é capturar tudo que a vítima digita, também capturando os cliques do mouse, *printscreen* da tela e vídeo da webcam (podendo ver tudo que o usuário está fazendo). Assim, é possível descobrir suas senhas do Facebook, Skype, Twitter, chats e, lógico, capturar números de contas, senhas e outras informações antes delas serem criptografadas por dispositivos de segurança do sistema financeiro. Depois de tudo capturado, é enviado (geralmente por e-mail) para alguém em algum lugar, que analisa o que foi digitado e levanta as informações necessárias.

Por terem a função de capturar tudo que é digitado, os *keyloggers* são utilizados por empresas que monitoram o que seus funcionarios estão digitando, pelos pais que querem saber o que os filhos estão digitando e acessando e até por governos para fazer espionagem.

□

Instalação de Trojan-Downloader: faz download de outros vírus para seu computador.

□

Instalação de Trojan-Banker: seu objetivo PRINCIPAL é obter os dados de autenticação de usuário e validação de transações em sistema de internet banking.

- **Inclusão de *Backdoors* (porta dos fundos)**: é um utilitário de administração remota que, uma vez instalado, permite um acesso de usuário e controlá-lo através de uma rede ou da internet. Um *backdoor* típico consiste de dois componentes: cliente e servidor. O servidor é a máquina atacada, e o cliente é o atacante. Isto é chamado de ligação direta, quando o cliente liga diretamente para o servidor. Um atacante vai usar o aplicativo cliente para se comunicar com os componentes do servidor, que são instalados no sistema da vítima.

O que o *backdoor* pode fazer?

Dependendo do quão sofisticado é um cliente, o *backdoor* pode incluir recursos como: ➢

- Permite criar, apagar, renomear, copiar ou modificar qualquer arquivo, executar comandos, alterar as configurações do sistema e modificar registros do Windows.

- Permite controlar o hardware do computador, para alterar suas configurações de desligamento ou reiniciar o computador sem a permissão do usuário.

- Permite que o atacante roube logins e senhas pessoais e monitore as atividades dos usuários (log).

- Fazer backup do que o usuário digitou no teclado e captura de tela.



Enviar os dados coletados para o destino especificado (endereço de e-mail, servidor FTP, conexão com um host remoto).



Acionar a webcam para monitorar o que se passa dentro da residência da vítima.



Alteração ou destruição de arquivos.

Ransomware

Este é um tipo de malware que bloqueia o sistema e exige resgate. Geralmente, depois de instalado, o programa irá criptografar o disco do computador ou bloquear o acesso da vítima ao sistema deixando uma mensagem de "resgate" que exige uma taxa para decodificar os arquivos ou restaurar o sistema. Essencialmente, os atacantes mantêm o computador como refém e tentam extorquir dinheiro em troca de liberar o acesso ao computador, mas é importante entender que a vítima não vai recuperar o acesso ao seu sistema, mesmo pagando o dinheiro do "resgate". É uma farsa.

Essas ameaças geralmente se instalam através de vulnerabilidades do computador da vítima, quando usuários desavisados abrem e-mails de *phishing* ou acessam sites maliciosos. Os *ransomwares* são detectados pelos antivírus com certa facilidade, pois costumam criptografar arquivos grandes, mas alguns possuem opções que escolhem inteligentemente quais pastas criptografar ou permitem que o atacante faça isso.

Rootkit

Um *rootkit* também é um *trojan* que busca se esconder de softwares de segurança e do usuário utilizando diversas técnicas avançadas de programação. Por definição, é um programa usado para que um *cracker* possa manter o controle sobre um sistema comprometido sem que o usuário saiba, agindo como *backdoor*, podendo ser instalado tanto localmente (quando alguém tem acesso físico à sua máquina) quanto remotamente.

Um dos problemas dos *rootkits* é que boa parte dos antivírus não conseguem localizá-los, ou seja, eles passam despercebidos, camuflados e o usuário de computador, mesmo com um antivírus instalado, não fica sabendo que há um programa malicioso instalado em sua estação de trabalho.

Possuem esse nome por serem, inicialmente, "kits" de programas para a plataforma Linux/Unix para manter o acesso total ao sistema previamente comprometido; e "root" é o usuário com o controle total do computador nas plataformas Unix.

No Windows, eles "infectam" os processos na memória, de modo que toda vez que um processo requisite alguma informação sobre os arquivos do *trojan*, esta informação seja anulada antes de ser retornada ao programa, o que fará com que os softwares acreditem que estes arquivos não estejam lá. Aparentemente vai estar tudo normal, a vítima vai poder continuar usando a máquina normalmente, mas haverá outras pessoas com acesso irrestrito a ela, que poderão usá-la remotamente da forma que quiserem.

Worms

Um *worm* é um programa similar a um vírus, com a diferença de que ele se autopropaga através de uma rede de computadores, sem ajuda de uma pessoa, e pode fazer um grande estrago na máquina da vítima. Esses programas são difíceis de ser detectados porque não criam arquivos

regulares que possam ser vistos. Eles muitas vezes são notados apenas quando começam a consumir recursos do sistema ou porque o sistema se torna mais lento ou a execução de outros programas simplesmente para. Também podem lotar o disco rígido (HD) devido às cópias que fazem de si mesmos.

Essas pragas se instalam nos computadores para piorar o desempenho, desconfigurar o sistema e principalmente roubar dados sigilosos e senhas.

Para um *worm* infectar uma máquina, primeiro ele precisa descobrir que a máquina existe. A maneira mais comum de um *worm* se propagar é através de anexos maliciosos em e-mails. Algum *worms* chegam a interceptar os e-mails antes de serem enviados para o servidor SMTP, acrescentando anexos. Isso pode ser feito trocando o IP do servidor SMTP para localhost nos arquivos de configuração.

Engenharia social

Esta prática visa a enganação ou exploração da confiança dos usuários levando-os a efetuar uma determinada ação para obter informações importantes ou sigilosas sobre eles. Geralmente o golpista se faz passar por outra pessoa ou instituição, ou finge ser um profissional em determinada área.

A diferença entre ataques de engenharia social e, por exemplo, a tentativa de um atacante conseguir acesso a um determinado site é a escolha das ferramentas utilizadas.

Um atacante irá procurar por vulnerabilidades no servidor da vítima enquanto um engenheiro social utilizará algumas técnicas de persuasão estimulando o **MEDO**, a **CURIOSIDADE**, a **GANÂNCIA** ou a **SIMPATIA** da vítima para obter a informação ou acesso desejado.

Na maior parte dos casos, o engenheiro social evitará contato visual com a sua vítima. Em vez disso, irá utilizar e-mails, mensagens instantâneas e chamadas telefônicas para

conduzir um ataque.

Phishing

De longe, é uma das técnicas mais conhecidas graças a campanhas de conscientização promovidas por grandes provedores de e-mail como o Google e o Yahoo. *Phishing* é um exemplo bastante simples e muito utilizado na engenharia social e que consiste, na maioria dos casos, no envio de e-mails não solicitados para a vítima, estimulando-a a acessar páginas (sites) fraudulentas, preencher formulários com seus dados privados ou despertar curiosidade fazendo com que clique em um link para fazer download de um arquivo malicioso (*malware*) capaz de transmitir para o atacante as informações que lhe interessam.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, os principais tipos de ações envolvendo *phishing* utilizados pelos atacantes são: ➢

Mensagens que contêm links para programas maliciosos.

Oferta de grandes lucros: mensagens de um milionário da África ou da China que esteja interessado em parceria para lavar dinheiro, golpe da pirâmide *etc.*

Fotos de conhecidos ou celebridades: notícias de celebridades, informação de que a pessoa está sendo traída *etc.*

Notícias e boatos: tragédias divulgadas na mídia, boatos

sobre personalidades, fotos de uma pessoa famosa que foi assassinada, filmagens de ator surpreendido consumindo drogas *etc.*

Reality shows: fotos e vídeos sobre BBB, A Fazenda *etc.*

Orçamentos e cotações de preços: geralmente com links para acessar os dados do produto.

Sites de comércio eletrônico: cobrança de débito, devolução de compra e outros fatos envolvendo grandes empresas do gênero.

Empresas de telefonia ou provedoras de acesso à internet: aviso de bloqueio de serviços, promoções, consulta detalhadas *etc.*

Falsos cartões virtuais: cartão do voxcards *etc.*

Avisos de órgãos do governo: CPF cancelado ou pendente de regularização, correção do programa para enviar o Imposto de Renda, título eleitoral cancelado *etc.*

SERASA ou SPC: inclusão de nome em cadastro de devedores, restrições financeiras, possibilidade de acessar o extrato com as informações *etc.*

Ameaças de órgãos do governo: mensagem da Polícia Federal sobre pornografia infantil em seu computador, intimação da Polícia Civil, informação sobre multa, cobrança de impostos, ação de despejo *etc.*

Transações bancárias: necessidade de instalar novo módulo de segurança *etc.*

Em maio de 2012 um ataque de phishing gerou muita repercussão na web e na mídia por ter sido dirigido a uma artista da TV.

O atacante enviou uma mensagem se passando por um funcionário do provedor da internet, mensagem esta que continha um formulário, que foi preenchido pela atriz com seus dados pessoais e inclusive com a senha do e-mail. A partir daí o atacante teve acesso ao e-mail e posse de algumas fotos que estavam na pasta de mensagens enviadas. O atacante quis obter vantagem econômica para não publicar as fotos na internet e, como não conseguiu, postou as fotos e estas se espalharam pelo mundo todo.

Spywares

Spyware são programas espiões cuja função é coletar informações sobre o usuário e seus costumes na internet com ou sem o seu conhecimento.

Eles podem ser usados para determinados fins como:

- Publicidade.

Coleta de informações pessoais.

-

A alteração da configuração do seu computador.

Mas a maioria dos spywares é maliciosa. Seu objetivo é, geralmente, capturar senhas, dados bancários e informações de cartão de crédito – e enviá-los através da internet para os fraudadores.

A propagação dos spywares é semelhante a dos cavalos de troia, porém se difere desses por não ter como objetivo que o sistema do usuário seja dominado ou manipulado por atacantes.

Adwares

Adwares são programas que estão disponíveis gratuitamente para download, mas são patrocinados por anúncios. É instalado um componente adicional, que se alimenta de publicidade, através da apresentação de anúncios pop-up ou baixando uma barra de ferramentas (*toolbars*) no navegador do usuário.

Alguns *adwares* são parentes próximos do spyware, isto porque alguns programas com adware coletam informações sobre o usuário para enviar aos anunciantes. O objetivo é caracterizar um alvo de veiculação de anúncios. Além disso, eles podem, inclusive, roubar a página inicial do navegador ou de busca, redirecionando a vítima para outros sites. O mecanismo pode apresentar anomalias no sistema ou incompatibilidades que causem problemas com outros programas. É até mesmo capaz de atrapalhar o funcionamento do sistema operacional.

Capítulo 4. O Que Um Atacante Faz Quando Invade Um Computador?

Como vimos, existem diversas formas de invadir um computador. As consequências também são bem variadas – em alguns casos objetiva-se apenas infectar computadores alheios para danificar seus componentes, seja excluindo arquivos, seja alterando o funcionamento do computador deixando-o vulnerável a outros tipos de ataques. Mas a maioria dos ataques não visa prejudicar a máquina, e sim o usuário, capturando informações com o objetivo de obter alguma vantagem financeira. Os ataques mais praticados são:

Fraude eletrônica

No Brasil, os crimes de informática superam até o narcotráfico.[8] Somos o terceiro país no ranking mundial neste tipo de crime. A Federação Brasileira dos Bancos (Febraban) divulgou que o internet banking é utilizado por 46% das contas ativas no país e 24% dos 66 bilhões de operações bancárias realizadas em 2011 foram feitas pela internet. E, no mesmo ano, as instituições pagaram cerca de R$ 1,2 bilhão a clientes que tiveram problemas em suas contas bancárias, como transferências e saques indevidos por meio eletrônico.[9]

A praticidade da rede não atrai as pessoas apenas para o uso do internet banking, mas também para as compras

virtuais, fato este que tem aumentado sensivelmente os números de fraudes envolvendo cartões de crédito em todo o Brasil. Arquivos alojados no computador da vítima roubam informações como número do cartão, data de validade e o código de segurança. Com essas informações, qualquer pessoa pode fazer compras no nome de quem quer que seja.

Estatísticas divulgadas pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) mostram que os golpes que utilizam páginas falsas de bancos e sites de comércio eletrônico tiveram aumento de 89% nas notificações recebidas pelo órgão, em relação ao primeiro trimestre de 2012, número cinco vezes maior que no primeiro trimestre de 2011.[10]

São justamente esses números, somados ao comportamento dos usuários, que atraem os criminosos para esta modalidade de crime.

Sequestros de dados

Muitos usuários salvam fotos, dados e arquivos pessoais em seus computadores sem manter cópias desse conteúdo em alguma mídia externa. Sabendo disso, atacantes, depois de introduzir um malware do tipo *ransomware*, sequestram esses dados e exigem resgate. Só depois de feito o pagamento a vítima receberá uma senha com as instruções ou utilitários que permitem restaurar as informações do sistema.

Esse tipo de extorsão é muito mais comum de que se pensa. Uma pesquisa feita por uma empresa de antivírus perguntou a 2.917 usuários se eles pagariam por um possível resgate no caso de perda ou "sequestro" de seus dados pessoais. A pesquisa mostrou um número alarmante: 8% disseram que já foram vítimas desse tipo de roubo de dados e tiveram que pagar resgate, o que se traduz em mais de cinco milhões de dólares por ano pagos aos

cibercriminosos.[11]

Ataques DDoS

Mesmo que você não faça nenhuma movimentação financeira e não tenha o costume de armazenar nenhum tipo de informação pessoal em seu computador você não está livre de ataques. O seu equipamento poderá ser transformado em um zumbi e passar a agir na rede de um atacante.

Essas redes zumbis são criadas quando usuários acessam links contaminados por códigos maliciosos. A partir daí, o atacante passa a controlar remotamente essas máquinas e poderá, por exemplo, promover um ataque **DDoS** (*Distributed Denial of Service*, na sigla em inglês) usado para derrubar grandes sites.

Por meio de um comando que parte de uma ou várias "máquinas mestres", o atacante ordena que os PCs zumbis acessem um endereço específico na mesma data e horário. Esse servidor pode ser responsável por diferentes tipos de serviços – como manter uma página de internet ativa, completar transações bancárias on-line, entre outros. O mais comum é que os ataques aconteçam nos servidores web, onde estão hospedados os sites de uma empresa.

Como um número muito grande de computadores tenta acessar ao mesmo tempo a página de um site, há uma sobrecarga no servidor, que fica, então, impossibilitado de atender a todas as requisições simultâneas de acesso dos "usuários". Alguns desses servidores podem simplesmente reiniciar ou parar de funcionar.

Em janeiro de 2012, após o FBI tirar do ar o site do Megaupload e prender vários dos seus responsáveis ao redor do mundo, o grupo de ativistas Anonymous decidiu realizar um ataque DDoS contra sites das empresas e agências envolvidas, como FBI, MPAA e RIAA, tirando todos do ar.[12] Em junho foi a vez dos portais brasileiros da

Presidência da República, da Receita Federal, do Ministério do Esporte, da Petrobras e do IBGE.

Ataques por botnet

Parece o enredo de um filme de ficção: milhares de células de robôs adormecidos ficam prontas para atacar sempre que o seu líder malévolo determinar e, uma vez ativados, os robôs causam estragos para a humanidade. Mas este cenário não é ficção, na verdade acontece todos os dias na era digital.

O que é um botnet?

O termo descreve uma rede de computadores interligados que realizam de forma coordenada uma tarefa.

Botnets podem transferir secretamente informações, como dados pessoais ou informações de cartão de crédito, para outros computadores. Os computadores (zumbis) são infectados com malware que faz com que eles ajam em nome da rede. Cada computador funciona de forma autônoma e segue as instruções de um computador mestre.

As redes maliciosas também podem ser usadas para transmitir vírus ou redirecionar as pessoas para um site específico, inundando-o com o tráfego e desligando-o como um método de ciberterrorismo. Como é o caso do famoso DDoS.

O sucesso de botnets vem de seu sigilo. A maioria dos usuários nem sequer sabe que o seu computador foi infectado.

Em março de 2013, foi revelado um golpe que atingiu **120 mil** computadores pessoais gerando um prejuízo de **US$ 6 milhões (quase R$ 12 milhões) por mês**.

O golpe foi identificado como "**Chameleon botnet**". Os atacantes conseguiram fazer os computadores gerarem **nove bilhões de cliques** em anúncios que pagam usuários por cada acesso.[13]

Ataques por spyware

Esses programas se instalam no computador com o objetivo de coletar informações de sites em que o usuário navega, preferências de aplicativos que utiliza ou até mesmo informações pessoais como o e-mail, para depois enviar esses dados a empresas que vendem informação para *spammers* (aquelas pessoas que enviam mensagens não solicitadas).

Muitas vezes, os atacantes instalam um *spyware* junto com um *keylogger* ou *screenlogger*. Sempre que o usuário acessa determinados sites de bancos ou de comércio eletrônico, o *keylogger* ou *screenlogger* é ativado para a captura de senhas bancárias ou números de cartões de crédito e para enviá-los através da internet para os fraudadores.

Já que estamos falando de espiões, chamo a atenção dos usuários para o uso das webcams. A webcam do seu computador permite que você faça chamadas de vídeo para os amigos, parentes ou uma reunião de videoconferência, mas essas mesmas câmeras também podem ser usadas sem o seu conhecimento. Sob certas circunstâncias, os atacantes podem explorar a sua webcam para espionar você.

Depois de ganhar acesso ao seu computador através de um trojan, que permite total controle do seu computador, o atacante pode ligar sua webcam a qualquer momento, além de ouvir o áudio do microfone do computador.

Imagine você ou seu filho(a), saindo do banho, e, enquanto se troca em seu quarto, que do outro lado há alguém olhando o tempo todo ou cronometrando o período em que não tem ninguém em casa, identificando objetos de valor para posteriormente planejar um assalto.

Para que um atacante acesse sua webcam, ela deve estar ligada para transmitir uma imagem. Se você quer saber se

alguém está espionando, verifique se a luz da câmera está ligada, já que geralmente todas as webcams têm uma luz que se acende quando está ativada.

Quando não estiver usando a webcam, cubra a lente com um pequeno pedaço de fita preta. Algumas webcams embutidas são projetadas com tampas de proteção que podem ser abertas ou fechadas manualmente. Se você utiliza uma webcam externa desconecte sempre que terminar de usá-la.

Atualize seu antivírus regularmente. Os atacantes podem instalar códigos que lhes dão acesso à webcam. Esta técnica é bem básica e chamada de *clickjacking* e pode vir na forma de um anexo de e-mail, ou programado em um Myspace ou aplicativo do Facebook. Qualquer download pode ter, potencialmente, malware, spyware ou adware anexo, portanto, tenha certeza de manter seu antivírus atualizado em todos os momentos.

Capítulo 5. Crimes Virtuais

Os crimes virtuais não são praticados apenas por atacantes com conhecimento sofisticado de informática. Ameaças cometidas por e-mails como calúnia (acusar alguém de um crime que não cometeu), agressão e desrespeito por motivo de cor, raça, etnia ou religião são cada vez mais frequentes entre os usuários, que utilizam na maioria das vezes redes sociais como Facebook, Twitter, YouTube ou os blogs para práticas desses delitos. Muitas vezes os autores acreditam que suas ações ficarão impunes.

O maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis, mas é importante saber que quando o computador é uma ferramenta para prática dos delitos, suscita a possibilidade de se amoldar aos tipos penais já existentes. Por exemplo, a calúnia pode ser praticada tanto em um jornal quanto na internet: é o mesmo crime, mudando apenas o meio de sua efetivação, potencializando a sua comunicação. Neste caso, as penas aplicadas são as mesmas, independentemente do meio utilizado para a prática do crime.

Principais delitos

A lista de crimes cometidos por meio eletrônico é extensa. Na grande maioria dos casos é possível adaptar os crimes virtuais à legislação vigente.

O Judiciário vem coibindo diariamente a sensação de

impunidade que reina no ambiente virtual e combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas como a Lei n. 9.296/96 – que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática – e a Lei n. 9.609/98 – que dispõe sobre a proteção da propriedade intelectual de programas de computador.

Para o Judiciário, 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizarem crimes comuns praticados através da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, a exemplo da distribuição de vírus eletrônico e dos ataques DDoS.

Veja alguns exemplos de crimes e leis que podem ser utilizados no meio eletrônico: ➢

USO INDEVIDO DE IMAGEM. Postar fotos de terceiros sem autorização pode levar a processo. O **Artigo 5º Inciso X da Constituição Federal** diz que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando direito à indenização pelo dano material ou moral".

INSULTOS. Falar mal ou insultar alguém numa rede social pode gerar processo com base no **Artigo 140 do Código Penal**, que pune "a injúria que ofende a dignidade ou decoro".

CALÚNIA. Quem inventar histórias falsas sobre alguém no Orkut, Twitter ou Facebook pode ser enquadrado no **Artigo 138 do Código Penal.**

DIFAMAÇÃO. Associar uma pessoa a um fato que ofende sua reputação. **Artigo 139 do Código Penal**.

AMEAÇA. Significa intimidar alguém, podendo ser por gesto, telefone, de forma escrita e e-mails. **Artigo 147 do Código Penal**.

DIVULGAÇÃO DE SEGREDO. Revelar segredos de terceiros na internet, ou de documentos/correspondência confidencial que possam causar dano, pode levar a processo com base no **Artigo 153 do Código Penal.**

FURTO. Utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro. **Artigo 155 do Código Penal.**

DANO. Enviar vírus, realizar ataques de DoS ou DDoS ou outro que destrua equipamentos ou seu conteúdo. **Artigo 163 do Código Penal.**

CÓPIA NÃO AUTORIZADA. Copiar ou plagiar obras de terceiros viola seus direitos autorais, o que cai no **Artigo 184 do Código Penal.**

ESCÁRNIO POR MOTIVO DE RELIGIÃO. Criar comunidade on-line que fale sobre pessoas e religiões. **Artigo 208 do Código Penal**.

□

FAVORECIMENTO DA PROSTITUIÇÃO. **Artigo 228 do Código Penal.**

□

ATO OBSCENO. **Artigo 233 do Código Penal.**

□

ESCRITO OU OBJETO OBSCENO. **Artigo 234 do Código Penal.**

□

INCITAÇÃO AO CRIME. **Artigo 286 do Código Penal.**

□

APOLOGIA DE CRIME. Criar comunidades virtuais (fóruns, blogs etc.) para ensinar como fazer "trambiques" ou "divulgar ações ilícitas realizadas no passado, que estão sendo realizadas no presente ou serão realizadas no futuro". **Artigo 287 do Código Penal.**

□

FALSA IDENTIDADE. Criar um perfil falso numa rede social, blog ou microblog pode levar a processo judicial com base no **Artigo 307 do Código Penal.**

□

INSERÇÃO DE DADOS FALSOS EM SISTEMAS DE INFORMAÇÕES. Fazer cadastro com nome falso em uma loja virtual. **Artigo 313-A do Código Penal.**

ADULTERAR DADOS EM SISTEMAS DE INFORMAÇÕES. Entrar na rede da empresa ou de concorrente e alterar informações sem autorização. **Artigo 313-B do Código Penal.**

PRECONCEITO OU DISCRIMINAÇÃO. Comentar em chats, e-mails, blogs e outros, de forma negativa, sobre raças, religiões, etnias *etc.* **Artigo 20 da Lei 7.716/89.**

PEDOFILIA. Troca de informações ou imagens envolvendo crianças ou adolescentes. **Artigo 241-A/241-B/241-C/241-De241-E da Lei nº 8.069/90 ECA.**

CRIME CONTRA A PROPRIEDADE INDUSTRIAL. Usar logomarca de empresa em um link na página da internet, em uma comunidade, em um material, sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir à confusão. **Artigo 195 da Lei 9.279/96.**

CRIME DE CONCORRÊNCIA DESLEAL. Empregar meio

fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem, por exemplo, através do uso da marca do concorrente como palavra-chave ou link patrocinado em buscador. **Artigo 195 da Lei 9.279/96.**

INTERCEPTAÇÃO DE COMUNICAÇÕES DE INFORMÁTICA. Monitoramento não avisado previamente. **Artigo 10 da Lei 9.296/96.**

CRIMES CONTRA SOFTWARE ("PIRATARIA"). Usar cópia de software sem licença. **Artigo 12 da Lei 9.609/98.**

NEGLIGÊNCIA. Este é um alerta importante para os pais que deixam seus filhos passar tempo demais no computador sem supervisão: não vigiá-los, nem criar regras para o uso consciente da internet, mesmo fora de casa, fere os **Artigos 932, Incisos I e IV e 1.634, Incisos I e V do Código Civil**, assim como os Artigos 3º e 4º do Estatuto da Criança e do Adolescente.

REFERENTE ÀS LEIS DE ROUBO DE PERFIL EM COMUNIDADES E BLOG. O remendo constitucional 12888-2/07 pune quem roubar perfil, blog ou comunidade com pena de um a quatro anos de prisão.

Na tabela a seguir pode ser visto um resumo da pesquisa realizada pela Symantec, onde são quantificadas as ações dos delitos antes relacionados à vida das pessoas. A proximidade dessas ameaças é muito grande e não é mais

necessário ficar exposto nas ruas para sofrer algum tipo de ataque – basta sentar diante de um computador e se conectar a essa nova realidade.

Vítimas de crimes	69% dos entrevistados em 24 países – 72% foram homens e 65% mulheres.
Dispositivos móveis	44% dos proprietários de celular no mundo usam o aparelho para acessar a internet; 10% tiveram seus dispositivos móveis atacados; 16% instalaram uma segurança mais atualizada.
Vírus ou *Malwares*	No mundo 54% enfrentaram problema com esse tipo de praga – no Brasil, 68%.
Hábitos arriscados	77% dos que usam wi-fi gratuito sofreram crime cibernético contra 62% que não usam.
Crime físico x cibernético	15% dos adultos foram vítimas de algum crime no mundo físico e 44% de crimes cibernéticos.
Pais e filhos	87% dos pais cujos filhos tiveram alguma experiência negativa on-line foram também vítimas de crime cibernético.
Complacência	41% dos adultos não atualizam os programas de segurança de seus computadores.
Providências	21% das vítimas relataram o crime à polícia.

O resumo desse estudo pode ser acessado em: http://br.norton.com/cybercrimereport/promo.

Furto de identidade

Neste tipo de contravenção criminosos usam dados pessoais alheios para aplicarem golpes na emissão de cartões de crédito, abertura de contas correntes, abertura de empresas, fazer empréstimos e compra de bens.

O furto de identidade não é novidade. Os ladrões sempre encontram maneiras de obter ilegalmente informações pessoais dos cidadãos por meio de golpes de confiança (veja engenharia social), roubando correspondência de caixas de correio ou até mesmo procurando em latas de

lixo. Agora que o furto de identidade alcançou a internet, os criminosos podem aplicar golpes em maior número de pessoas, o que o torna muito mais rentável.

A Serasa Experian registrou 2,14 milhões de tentativas de fraudes contra o consumidor em 2012; um aumento de 10% se comparados aos 1,96 milhão de 2011. Só de janeiro a maio de 2013, foram registradas 837.641 tentativas de fraude.

Segundo a empresa, o resultado mostrou que a cada quinze segundos um consumidor brasileiro foi vítima de tentativa de furto de identidade. Isso acontece porque é comum as pessoas fornecerem seus dados pessoais em cadastros na internet sem verificar a idoneidade e a segurança dos sites. Outro fator impulsionador desse tipo de ação é a popularização das mídias sociais.[14]

O Phishing é um dos meios mais utilizados pelos atacantes para obter o maior número de informações possível do usuário, pois quanto mais dados o golpista tem disponível, mais convincente ele será quando estiver se passando pela vítima.

Enquanto escrevia este livro recebi um *Phishing* na minha caixa postal onde o atacante tenta despertar minha curiosidade. O remetente era uma pessoa que realmente estava na minha lista de contatos, o que me leva a crer que sua máquina está contaminada e talvez ele nem saiba disso. A mensagem fraudulenta dizia que ele estava precisando de dinheiro e pedia para eu visualizar a cópia de um cheque que eu teria passado para ele.

nbsp;microfilmagem cheque sem fundo :
Visualizar debito.pdfnbsp;(115,5 KB) “aquele cheque que tu deu pra mim
voltou pela segunda vez”
em nome de: ----------

Ao clicar na imagem do cheque é transferido para o meu

computador um trojan que, além de começar a espionar minhas ações até conseguir obter alguma vantagem, ainda usará minha lista de contatos para se autoenviar, aumentando assim o número de vítimas.

Volte ao Capítulo 3 e reveja os principais tipos de ações envolvendo *phishing* utilizados pelos atacantes.

Crimes virtuais nas redes sociais

A necessidade do ser humano de interagir fez das redes sociais o maior ponto de encontro de pessoas com algo em comum.

Nas redes você pode convidar para fazer parte do seu grupo as pessoas de quem você gosta, e por meio destas chegar a outras de quem você havia se distanciado ou mesmo perdido por completo o contato.

O brasileiro está cada vez mais conectado. Uma pesquisa feita no segundo semestre de 2012 pelo **Ibope NetRatings** apontou 83,4 milhões de brasileiros com acesso à internet, tendo este número pulado para **102 milhões em abril de 2013** segundo a empresa de audiência on-line Navegg. As conexões em domicílios e no trabalho foram as principais responsáveis pela expansão dos internautas. O Brasil é o quinto país com o maior número de conexões à internet.

Outra pesquisa realizada pela Hi-Mídia em parceria com a M.Sense identificou que, entre os internautas do Brasil, 95% deles acessam ao menos uma vez uma rede social por mês.

O Facebook e o Orkut são as redes mais acessadas no país. Do total de internautas que acessaram alguma rede social (95%), 72% deles afirmaram que acessa o Facebook ao menos uma vez ao dia e 41% utiliza o Orkut.

Quando o assunto é Facebook, o Brasil é o que mais ganhou novos usuários ativos mensais – quase 30 milhões – de 1º

de janeiro a 31 de dezembro de 2012, de acordo com estudo divulgado pelo ***SocialBakers***[15], plataforma que monitora o uso das redes sociais mundialmente. Nosso país está em segundo lugar no ranking mundial de perfis cadastrados com 65 milhões, atrás apenas dos Estados Unidos, com aproximadamente 164 milhões de perfis cadastrados na rede. Índia, Indonésia, México completam a lista dos cinco primeiros países.

Com números tão expressivos, não é de se estranhar que pessoas mal-intencionadas escolhessem este palco para prática de diversos crimes.

Pornografia infantil (pedofilia)

Consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da web, e-mail, newsgroups, salas de bate-papo (chat), ou qualquer outra forma. Compreende, ainda, o uso da internet com a finalidade de aliciar crianças ou adolescentes para realizarem atividades sexuais ou para se exporem de forma pornográfica.

Casos de pornografia infantil dominam as denúncias de crime na internet feitas no Brasil. De janeiro de 2006 a outubro de 2012, 40,5% do que foi denunciado no país supostamente abrigava conteúdo desse tipo. O levantamento inédito é da ONG Safernet, especializada em segurança na rede.[16]

Como os pedófilos agem Para conquistar a confiança das crianças e dos adolescentes os criminosos utilizam perfis falsos e uma linguagem diferenciada, com intuito de programar encontros virtuais e presenciais que viabilizam a prática de atos de violência sexual.

Em muitos casos oferecem oportunidades imperdíveis, presentes ou até mesmo dinheiro para convencer a vítima a marcar um encontro ou pedem para que se façam fotos e

vídeos pornográficos.

Comportamento de crianças e adolescentes na internet Um estudo realizado em outubro de 2012 pelo CGI (Comitê Gestor da Internet) apontou ser preocupante a popularização das redes entre crianças e adolescentes. Os números indicam que 2,70% dos jovens entre 9 e 16 anos têm seu próprio perfil em algum site de relacionamento e desses 13% postaram os endereços de casa na internet e divulgaram seus telefones.

O mesmo estudo mostrou que as crianças não sentem pudor em publicar informações privadas e fotos dentro das redes sociais. 86% dos entrevistados possuem ao menos uma foto de seu rosto publicada, 69% já divulgaram seu sobrenome e 28% informaram a escola em que estudam.

23% dos jovens já tiveram contato com desconhecidos por meio da Internet ou já tiveram encontro real.[17]

Foi o que aconteceu com uma estudante de 14 anos em São Paulo, em caso mostrado pela mídia em agosto de 2012. Após contato feito através de uma sala de bate-papo, a adolescente foi convencida por um casal a participar de uma sessão de sadomasoquismo, onde foram feitas algumas fotos e posteriormente divulgadas na internet. Em troca, a estudante ganhou um espartilho.

O casal foi preso logo depois que o pai da menina percebeu mudanças de comportamento na filha e passou a vigiá-la, instalando um software espião no notebook da adolescente. Ele informou à polícia, que prosseguiu com as investigações.[18]

Como a polícia tem agido nos casos de pedofilia Pouco conhecida pelo público, a Polícia Civil de São Paulo criou em novembro de 2011 a **4ª Delegacia de Repressão à Pedofilia**, única delegacia no Brasil especializada nesse tipo de crime. Investigadores passando-se por crianças conseguem se infiltrar em redes de pedofilia que agem em

diversas redes sociais. O trabalho, pioneiro, resultou em um cadastro e um banco de dados, que contêm dados como foto, nome, cor de pele, idade e histórico de crimes dos pedófilos, permitindo rastrear muitos abusadores de crianças. Segundo a delegacia, 40% desses criminosos têm entre 18 e 40 anos, 25% estão acima dos 40 e o restante são menores de idade.

O que é sexting O termo é originado da união de duas palavras em inglês: "sex" (sexo) e "texting" (envio de mensagens). Consiste no envio de conteúdos sexuais (principalmente fotografias e/ou vídeos), produzidos geralmente pela própria pessoa remetente ou com seu consentimento, para outras pessoas através do celular para grupos de redes sociais, e-mail, salas de bate-papo e comunicadores instantâneos. O fenômeno criado por jovens nos EUA ganha cada vez mais popularidade no Brasil, até porque a tecnologia vem avançando e as facilidades da internet, dos aplicativos e das redes sociais colaboram para esta prática.

□

Preocupação. Uma pesquisa realizada pela ***Comunidade eCGlobal***, em parceria com a iniciativa **TelasAmigas**, revelou dados exclusivos sobre a prática do sexting no Brasil e em outros países da América Latina em relação a comportamento, opinião e prevenção. A pesquisa apontou que esta prática tem se tornado um fenômeno atual, com **40%** da população pesquisada praticando-o. Inclusive, a maioria das pessoas que praticaram sexting, de uma forma ou outra, nunca ouviu falar da expressão.[19]

□

Perigo. No Brasil os principais riscos associados ao

sexting são **extorsão (59%), cyberbullying (45%), danos à honra, intimidade e imagem (42%) e pornografia infantil (36%)**. Este último dado deixa um alerta, já que muitos dos praticantes do sexting são menores, o que contribui para a ação dos pedófilos que já criaram alguns websites dedicados a coletar e explorar comercialmente fotos e vídeos criados por sexting. Um estudo da Internet Watch Foundation (IWF) comprovou que **88% das imagens e vídeos de tipo erótico ou sexual autoproduzidas por jovens e publicadas na WWW** (especialmente nas redes sociais e sites dedicados a emissões de webcam), **são captadas e republicadas sem permissão em outros sites**, especificamente em **sites pornôs**.[20]

□

Riscos psicológicos. Uma pessoa cuja imagem ou vídeo erótico é distribuído sem controle pode ser publicamente humilhada e molestada (cyberbullying se menor de idade), e sofrer sérios problemas por causa disso como ansiedade, depressão, baixa autoestima, trauma, humilhação, isolamento social *etc.* Alguns especialistas argumentam que o risco social é maior em cidades pequenas. Há casos de adolescentes que tiveram de abandonar a escola ou ir para outro lugar por causa da difusão dessas imagens. No Canadá a prática do sexting por uma adolescente de 15 anos levou-a ao suicídio logo depois de ser vítima de cyberbullying. Sua história pode ser vista em um vídeo de nove minutos postado no YouTube chamado "Minha história". A adolescente conta que usava chats de webcam para conhecer e falar com novas pessoas on-line. Ela disse que as pessoas a achavam "impressionante, linda, perfeita" e que um homem a pressionou para mostrar os seios. Logo depois, Amanda

Todd recebeu uma mensagem no Facebook de um homem desconhecido dizendo para ela "dar um show" para ele, caso contrário ele iria enviar o vídeo onde Todd mostrava os seios para todos. Durante as férias de Natal, Amanda disse que a polícia chegou a sua casa às quatro da manhã para lhe dizer que o vídeo havia sido postado na rede. A jovem relata que nunca conseguiu tirar o vídeo do ar e ter sua vida de volta. Passou a ter depressão e síndrome do pânico, até chegar ao suicídio. [21]

□

Responsabilidades dos pais. É importante que os pais conheçam as amizades dos seus filhos, o seu comportamento dentro e fora de casa. Pergunte sobre sua atividade na internet e nos telefones. Procure fazê-los entender que as fotos e mensagens enviadas através dos seus celulares não são realmente anônimas ou privadas e que outros podem transmiti-las sem o seu consentimento. No lugar das velhas dicas para não receber doces nem carona de estranhos, hoje os pais precisam alertar os filhos para não divulgarem dados pessoais na internet, não aceitarem convites para se encontrarem com amigos virtuais e nem receberem arquivos de estranhos – sob pena de responderem pelo crime de ***NEGLIGÊNCIA*** descrito anteriormente.

Apologia a crime ou a criminoso

Criminosos estão usando os sites de relacionamentos para propagar fotos com armas, vídeos enaltecendo o crime e incentivando o uso de drogas, fazendo clara apologia a diversos crimes e facções criminosas.

Na maioria das vezes as imagens postadas servem como prova; e mesmo que as mensagens não sejam suficientes para constatar o delito, elas podem servir de pista para a

polícia.

Policiais do Rio de Janeiro prenderam na noite do dia 04 de outubro de 2012 um traficante que postou fotos em uma rede social portando armamento pesado.

Em seu perfil, o jovem se vangloriava por estar sob efeito de drogas. Nas fotos o criminoso aparecia portando fuzis, granadas e pistolas no alto de um morro. Nas publicações ele se dizia integrante de uma facção e revelava a participação em confrontos contra criminosos de uma organização rival.[22]

Em outro caso, em agosto de 2011 na cidade Taubaté, um criminoso postou vídeo onde aparecia mostrando duas armas e dizendo "Tamo preparado para a guerra". Ainda desdenhava do trabalho da polícia. "Pode vim policinha, pode vim". O vídeo chamou a atenção da Polícia Militar, que efetuou a prisão do bandido e, além de encontrar o computador com o vídeo, encontrou também 22 pedras de crack.

Sequestradores escolhem vítimas pela internet

A mídia deu destaque a um caso de sequestro que aconteceu em 2010. Um estudante de 19 anos foi mantido refém em uma casa, a 150 quilômetros de Sorocaba, em Ilha Comprida, litoral sul paulista.

Nove sequestradores foram presos. O que chamou a atenção da polícia nesse caso foi a forma como os sequestradores descobriram o perfil e a rotina das vítimas: a quadrilha escolhia as pessoas sem sair de casa. Tudo era feito pela internet.

Segundo a polícia, os criminosos passavam horas e horas em sites de relacionamento, à procura de pessoas com sinais de riqueza. Os sequestradores olhavam principalmente as fotos, para saber, por exemplo, como era a casa da família e se a possível vítima fazia viagens para o exterior.[23]

Vejo muita gente nas redes sociais adicionando outras pessoas que nem ao menos conhecem apenas para ter uma lista de amigos enorme passando-se por popular, dando de mão beijada todas as informações de que os criminosos precisam para agir.

O perigo de aceitar "amigos" estranhos on-line é justamente saber se este estranho é quem realmente se diz ser. Os usuários deixam à disposição seus perfis colocando em risco sua integridade física e de seus familiares. Sem muito esforço, os criminosos podem coletar interesses das pessoas, localização, movimentos e se estão fora de casa.

Na dúvida, é melhor reter a informação. Qualquer rede social, hoje, tem controles de privacidade. Você pode definir quem vai ver tal conteúdo, quem vai visualizar tais fotos. Desta forma, só aquelas pessoas que você realmente conhece e que não vão comprometer você de nenhuma forma terão acesso.

Cyberbullying

Cyberbulling é a ação intencional de alguém fazer uso das tecnologias de informação e comunicação (TICs) para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa.

Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de forma imediata os resultados da sua ação, minimizando um possível arrependimento ou remorso.

Essa realidade cria um falso sentimento de que na internet pode-se dizer ou fazer coisas que normalmente não seriam feitas presencialmente. É importante frisar que no cyberbullying o agressor geralmente está acobertado pelo anonimato, atingindo um universo sem proporções, deixando as vítimas ainda mais vulneráveis, enquanto que no bullying o agressor é identificado e as agressões são

regionalizadas, fazendo com que a vítima encontre refúgio fora do ambiente onde foi hostilizada.

O cyberbullying é comum entre os menores, mas a justiça vem decidindo que a responsabilidade – neste caso é dos pais, que devem saber o que os filhos fazem na rede, para que possam educá-los seja no ambiente real ou digital. Veja o caso a seguir.

A Justiça do Paraná condenou os pais de duas adolescentes ao pagamento de R$ 15 mil como indenização por danos morais, em razão destas terem colocado no perfil de uma página de relacionamento social da vítima mensagens de cunho pejorativo. Após perder o acesso a seu perfil, pois as infratoras haviam trocado a senha, a vítima não se importou com o fato e só alguns meses depois, alertada por uma professora, descobriu o ocorrido e constatou as ofensas. A vítima procurou então a policia, que, mediante inquérito policial, chegou à identidade de quem postou as ofensas.[24]

Crimes contra a honra

Difamar, caluniar e denegrir a imagem das pessoas através das redes sociais já virou até profissão. Em outubro de 2012 o delegado da 4ª Delegacia de Investigação sobre Fraudes Financeiras e Econômicas de São Paulo prendeu em flagrante um criminoso cuja especialidade era criar, sob encomenda, blogs para difamar, caluniar e denegrir a imagem das pessoas.

Umas de suas vítimas foi o presidente da Microcamp, Eloy Tuffi. O criminoso criou um blog com posts que denegriam a imagem pessoal e profissional de Eloy. Certo de que os criminosos e mandantes serão punidos, Tuffi faz um apelo a todas as vítimas de crimes Virtuais. “Denunciem. Não podemos nos intimidar. Ninguém tem o direito de nos caluniar”.[25]

Mulheres são maiores vítimas da chamada

"pornografia da vingança ou vingança do mouse"

O meu blog www.crimespelainternet.com.br recebe diariamente dezenas de denúncias envolvendo crimes contra a honra, cujos motivos são diversos, porém nenhum justificável. Certas perseguições são tão absurdas que se torna difícil acreditar que alguém seja capaz de fazer. Como exemplos temos diversos casos de ex-namorado(as) que, muitas vezes inconformados com o fim do relacionamento, postam fotos ou filmes para expor a intimidade do casal, causando transtornos na vida pessoal da pessoa agredida, comprometendo relações familiares e até de empregos.

No começo de julho de 2012, a ex-assessora parlamentar Denise Leitão Rocha foi exonerada do cargo comissionado que ocupava no Senado depois do vazamento de um vídeo íntimo que a mostrava fazendo sexo. Denise afirmou que sua vida se transformou em um "inferno" desde que o vídeo começou a ser divulgado. "Infelizmente, fui vítima de um canalha e estou sofrendo por isso", declarou.[26]

Outro caso aconteceu com uma jovem que teve sua intimidade devastada através de fotos e vídeos de momentos íntimos que foram publicados na internet pelo ex-namorado que afirmava ter sido traído pela garota. O perfil se espalhou por toda a web e chegou ao **Trending Topics do Twitter.**[27]

Quando não é divulgando fotos ou vídeos, é criando situações constrangedoras. Uma dentista de Porto Alegre, depois de terminar um relacionamento, começou a receber ligações de pessoas querendo contratá-la para programas sexuais. Após breve investigação, descobriu que o autor do e-mail que divulgava seu telefone era o ex-namorado. Depois de a indenização ter passado de R$ 15 mil para R$ 30 mil, o processo está no STJ aguardando decisão.[28]

De cada **dez** casos de difamação na internet **oito** são de mulheres prejudicadas por seus ex-companheiros.

Perfis falsos

Uma conduta que cresce a cada dia no meio eletrônico, principalmente nas redes sociais, são os chamados perfis falsos, também conhecidos como 'fakes' com o uso não autorizado de imagens de terceiros divulgando conteúdos que atacam honra e a imagem destes.

Quem cria perfil falso usando a imagem de outra pessoa viola o previsto na Constituição Federal em seu artigo 5º, inciso X, bem como o direito de personalidade previsto pelo Código Civil.

Esta prática pode incorrer em crime de **falsa identidade** quando for para obter vantagem, em proveito próprio ou alheio, *ou para causar dano a outrem*. Além disso, poderá incidir a repercussão cível em que a pessoa lesada poderá requerer ressarcimento pelos danos morais causados.

Só no Facebook, segundo a própria empresa, cerca de **83 milhões** de contas de usuário da rede social podem ser falsas.

Um projeto de lei criado pela deputada federal **Liliam Sá (PSD-RJ)** poderá qualificar como criminoso quem mantiver um perfil falso na internet. A autora do projeto sugere que as punições para a infração sigam o decreto-lei 2848/1940, número de registro do Código Penal, ou seja, o cidadão poderá receber multa, ter seus direitos restringidos ou ser preso, dependendo da sentença atribuída pelo Judiciário. A íntegra do ***projeto de lei 5475/2013*** – apresentado em 26 de abril de 2013 – está disponível no site da Câmara Federal.[29]

Xenofobia e bairrismo

A xenofobia é uma forma de discriminação social que consiste na aversão a diferentes culturas e nacionalidades. Considerada crime de ódio, a xenofobia mostra-se através de humilhação, constrangimento, agressão física e moral àquele que não é natural do lugar do agressor. Nas redes

sociais a xenofobia vem sendo praticada por pessoas que se esquecem ou não sabem que a liberdade de expressão tem limites.

Em novembro de 2010, quando as pesquisas de boca de urna anunciaram a vitória de Dilma Rousseff na eleição para a Presidência da República, uma estudante de direito de São Paulo postou no Twitter mensagens preconceituosas contra nordestinos. O Ministério Público Federal denunciou a estudante por crime de discriminação ou preconceito de procedência nacional e ela foi condenada a pagar multa e prestar serviço comunitário. [30]

Em outra ação, o Ministério Público do Estado de São Paulo denunciou três homens por discriminação contra nordestinos veiculada em e-mails enviados à Escola de Samba Acadêmicos do Tucuruvi, que em 2011 homenageou os nordestinos que residem em São Paulo com o enredo *Oxente, O que Seria da Gente sem Esta Gente? São Paulo, A Capital do Nordeste.* Os denunciados enviaram em dezembro de 2010 uma série de mensagens criticando a escolha com termos que, segundo o MP-SP, caracterizam discriminação e preconceito contra os nordestinos: "Vocês deveriam ser proibidos de desfilar em uma avenida da minha cidade o enredo nojento e racista desses", diz um dos e-mails."Querem exaltar o nordeste, desfilem por lá, e não na minha cidade que se chama São Paulo, capital do Estado de São Paulo", diz outro trecho da mensagem eletrônica enviada por um dos denunciados. Em outro e-mail, um deles afirma: "Temos de valorizar a cultura paulista e não esse povinho de cabeça chata".

Os denunciados foram localizados depois que os provedores de internet, cumprindo ordem judicial, informaram os titulares das contas dos e-mails enviados à Escola de Samba.[31]

Casos de polícia

Torcidas marcam encontros para brigar Outra prática criminosa está chamando a atenção das autoridades policiais. Trata-se de eventos marcados por torcidas organizadas de grandes clubes para brigar e destruir patrimônio público. Em 25/03/2012 uma avenida de São Paulo virou palco de uma verdadeira batalha campal entre duas torcidas. Segundo a Polícia Militar, cerca de quinhentos torcedores de dois clubes se enfrentaram e dois deles acabaram baleados. Os torcedores estavam armados com paus, canos e rojões. Barulhos de tiros foram ouvidos também. O confronto pode ter sido marcado nas redes sociais.[32]

Eleitores cometem crime ao postar fotos de votação na internet

Basta alguns instantes para percebermos que as pessoas postam de tudo nas redes sociais. Tiram fotos de tudo que acham que vai chamar a atenção e para verem seus posts sendo curtidos e compartilhados.

No primeiro turno das eleições municipais de 2012 em São Paulo, mais de cem fotos com a "urna eletrônica" podiam ser vistas no Instagram, mídia social especializada em fotos. Eleitores se fotografaram no momento em que votavam, violando o sigilo de voto. As fotos eram acompanhadas de mensagens de comemorações e expectativas dos eleitores nos seus candidatos. Em uma delas, um eleitor postou a frase "tirando foto escondido da #urna". Todos foram presos em flagrante cometendo o delito. A punição para este crime é de detenção de 6 meses a 1 ano, que pode ser substituída por prestação de serviços à comunidade pelo mesmo período e multa.[33]

MEC elimina candidatos que postaram fotos da prova do Enem No início de novembro de 2012 foi a vez do Ministério da Educação (MEC) agir coercitivamente

eliminando 63 candidatos que, em desrespeito ao edital do Enem, postaram imagens das provas nas redes sociais. O que eles não imaginavam era que o MEC estaria monitorando as redes sociais.[34]

TJ-SP nega recurso a condenado por vender abortivo na internet

Em novembro de 2009, após uma reportagem do G1 que apontou a facilidade da compra de abortivos pela internet, a polícia chegou até um homem em Atibaia, no interior de São Paulo. Ele foi condenado a 13 anos e 4 meses de prisão com base no artigo 273 (crime contra a saúde pública) do Código Penal, mas foi autorizado a recorrer em liberdade. Em 06 de novembro de 2012, o Tribunal de Justiça de São Paulo (TJ-SP) negou o recurso sem analisar o mérito do pedido, por entender que o tipo de recurso protocolado, um recurso especial, não era o instrumento adequado para o caso.[35]

Justiça Federal aceita denúncia contra neonazista preso em BH

Em Belo Horizonte, a Polícia Civil prendeu um jovem conhecido como "Donato di Mauro" suspeito de divulgar fotos no Facebook em que aparece enforcando um morador de rua na região da Savassi. O caso ocorreu em abril de 2013 e provocou revolta. Na época, ele ainda colocou a legenda: "Quer fumar "crackinho", quer? Em meio a praça pública cheia de criança?", dando a entender que a vítima era usuária de drogas.[36]

Justiça Federal condena 25 réus por crimes virtuais

Em julho de 2013, a Justiça Federal de Imperatriz condenou 25 pessoas pelos crimes de furto praticados pela internet. As ações penais apuraram os crimes da chamada "**Operação Galáticos**", realizada pela Polícia Federal em 2006. Os criminosos faziam parte de uma quadrilha que

utilizava programas para capturar senhas bancárias de clientes de vários bancos, principalmente da Caixa Econômica Federal. Com os dados, os criminosos transferiam valores para contas de “laranjas”, realizavam compras pela internet, recargas de celulares e pagamentos de boletos bancários. A operação foi batizada de ‘**Galáticos**’ porque era assim que os criminosos se autodenominavam e faziam questão de ostentar bens adquiridos com o produto do roubo, especialmente carros de luxo. As penas variaram de 2 anos a 10 anos, dependendo do crime em que cada um dos réus foi enquadrado.[37]

Esses são alguns exemplos dos 55 mil casos relacionados a crimes virtuais que já foram julgados pela justiça brasileira. É ilusão pensar que estar atrás de uma tela de computador garantirá o anonimato e a impunidade.[38]

Capítulo 6. Como se Proteger de Ataques e Crimes Virtuais

Todos os dias pessoas são ofendidas nas redes sociais, outras são cobradas por compras que nunca fizeram, centenas de contas são saqueadas e muitas vítimas nunca recebem os produtos que compraram na internet. Neste cenário fica claro que na web nada é 100% seguro e que qualquer um pode ser vítima. É importante que os usuários estejam cientes dos riscos e possam se prevenir de forma adequada.

Pensando nisso, diversos órgãos governamentais e privados se dedicam a desenvolver um conjunto de ações visando o uso ético, responsável e seguro da internet no Brasil. Todos com um objetivo em comum: estimular os brasileiros a aproveitar todo o potencial da rede, adotando os cuidados necessários para utilizarem com segurança este grande espaço coletivo.

Entre as ações desenvolvidas por esses órgãos estão as cartilhas com diversas dicas para o uso seguro da internet, que são disponíveis para consulta na forma ilustrada e também em formato PDF e geralmente podem ser usadas sem restrições para divulgação.

Basicamente, todo material produzido aborda alguns pontos que de uma forma geral ajuda o usuário a utilizar o computador e a internet com maior segurança. No site do Centro de Estudos, Resposta e Tratamento de Incidentes de

Segurança no Brasil (CERT.br) o leitor encontrará diversos fascículos para download. Basta acessar o link: http://cartilha.cert.br/

No meu blog ***crimes pela internet*** o leitor encontrará diversas cartilhas desenvolvidas por outros órgãos, além de, é claro, as cartilhas do CERT.br. Basta acessar o link: http://www.crimespelainternet.com.br/category/cartilhas/

Mantenha o seu computador protegido

Um estudo indica que 16% dos computadores no Brasil não possuem software contra ameaças virtuais instalado, o que os torna mais vulneráveis a invasões de atacantes e a vírus.

Os dados são de um levantamento divulgado pela companhia de segurança digital McAfee. Foram analisados cerca de 28 milhões de computadores por mês em 24 países diferentes durante o ano passado.[39]

Com alguns cuidados básicos é possível manter o seu computador seguro.

Sistemas operacionais e demais programas

O sistema operacional e os programas devem estar sempre atualizados, pois isso ajuda a proteger o computador contra vírus e outras ameaças. Falhas de segurança que podem ser exploradas por atacantes são corrigidas.

É comum as primeiras versões de um programa conterem erros que comprometem a segurança do seu computador. Só para se ter uma ideia, a **Microsoft** lançou o seu novo sistema operacional, Windows 8, em 26 de outubro de 2012 e já na semana seguinte, em 09 de novembro de 2012, anunciou a liberação de seis atualizações de segurança para corrigir dezenove vulnerabilidades no Windows, no Internet Explorer e no framework .Net.[40]

Utilize sistemas operacionais e outros programas originais e autorizados. Se o seu sistema operacional e demais programas não forem originais, você não poderá contar com

o benefício das atualizações.

Mantenha o seu navegador (Internet Explorer, Firefox, Google Chrome...) sempre atualizado. Uma pesquisa realizada pela Kaspersky com sua base de usuários no mundo todo revela que, quando uma nova versão de um navegador é lançada, leva-se mais de um mês para a maioria dos usuários fazer o upgrade.[41]

Antivírus e anti-spyware

O antivírus é obrigatório em qualquer computador. Um bom antivírus é capaz de identificar e eliminar phishing, spyware, rootkit e deve ter ainda sistemas para verificar vírus em e-mails, mensageiros e programas de trocas de arquivos P2P. Esses programas estão sempre à procura de novas ameaças que se disseminam na web, por isso existem atualizações diárias que mantêm a segurança.

Recomenda-se usar antivírus de fabricantes conhecidos, mesmo se forem gratuitos, para não cair no golpe do antivírus falso, os chamados scareware. Um scareware exibe um resultado falso de uma varredura nos arquivos, mas na verdade são fraudes que levam o usuário a comprar um programa antivírus falso.

Poucos dias depois do lançamento do Windows 8, começou a circular na internet, segundo a *Trend Micro*, o primeiro antivírus falso (scareware) para o novo sistema operacional. O programa, logo depois de fazer uma falsa varredura dos arquivos, incentivava os usuários a adquirir o produto, que alegava ser o primeiro antivírus desenvolvido especificamente para Windows 8.[42]

Outra observação importante é saber que não é aconselhado ter mais de um antivírus instalado no computador porque isso faz com que o desempenho da máquina seja afetado, além de gerar uma incompatibilidade entre os aplicativos, ou seja, é um atrapalhando o outro.

Os antivírus atuais já incorporam detecção de spyware, mas

existem programas específicos para detectar e remover spyware e adwares, os chamados anti-spywares. O que difere um anti-spyware de um antivírus é a classe de programas que eles removem, pois nem sempre é fácil determinar o que é um adware e um spyware. Portanto, nada impede o usuário querer ter um antivírus e um anti-spyware ao mesmo tempo.

Firewall

A maioria dos sistemas operacionais possui um firewall, que é fundamental para a segurança do computador. Quando alguém tenta se conectar ao seu equipamento, essa tentativa é chamada "pedida não solicitada". Nessa hora, entra em ação o firewall, cuja função consiste em regular (monitorar, filtrar) o tráfego de dados entre redes distintas, impedindo a transmissão ou recepção de acessos nocivos ou não autorizados na rede, formando assim uma forte barreira que impede que invasores roubem seus dados e informações pessoais.

Instrua todas as pessoas que usam o seu computador para que elas façam bom uso dele e não baixem arquivos desconhecidos.

Navegue com segurança

Os atacantes procuram por vulnerabilidades, e ter um computador bem configurado diminuirá as possibilidades de ataque. Depois disso é o próprio usuário que precisará tomar certos cuidados para utilizá-lo com segurança. Conheça algumas dicas: ➢

- Ao navegar na internet nunca clique em links que apontem para sites desconhecidos sem antes conferir o seu destino. Para isso, clique com o botão direito do mouse sobre o link e confira suas propriedades.

Alguns serviços exigem nome do usuário e senha para fazer o ***login*** (registro de entrada). Após utilizar esses serviços nunca se esqueça de fazer o ***logout*** (sair, desconectar) para sair do site. Pode parecer óbvio, mas muita gente realiza este procedimento simplesmente fechando a janela do navegador ou entrando em outro endereço a partir dali.

Antes de se cadastrar em sites, faça uma pesquisa para verificar se aquele endereço tem registro de alguma atividade ilegal. Se um site pede o número do seu cartão de crédito sem que você tenha intenção de comprar, as chances de se tratar de uma fraude são grandes. Além disso, suas informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone, por exemplo.

É importante usar navegadores diferentes para tarefas distintas. Use um navegador para sites em geral, fóruns, notícias, blogs. Quando usar sites de banco ou e-mail, use outro navegador. Assim, se um navegador for infectado por um vírus específico de browsers, o outro não será afetado.

Crie senhas difíceis e mude-as periodicamente

Senhas são intransferíveis, particulares e sigilosas. Suas senhas são o principal meio de proteção contra o acesso não permitido ao computador.

Um estudo divulgado pela empresa de segurança SplashData criou uma lista das senhas mais fracas utilizadas pelos usuários de computadores. A mais usada é

a própria palavra *password* (senha em inglês), seguida por 123456 e 12345678. Logo depois aparecem senhas como abc123 e qwerty (a sequência das seis primeiras teclas alfabéticas de qualquer teclado). Na lista ainda é possível encontrar as sequências numéricas 111111, 123123 e o nome Jesus.[43]

É necessário senhas fortes para todas as contas no seu computador. Siga essas dicas: ➢

Evite as muito simples, como 12345, ou nomes de parentes, datas de aniversário *etc.*

Não use senhas de combinações que tenham menos de seis caracteres.

Crie senhas longas, forme uma frase que faça sentido para você.

Insira pontos, vírgulas, arrobas e números, para tornar a sua frase indecifrável. Use também letras maiúsculas misturadas com minúsculas.

Fuja de palavras de dicionários (mesmo em outros idiomas).

Tenha uma senha diferente para cada serviço.

Ignore perguntas de segurança. Há um número limitado de respostas para perguntas como "qual sua cor favorita?" Atacantes podem usar essas informações para ter controle de suas contas e mudar suas senhas.

Troque suas senhas periodicamente; fazendo isso, você diminui muito as chances de ser atacado. Lembre-se: se alguém conseguir descobrir a senha do seu e-mail, por exemplo, poderá acessar as suas mensagens sem que você saiba e trocar sua senha para impedir que você tenha acesso.

Cuidado ao fazer compras pela internet

Muitas são as vantagens em fazer compras pela internet. Com alguns cliques você pode comparar preços sem ter que ir de loja em loja, comprar passagens áreas, agendar hotéis, comprar roupas e até itens de supermercado, tudo isso sete dias por semana, 24 horas por dia, sem enfrentar filas.

Este é um mercado que só cresce no país. Em 2011, mais de 24 milhões de brasileiros fizeram compras on-line. Em 2012, o setor faturou mais de R$ 22,5 bilhões, um aumento de 20% sobre o ano anterior. Mas este mercado não só atrai novos consumidores como também golpistas; portanto, é preciso ter alguns cuidados para fazer suas compras com segurança.

Tenha cuidado especial ao comprar itens populares, como MP3 players, câmeras digitais, smartphones, TVs LCD, notebooks, tablets e navegadores GPS. Itens mais desejados são mais explorados, o que pode tornar a compra mais arriscada.



Risco: Não receber produto nenhum. ***Dica:*** Desconfie de produtos muito abaixo do preço de mercado.

Pesquise sobre o site em que você pretende comprar e veja o que as outras pessoas estão dizendo sobre ele.

Risco: Informar dados pessoais, de contas correntes e números de cartões de créditos a estelionatários. ***Dica:*** Saiba com quem você está negociando: qualquer um pode anunciar a venda de um produto na internet. Antes de comprar verifique os dados e monitore as avaliações do vendedor. Havendo qualquer ocorrência indicando que houve pagamento sem envio do produto, desista de sua compra. Evite também o vendedor que opere somente usando telefone celular. Não envie suas informações financeiras por e-mail. Se fizer uma compra e precisar enviar dados pessoais, procure indicadores de que o site é seguro, como um ícone de cadeado na barra de status do navegador ou uma URL que comece com "https:" (o "s" significa "seguro").

Risco: Comprar um produto e receber outro diferente do que se comprou e depois não conseguir trocar ou receber o pagamento de volta. ***Dica:*** Verifique os termos da negociação, a localização física, a entrega, formas de pagamentos, garantia do produto e condições de troca. Caso você o devolva, descubra quem pagará os custos de remessa e quando você receberá seu pedido.

Leia as políticas de privacidade e, caso não haja uma, desconsidere fazer compras neste site. Observe também quais informações pessoais os operadores do site coletam, o porquê e como eles as usarão.

Imprima e guarde registros de suas transações on-line, inclusive descrição e preço do produto, recibos e cópias de

todos os e-mails enviados ou recebidos do vendedor.

Se o produto não foi entregue e o fornecedor não retorna o contato, tente o estorno ou a devolução do valor pago com a empresa do cartão de crédito ou intermediária do pagamento.

Não deixe de registrar a queixa no Procon da sua cidade sobre a loja virtual.

Proteja-se dos golpes

Segundo dados divulgados pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), no segundo trimestre de 2012 houve um aumento de 89% dos golpes na internet que utilizam páginas falsas de sites de comércio eletrônico em relação ao primeiro trimestre do mesmo ano.[44]

É muito simples clonar a aparência de um site ou até mesmo criar uma URL parecida com a original que leve o usuário a acreditar que está em uma loja de confiança (ataque conhecido como phishing).

Desconfie de e-mails com promoções que indicam um link, mesmo que aparentemente eles sejam de uma loja onde você realmente é cadastrado. Esses e-mails, embora utilizem logotipos e aparências iguais aos originais, remetem o usuário para uma armadilha. Na dúvida, prefira digitar o endereço a acessá-lo através de um link, pois o golpe pode estar camuflado.

Faça uma consulta sobre a loja no site **Reclame Aqui** (www.reclameaqui.com.br) ou no **Confiometro** (www.confiometro.com.br) para saber se existem reclamações contra ela. Uma busca rápida pode revelar resultados sobre atrasos na entrega, problemas com trocas, produtos danificados *etc.*

Pesquise também nos sites de busca. Veja o que aparece sobre a loja quando você digita seu nome no Google, por exemplo. Você pode encontrar tanto reclamações quanto

boas indicações.

Realize operações bancárias com segurança

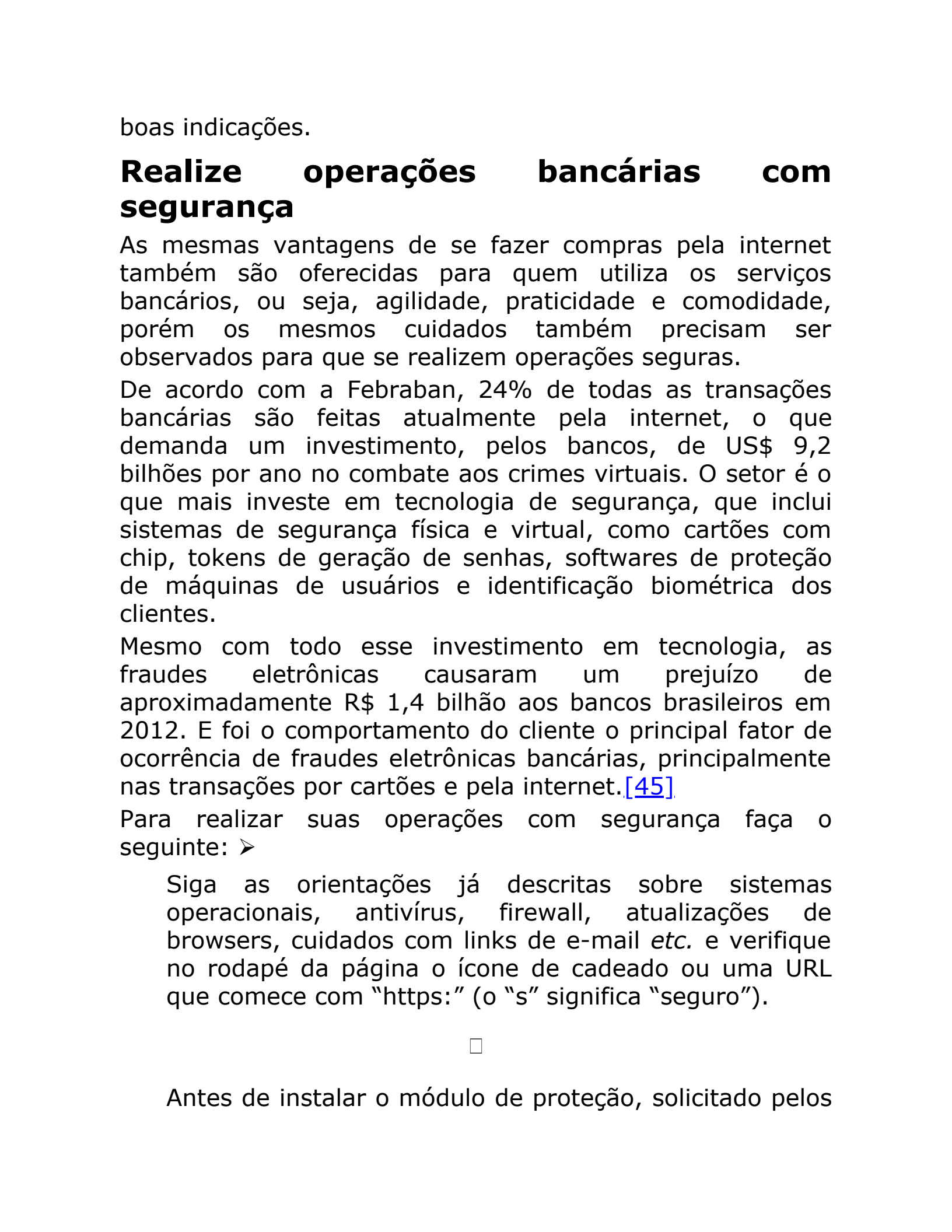
As mesmas vantagens de se fazer compras pela internet também são oferecidas para quem utiliza os serviços bancários, ou seja, agilidade, praticidade e comodidade, porém os mesmos cuidados também precisam ser observados para que se realizem operações seguras.

De acordo com a Febraban, 24% de todas as transações bancárias são feitas atualmente pela internet, o que demanda um investimento, pelos bancos, de US$ 9,2 bilhões por ano no combate aos crimes virtuais. O setor é o que mais investe em tecnologia de segurança, que inclui sistemas de segurança física e virtual, como cartões com chip, tokens de geração de senhas, softwares de proteção de máquinas de usuários e identificação biométrica dos clientes.

Mesmo com todo esse investimento em tecnologia, as fraudes eletrônicas causaram um prejuízo de aproximadamente R$ 1,4 bilhão aos bancos brasileiros em 2012. E foi o comportamento do cliente o principal fator de ocorrência de fraudes eletrônicas bancárias, principalmente nas transações por cartões e pela internet.[45]

Para realizar suas operações com segurança faça o seguinte: ➢

Siga as orientações já descritas sobre sistemas operacionais, antivírus, firewall, atualizações de browsers, cuidados com links de e-mail *etc.* e verifique no rodapé da página o ícone de cadeado ou uma URL que comece com “https:” (o “s” significa “seguro”).



Antes de instalar o módulo de proteção, solicitado pelos

bancos, certifique-se de que o autor é realmente a instituição.

Nunca utilize computadores públicos, nem equipamento que não conheça (lan houses e cafés) ou redes wi-fi públicas.

Procure sempre digitar o endereço manualmente na barra do navegador, nunca clique em links recebidos via e-mail, mensagens, SMS, redes sociais *etc.*

Na página do banco, fique atento para o verdadeiro destino dos links em que você clica: posicione o cursor do mouse sobre ele e confirme, na parte inferior do navegador, para onde ele vai levar você.

Quando acessar a página do banco, digite a senha errada na primeira vez. Se o erro for indicado, você está no lugar certo. Como sites falsos não têm como conferir a informação, pois querem apenas roubar sua senha, eles não vão acusar nenhum erro.

Utilize endereço terminado em "**b.br**". Os principais bancos do país já usam o domínio "**b.br**" que amplia a segurança das operações bancárias on-line, adicionando mais criptografia e tornando os sites mais fidedignos na identificação ➢

Quando for utilizar o teclado virtual, minimize a página. Se o teclado virtual for minimizado também, está correto. Se ele permanecer na tela sem minimizar, é falso! Não tecle nada.

Troque periodicamente a senha utilizada para acessar seu banco.

Quando terminar tudo o que você fez no banco, lembre-se de clicar em ***Sair*** para encerrar sua sessão.

Acompanhe sua conta corrente. Caso constate qualquer crédito ou débito irregular, entre imediatamente em contato com a central de relacionamento do seu banco.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) lançou uma Cartilha de Segurança dedicada aos cuidados com o internet banking.

O manual traz orientações – como os riscos de divulgar informações bancárias por e-mail e telefone, cuidados com mensagens atribuídas a bancos e que podem conter códigos maliciosos ou induzir acesso a páginas falsas – para que o usuário possa utilizar sites bancários com mais segurança.

A cartilha na íntegra está disponível em:

http://www.crimespelainternet.com.br/cert-br-lanca-manual-online-sobre-seguranca-em-internet-banking/

http://cartilha.cert.br/fasciculos/

Cuidado com downloads

Cuidado ao baixar arquivos ou música, pois muitos

malwares se passam por músicas, vídeos, fotos, aplicativos e outros para enganar o usuário. Por isso, toda vez que concluir um download, não execute o arquivo logo após o término. Faça sempre uma varredura com o programa antivírus e certifique-se de que o arquivo está limpo.

Se você tem dúvida se o antivírus está ou não cumprindo com a função dele e recebeu ou deseja enviar um arquivo específico, você pode utilizar os antivírus on-line. Uma dica é o **verificador de malware Jotti** (http://virusscan.jotti.org/pt-br).

Estando na página, selecione o arquivo e clique em Enviar. Pronto! Você terá uma varredura on-line de mais de vinte antivírus, dando assim uma probabilidade muito maior de proteção para a sua máquina.

Outro inconveniente são as barras de ferramentas dos mais diversos tipos que se instalam ao obter programas gratuitos. Para evitar que o seu navegador fique recheado dessas barras é preciso acompanhar todas as etapas de instalação, evitando passar muito rapidamente, pois durante este processo o programa pode deixar de maneira pré-marcada a ativação conjunta de outros programas. Não aceite nada além da instalação de seu software (basta geralmente controlar as opções que devem ser desmarcadas durante a instalação e ler bem todas as Condições Gerais de Utilização).

Cuidado com e-mails

O e-mail é uma das principais ferramentas utilizadas pelos atacantes para tentar aplicar golpes e distribuir malwares. Só nos seis primeiros meses de 2012 houve um aumento de 56% de ataques por e-mail em relação a todo o ano de 2011. A engenharia social é a prática mais utilizada pelos criminosos, que usam termos de notificações e nomes de instituições financeiras para atrair as vítimas. Palavras como “pagamento”, “alerta” e “fatura” são os mais

populares em e-mails maliciosos.[46]

Com o intuito de conscientizar a comunidade sobre os principais golpes que estão em circulação, o CAIS – Centro de Atendimento a Incidentes de Segurança (http://www.rnp.br/cais/fraudes.php) – mantém em seu site um catálogo de fraudes ordenadas de acordo com a data de distribuição e disponibilizadas para consulta.

Veja algumas técnicas de persuasão e pense se algum dia você já não foi vítima de algum desses exemplos.

MEDO: — Pendências no Serasa – Uma mensagem é enviada ao usuário informando que existem pagamentos em atraso para o seu CPF, mas ao acessar o link disponível no corpo da mensagem é indicado o download de um software malicioso.

— Cheque Protestado – O usuário recebe um e-mail afirmando que um cheque foi protestado e que a cópia está em anexo, mas ao clicar no link é indicado o download.

— Intimação – Uma mensagem é enviada informando que o usuário está intimado a comparecer em uma audiência, disponibilizando um link para acesso do documento de intimação. Mas ao acessá-lo é realizado o download do malware.

— Título de eleitor cancelado – A fraude se passa com um e-mail que afirma que o usuário teve seu título de eleitor cancelado temporariamente, mas ao clicar no link inicia-se o download do malware.

CURIOSIDADE: — Fotos em anexo – A falsa mensagem tenta se passar por uma conversa entre amigos sobre supostas fotos. O link da mensagem realiza o download de um arquivo malicioso que tem o objetivo de roubar dados do usuário e/ou danificar o seu computador.

— Vídeo íntimo de artista famosa – A fraude contém um link para o suposto vídeo de alguma artista famosa, mas na verdade o link instala um trojan.

— Fotos da traição – A mensagem, que teria sido enviada por um amigo da vítima, contém um link para uma suposta foto com imagens de uma traição. Mais um link para download contendo um arquivo malicioso.

— Autorização para foto no Facebook – Comunicado falso do Facebook informando que alguém deseja utilizar uma foto da vítima. O link para a suposta foto leva ao download do arquivo malicioso.

GANÂNCIA: — Loterias – O usuário recebe uma mensagem afirmando que foi contemplado com um prêmio de loteria, mas para reclamar o prêmio necessita enviar dados pessoais a uma conta de e-mail suspeita.

— Sorteado para ganhar um novo iPad – Aqui o fraudador afirma que o usuário foi contemplado com um prêmio. Ao clicar no link disponível, o usuário é direcionado a uma página onde preenche todos os seus dados sem nenhum resultado ao final.

— Premiação de 1.500 euros – Nesse contato o fraudador utiliza técnicas de engenharia social na tentativa de aquisição de dados do usuário para que tenha acesso ao benefício.

SIMPATIA: — Cartão Virtual VoxCards – A falsa mensagem informa o recebimento de um cartão virtual do site em questão. O link da mensagem realiza o download de um arquivo malicioso que pode furtar dados e/ou danificar o computador do usuário.

— Cartão de Natal – A fraude passa pelo envio de um cartão de Natal. O link leva ao arquivo malicioso, um trojan.

Essas são algumas das **4628** (*em 08/07/2013*) fraudes

cadastradas no **CAIS.** Sempre que você receber um e-mail e não tiver certeza de que se trata de uma fraude, acesse **http://www.rnp.br/cais/fraudes.php** e verifique o catálogo.

Em todos esses exemplos apresentados, os atacantes procuram induzir o usuário a realizar alguma tarefa, e o sucesso do ataque depende **única** e **exclusivamente** da decisão do usuário em fornecer informações sensíveis ou executar programas.

Algumas características como remetentes estranhos, falta de contatos e erros de português podem mostrar que a mensagem é falsa.

Desconfie mesmo se o e-mail vier de alguém que você conhece. É muito comum abrir uma mensagem e confiar em seu conteúdo quando se vê que a mensagem partiu de um conhecido. Mas não se esqueça de que conhecidos também estão sujeitos a ter suas máquinas infectadas e que muitos malwares se autoenviam para a lista inteira de contatos.

Tenha muita atenção com arquivos com extensões .zip, pois são os mais aproveitados pelos criminosos. Dentro destes arquivos compactados existem outros de formato executável (.EXE) ou de documento (.PDF), que aproveitam de brechas do sistema operacional para contaminar os computadores e enviar dados pessoais aos criminosos.

Siga as orientações descritas sobre senhas para evitar problemas com o uso indevido.

Ter um antivírus instalado não garante a sua segurança, até porque não existe antivírus que identifique 100% dos malwares existentes. Um malware recém-criado, por exemplo, pode não estar contido no mecanismo de identificação do seu antivírus.

Quando receber algum e-mail duvidoso encaminhe para **phishing@cais.rnp.br.** Envie com uma cópia do e-mail original e também comunique à instituição que está sendo

utilizada no golpe.

Um visitante do meu blog www.crimespelainternet.com.br, sabendo do perigo que corria, mandou a seguinte mensagem: "Recebi um e-mail do DPF,CTI Brasília-DF,dizendo para comparecer em uma audiência relativa ao procedimento investigatório 363.234/2013,em epígrafe,em tramitação nesta regional. Tem um anexo (que não abre). Estou desconfiado ser um vírus,pois nunca tive problemas com nenhum órgão federal. Por favor vocês podem me dar um retorno para saber a autenticidade deste e-mail? Grato desde já. Moro em Porto Alegre-RS"

Perceba que esta mensagem contém todas as características de um e-mail fraudulento – neste caso orientei o meu visitante a enviar o conteúdo do e-mail para o **CAIS**.

Cuidado com salas de bate-papo (chat)

Desde que a internet começou a ganhar popularidade, as salas de bate-papo viraram atração para quem quer criar novas amizades ou até mesmo "matar" o tempo ocioso. O grande chamativo desse serviço é a possibilidade de preservar o anonimato, mas o anonimato pode ser um tanto quanto perigoso, pois você não sabe realmente quem está do outro lado.

Nas salas de bate-papo, o golpista vai ganhando a confiança da futura vítima através da conversa. Aos poucos vai convencendo a pessoa a fornecer seus dados, como telefone, endereço residencial *etc.*

Os golpes ocorrem principalmente com crianças e adolescentes, mas muitos adultos também são vitimados. Veja como não cair nas armadilhas: ➢

- Jamais divulgue informações confidenciais, nem fotografias ou vídeos pessoais.



Evite marcar encontro com alguém que conheceu pela internet, mas, se resolver marcar, prefira lugares públicos, movimentados e conhecidos. Evite locais desertos. Diga a parentes ou amigos onde está indo.



É fácil mentir e fingir ser outra pessoa na internet. As crianças, em especial, precisam saber que um novo "amigo" pode ser um adulto mal-intencionado.



Tempo de conversa não garante a confiança nem a veracidade das informações, tome cuidado. Veja este caso concreto: uma jovem de Campo Grande que mantinha contato com uma "amiga virtual" de Salvador foi encontrada quase sem vida em 16 de outubro de 2012, depois de ter viajado para se encontrar com a suposta amiga. A mãe da vítima diz que elas tinham contato há mais de três anos e inclusive já tinha visto as jovens conversando via videoconferência e que a outra se apresentou sendo evangélica, separada, com filhos e que morava nos fundos da casa da mãe. Depois de uma denúncia, a polícia encontrou a jovem jogada em uma ribanceira, toda machucada com indícios de violência sexual.[47]

Cuidado ao fazer cadastros

Não coloque seu e-mail em sites desconhecidos. O risco é que suas informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone, ou ainda ser inserido em listas de spam.

Se você realmente necessita utilizar o serviço disponibilizado por algum site e este exige que você coloque um e-mail válido para cadastro, utilize um e-mail

descartável.

Um e-mail descartável permite que você faça cadastros em sites sem precisar revelar seu e-mail verdadeiro, mantendo sua privacidade.

Existem diversas opções de e-mail temporário. Recomendo alguns que testei: ➢

Emailtemporario.com.br

10 Minute Mail

Mailinator

Para quem tem Yahoo, esta opção já está disponível há bastante tempo lá nas opções: e-mails descartáveis.

Tenha bom senso

Como você deve ter notado, o bom senso é a melhor maneira de proteção. É importante lembrar que cada informação nova divulgada é um dado novo que o criminoso poderá usar.

Capítulo 7. Como Agir em Caso de Crimes Virtuais

É possível punir quem comete crimes virtuais da mesma forma que se pune quem pratica qualquer outro tipo de crime. Para se chegar ao autor de um crime virtual é muito importante que a vítima preserve todas as evidências do acontecido.

Colete e preserve as evidências

Imprima e salve arquivos, e-mails, telas, páginas de internet, tudo que possa comprovar o crime. No mundo virtual as evidências podem desaparecer de uma hora para outra.

Preserve as provas em algum tipo de mídia protegida contra alteração, como um CD-R ou DVD-R.

Todas as provas ajudam como fonte de informação para a investigação da polícia.

Atribua validade jurídica às provas obtidas

Procure um cartório para registrar uma **Ata Notarial** das evidências, pois este documento pode ser usado como prova na justiça.

O que é uma ata notarial?

Ata notarial é um instrumento público por meio do qual o

tabelião ou preposto, a pedido da pessoa interessada, constata fielmente os fatos, as coisas, comprova o seu estado, a sua existência e a de pessoas ou situações que lhe constem, com seus próprios sentidos, portando por fé que tudo aquilo presenciado e relatado representa a verdade plena.

Este ato é redigido e lavrado por um tabelião de notas em livro próprio – podendo evidentemente ser obtida em qualquer Tabelionato de Notas ou Registro Civil cumulado com Notas.

Para que serve?

A ata notarial serve para pré-constituir prova dos fatos. Muitas vezes não temos como provar uma situação potencialmente perigosa ou danosa. O tabelião é, portanto, uma testemunha oficial cujo ato vai desencadear a fé pública e fazer prova plena perante qualquer juiz ou tribunal.

Como utilizar nos casos de internet?

A ata notarial comprova inúmeros fatos, dentre eles: ➢

Prova o conteúdo divulgado em páginas da internet.

Prova o conteúdo da mensagem e o IP emissor.

Textos que contenham calúnia, injúria e/ou difamação.

Uso indevido de imagens, textos [livros], filmes, logotipos, marcas, nomes empresariais, músicas e infrações ao direito autoral e intelectual.

- Concorrência desleal.
- Consulta em páginas de busca.
- Comunidades on-line que conectam pessoas através de uma rede de amigos.
- Consulta do CPF no sítio da receita federal *etc.*

Nas verificações (tanto no meio físico, quanto no eletrônico), o tabelião constata os fatos, relatando fielmente tudo aquilo que presenciou. A ata notarial tem força certificante para comprovar a integridade e a veracidade destes documentos, atribuir autenticidade, fixar a data, hora e existência do arquivo eletrônico.

Essas atas notariais – utilizadas em atos processuais ou extrajudiciais – se revelam meio seguro e adequado para se constatar um sítio eletrônico. Isso porque esse meio é suficiente para autenticar o conteúdo de um endereço eletrônico (www) em determinado momento e preservá-lo para o futuro com plena segurança (sob manto da fé pública).

Lembrando que os livros e arquivos dos tabeliães não têm prazo de validade e serão mantidos sempre em local seguro e apropriado.

Preciso de advogado?

Não, você pode solicitar diretamente ao tabelião. Se você tiver um advogado, consulte-o e decida com ele sobre a conveniência de fazer uma ata notarial.

Faça um boletim de ocorrência

Procure a Delegacia de Polícia do seu bairro para registrar a ocorrência. Em alguns estados existem **delegacias especializadas em crimes virtuais**. Veja se o seu estado já possui este serviço no Capítulo **8** deste livro.

Como registrar ocorrência dos crimes contra a honra e ameaça

Crimes contra o patrimônio, como clonagem de cartões, estelionato e desvio de dinheiro, são as ocorrências criminais mais investigadas pelas diversas delegacias especializadas em crimes virtuais espalhadas pelo país. Crimes como calúnia, injúria e difamação, envolvendo nome e imagem de terceiros, aparecem logo em seguida. De janeiro a setembro de 2012, em uma análise dos 1.093 registros computados pela Delegacia de Repressão aos Crimes de Informática (DRCI) do Rio de Janeiro, quase 49% correspondem a casos de injúria, difamação e calúnia. Os chamados crimes contra a honra.[48]

Se você foi vítima de crimes contra a honra ou de ameaça, de posse das provas coletadas, procure a delegacia mais próxima de sua residência e registre a ocorrência. Você também pode ir a uma delegacia especializada em crimes virtuais.

Em São Paulo, a Polícia Civil disponibiliza em seu site (http://www2.policiacivil.sp.gov.br) a **Delegacia Eletrônica de Polícia Civil do Estado de São Paulo**. Seu papel é proporcionar ao cidadão a facilidade de registrar um boletim de ocorrência sem sair de casa. Entre os serviços estão: crimes contra a honra como injúria, calúnia ou difamação e ameaça e insultos verbais de natureza homofóbica ou racista.

O valor do boletim eletrônico de ocorrência é o mesmo do boletim de ocorrência registrado em uma delegacia, pois trata-se de um documento oficial emitido pela Polícia Civil

do Estado de São Paulo e assinado por uma autoridade policial.

Depois que a vítima transmite as informações on-line, um policial entra em contato, confirma alguns dados e registra o **BEO** (Boletim Eletrônico de Ocorrência). Feito isto, a denúncia é enviada para as Delegacias de Polícia das áreas ou municípios onde ocorreram os fatos.

Logo após esse registro, a vítima precisará ir ao distrito policial do seu bairro em até seis meses para fazer a representação da ocorrência. Como os crimes são classificados pela lei como de "natureza privada", é necessário que a pessoa atingida solicite de forma presencial à polícia que dê continuidade às investigações Procure na página oficial da Polícia Civil do seu estado se existe esta opção; se não existir, vá pessoalmente a uma delegacia e registre a ocorrência. O que não pode é deixar de denunciar.

Vítimas que tiveram fotos ou vídeos íntimos divulgados têm seus casos analisados através do **artigo de crimes contra a honra**: como difamação (o ato de disponibilizar imagens íntimas de uma pessoa) ou injúria (ofensas realizadas em meio digital). Mesmo que a pessoa tenha admitido que seu parceiro tirasse as fotos, não é permitido que tais imagens sejam repassadas. Portanto, quem teve a integridade manchada na internet possui total respaldo judicial.

Como registrar ocorrência de ameaças por e-mails

No caso de ameaças ou crimes contra a honra através de e-mail é preciso, além de preservar o conteúdo da mensagem, identificar o cabeçalho do e-mail e imprimi-lo como prova.

Através do cabeçalho do e-mail é possível saber os dados do remetente e destinatário, como **o endereço IP de origem, data e hora da transmissão e a referência à hora GMT**, dentre outras informações relevantes.

É comum um cabeçalho possuir várias linhas que começam com a palavra *received*. A palavra mostra por quantos servidores a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o **último** *received* (os "received" estão em ordem decrescente, ou seja, o primeiro "received" de baixo para cima mostrará a máquina mais recente por onde sua mensagem passou). Ele irá indicar o computador do remetente.

Veja como ler o cabeçalho dos seus e-mails nos webmails e gerenciadores de e-mails mais usados.

Gmail ➢

Acesse a sua conta do Gmail.

Abra a mensagem com os cabeçalhos que você deseja visualizar.

Clique na seta para baixo próxima a **Responder**, no canto superior direito da mensagem.

Selecione **Mostrar original**.

Os cabeçalhos completos serão exibidos em uma nova janela.

Hotmail ➢

Faça login na sua conta do Hotmail.

Selecione **Caixa de Entrada** no menu à esquerda.

□

Clique com o botão direito do mouse na mensagem cujos cabeçalhos você deseja visualizar e selecione **Exibir código-fonte da mensagem**.

Os cabeçalhos completos serão exibidos em uma nova janela.

Yahoo!

□

Faça login na sua conta de e-mail do Yahoo!

□

Selecione a mensagem cujos cabeçalhos você deseja visualizar.

□

Clique no menu suspenso **Ações** e selecione **Exibir cabeçalho completo**.

Os cabeçalhos completos serão exibidos em uma nova janela.

AOL

□

Faça login na sua conta da AOL.

□

Abra a mensagem cujos cabeçalhos você deseja visualizar.

□

No menu “Ação”, selecione **Exibir origem da mensagem**.

Webmail do Excite ➢

Faça login na sua conta do Excite.

Abra a mensagem cujos cabeçalhos você deseja visualizar.

Clique no ícone **View Full Headers** (Visualizar cabeçalhos completos) localizado à direita da linha “From:” (“De:”).

Gerenciadores de e-mails locais *Apple Mail* ➢

Abra o Apple Mail.

Clique na mensagem cujos cabeçalhos você deseja visualizar.

Vá para o menu **Visualizar**.

Selecione **Mensagem** e, em seguida, **Cabeçalhos longos.**

Mozilla ➢

Abra o Mozilla.

Abra a mensagem com os cabeçalhos que você deseja visualizar.

Clique no menu **View** (Exibir) e selecione **Message Source** (Origem da mensagem).

Os cabeçalhos completos serão exibidos em uma nova janela.

Outlook ➢

Abra o Outlook.

Clique na mensagem cujos cabeçalhos você deseja visualizar.

Clique com o botão direito do mouse e em seguida **Exibir origem da mensagem.**

Em versões anteriores do Outlook:

1. Abra o Outlook.
2. Abra a mensagem com os cabeçalhos que você deseja visualizar.
3. Clique no menu **Exibir** e selecione **Opções...**.

Os cabeçalhos completos serão exibidos em uma nova janela.

Outlook Express ➢

Abra o Outlook Express.

Da sua caixa de entrada, localize a mensagem com os cabeçalhos que deseja visualizar.

Clique com o botão direito do mouse na mensagem e selecione **Propriedades**.

Abra a guia **Detalhes** na caixa de diálogo.

Os cabeçalhos completos serão exibidos na caixa de diálogo.

Opera ➢

Abra o Opera.

Clique na mensagem com os cabeçalhos que deseja visualizar para que sejam exibidos na janela abaixo da caixa de entrada.

Clique em **Exibir todos os cabeçalhos** do lado oposto do campo **Para**.

Os cabeçalhos completos serão exibidos na janela a seguir.

IncrediMail ➢

Abra o IncrediMail.

Usando sua caixa de entrada, localize a mensagem com os cabeçalhos que deseja visualizar.

Clique com o botão direito do mouse na mensagem e selecione **Propriedades**.



Abra a guia **Detalhes** na caixa de diálogo.

Os cabeçalhos completos serão exibidos na caixa de diálogo.

IG Mail ➢

Abra o IG Mail.



Abra a mensagem com os cabeçalhos que você deseja visualizar.



Clique em "**Mais**" representado por uma seta para baixo que fica no canto superior direito da mensagem colado com o botão responder. No menu suspenso que se abrir clique em "**Mostrar origina**l".

Os cabeçalhos completos serão exibidos na caixa de diálogo.

Os cabeçalhos dos e-mails indicam de onde uma mensagem é enviada e registram o caminho específico que ela segue ao passar por cada servidor de e-mail.

Para ler um cabeçalho, siga o caminho de uma mensagem cronologicamente, lendo a partir da parte inferior do cabeçalho, e trabalhando de baixo para cima.

Este é um exemplo de um cabeçalho de mensagem para um e-mail enviado de moisescassanti@uol.com.br para moisescassanti@hotmail.com**.**

Received: from uol.com.br (a4-weasel19.host.intranet [10.131.133.79]) by a4-shark3.host.intranet (Postfix) with ESMTP id 8BDC33800088

for <moisescassanti@hotmail.com>; Tue, 20 Nov 2012 20:09:41 -0200 (BRST) Date: Tue, 20 Nov 2012 20:09:41 -0200

From: moisescassanti <moisescassanti@uol.com.br> To: "moisescassanti@hotmail.com" <moisescassanti@hotmail.com> Message-Id: <50abffa588fca_506956599384de@a4-weasel19.tmail> Subject:

Mime-Version: 1.0

Content-Type: text/html; charset=utf-8

X-SenderIP: 187.57.197.235

X-SIG5: f94123a202a7751280d471cb00e5a8b2

Return-Path: moisescassanti@uol.com.br X-OriginalArrivalTime: 20 Nov 2012 22:09:43.0807 (UTC) FILETIME=[BEAD50F0:01CDC76B]

Esta mensagem é um teste para mostrar como ler cabeçalho completo de e-mails
 <h2>Â </h2>

Passamos para a análise: ** **Esta mensagem é um teste para mostrar como ler cabeçalho completo de e-mails
 <h2>Â <h2> ** ** Este é o assunto do e-mail.

X-OriginalArrivalTime: 20 Nov 2012 22:09:43.0807 (**UTC**) Este é um carimbo de data e hora colocado na mensagem quando ela passa pela primeira vez por um servidor executando o Microsoft Exchange.

Return-Path: moisescassanti@uol.com.br Esta entrada especifica como chegar ao remetente da mensagem.

X-SenderIP: 187.57.197.235
Este é o número do IP do remetente.

Content-Type: text/html; charset=utf-8
Este é um cabeçalho MIME adicional. Ele informa aos programas de e-mail compatíveis com MIME o tipo de conteúdo esperado na mensagem.

Mime-Version: 1.0
Este parâmetro especifica a versão do protocolo MIME que foi usada pelo remetente.

Message-Id: <50abffa588fca_506956599384de@a4-weasel19.tmail> Este número foi atribuído a essa mensagem (pelo UOL) para fins de identificação. Esta ID estará sempre associada à mensagem.

To: "moisescassanti@hotmail.com" moisescassanti@hotmail.com Esta é a pessoa para a qual a mensagem está endereçada.

From: moisescassanti <moisescassanti@uol.com.br> Essa mensagem foi enviada por moisescassanti a partir do endereço de e-mail moisescassanti@uol.com.br.

Date: Tue, 20 Nov 2012 20:09:41 -0200
Indica a data e a hora em que a mensagem de e-mail foi

enviada, com base no relógio do computador do remetente.

Received: from uol.com.br (a4-weasel19.host.intranet [10.131.133.79]) by a4-shark3.host.intranet (Postfix) with ESMTP id 8BDC33800088

for <moisescassanti@hotmail.com>; Tue, 20 Nov 2012 20:09:41 -0200 (BRST) Date: Tue, 20 Nov 2012 20:09:41 -0200

Esta informação diz que a transferência da mensagem ocorreu na terça-feira, 20 de novembro de 2012, às 20:09:41 Hora Oficial do Pacífico (2 horas atrás da Hora de Greenwich); por isso o "–0200").

Obtida a informação do **endereço IP, a data da comunicação, e o horário indicando o fuso horário utilizado – GMT ou UTC** –, com uma ordem judicial é só requisitar ao provedor que diga a quem pertence o **IP** solicitado.

Caso não seja possível identificar o **número IP, data, hora, GMT ou UTC,** mas conste o endereço eletrônico do remetente, a autoridade policial ou o membro do Ministério Público pode requerer judicialmente a quebra do sigilo de dados telemáticos para que o provedor do e-mail forneça o endereço IP da máquina que autenticou esta conta, na data e horário do e-mail remetido.

Não encaminhe o e-mail com o conteúdo ofensivo para ninguém, nem para a polícia. Fazendo isso você simplesmente está destruindo evidências sobrescrevendo o header (cabeçalho) da mensagem original por tags do seu provedor de e-mail SMTP.

É bom lembrar que, em caso de ofensas ou calúnias enviadas por e-mail, não existe crime se somente a **pessoa alvo das difamações** recebeu a mensagem. Já e-mails enviados a terceiros ou sites com conteúdo ofensivo configuram crime. De acordo com a legislação atual, os servidores não podem ser responsabilizados criminalmente

pelo conteúdo dos sites que hospedam.

Como fazer denúncia de crimes contra os direitos humanos na internet?

Através da SaferNet

A SaferNet, em parceria com o Ministério Público Federal, mantém a Central Nacional de Denúncias de Crimes Cibernéticos, um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação dos direitos humanos praticado através da internet.

Você poderá denunciar crimes de: **pornografia infantil, racismo, homofobia, xenofobia, apologia e incitação a crimes contra a vida, neonazismo e tráfico de pessoas** através do link: http://www.safernet.org.br/site/denunciar

Em sete anos, a SaferNet Brasil recebeu e processou 3.173.061 denúncias anônimas envolvendo 472.840 URLs distintas escritas em nove idiomas e hospedadas em 52.962 hosts diferentes, conectados à internet através de 28.131 números IPs distintos, atribuídos para noventa países em cinco continentes. As denúncias foram registradas pela população através dos sete hotlines brasileiras que integram a Central Nacional de Denúncias de Crimes Cibernéticos.[49]

O crime que recebe mais denúncias no Brasil é o de pornografia infantil — 38,65% seguido pelo crime de racismo. Na sequência, aparecem apologia ao crime, homofobia, intolerância religiosa e xenofobia. O gráfico a seguir mostra os dados do período de janeiro de 2006 a outubro de 2012.



Através do Ministério Público Federal (MPF)

No site do **MPF** está disponibilizada uma ferramenta, a **Digi Denúncia**, que recentemente foi reformulada para receber denúncias de crimes eletrônicos. Para isso, a vítima deve acessar o link www.prsp.mpf.gov.br/noticias-prsp/aplicativos/digi-denuncia, preencher o formulário on-line e decidir se deseja *manter o anonimato ou não*.

A denúncia será analisada pelo **MPF**, que identificará se há ocorrência de possíveis crimes que atinjam o bem-estar social, como a ***exploração sexual de crianças e adolescentes ou crimes de ódio, como o racismo***.

Apesar desta ferramenta específica para crimes praticados pela internet só estar disponível nos sites do MPF dos estados de **São Paulo, Paraná e Rio Grande do Sul**, é possível registrar uma ocorrência a partir de **qualquer lugar do Brasil**.

Após a denúncia, o **MPF** envia o processo via e-mail para a Procuradoria Geral do Estado de onde se originou a ocorrência. A partir daí, passa a ser acompanhada pelo procurador mais próximo da região.

Veja como proceder: 1.

Acesse a página do Digi Denúncias (www.prsp.mpf.gov.br/noticias-prsp/aplicativos/digi-denuncia).

2. Depois de assinalar que o crime que você presenciou ocorreu através da internet, indique a situação ilegal que você encontrou.
3. Indique qual endereço eletrônico está sendo denunciado.
4. Faça comentários com os detalhes do crime que você quer testemunhar.
5. Aponte se é possível identificar os envolvidos, o estado e a cidade onde o crime aconteceu.
6. Caso seja possível, anexe um ou mais arquivos comprovando o crime.
7. Assinale se deseja permanecer ou não no anonimato.

Como solicitar a remoção do conteúdo ilegal e/ou ofensivo diretamente ao provedor de serviço

Em caso de conteúdo ofensivo ou ilegal, envie uma *Carta Registrada* para o prestador do serviço de conteúdo na internet, que deve preservar todas as provas da materialidade e os indícios de autoria do(s) crime(s).

Deve-se requerer basicamente que o provedor não exclua os registros ou logs que comprovem o crime eletrônico e, principalmente, que retire eventual conteúdo do ar em um prazo, sob pena de ser considerado solidariamente responsável pelo crime eletrônico, pela teoria do favorecimento.

Segue-se um modelo de carta genérico. Para utilizá-lo, deve-se preencher os espaços em branco e inserir os dados pertinentes, alterar os dados de exemplo e substituí-los

pelas informações adequadas ao caso concreto. Observe também se o fundamento legal utilizado neste modelo corresponde ao seu caso. Como cada petição tem uma fundamentação jurídica diferente, você deverá escolher a que mais se adequar com a situação concreta e, se necessário, poderá recorrer a um **advogado** para orientá-lo.

Modelo carta ao provedor denunciando abuso. **(Ministério Público do estado de Minas Gerais)**[50]

Carta modelo

Cidade , (DATA)

Ao Senhor(a) Diretor(a) da (Nome da Empresa prestador de serviço responsável por hospedar o conteúdo ilegal e/ou ofensivo) Prezado Senhor,

(Nome do interessado), (Nacionalidade), (Profissão), (Estado Civil), portador da Carteira de Identidade nº (xxx), inscrito no CPF sob o nº (xxx), residente e domiciliado à Rua (xxx), nº (xxx), Bairro (xxx), Cidade (xxx), Cep. (xxx), no Estado de (xxx), com fundamento na Constituição da República, art. 5º, X, dispositivo este que assegura a todo cidadão o direito à inviolabilidade da "intimidade, vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente da sua violação", vem notificar o que se segue para, ao final, pleitear as providências cabíveis e expressamente indicadas: **DOS FATOS**

(Aqui, narrar em detalhes o fato que enseja a busca pelo direito pretendido) **DO DIREITO**

Como se depreende dos fatos supranarrados, o requerente tem sido vítima do crime de: "Selecione o(s) crime(s) de que julgar ser vítima)".

Crime de Ameaça Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa.

Parágrafo único - Somente se procede mediante representação.

Crime de Falsa Identidade Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Crime de Calúnia Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º - É punível a calúnia contra os mortos.

Exceção da verdade

§ 3º - Admite-se a prova da verdade, salvo: I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível; II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141; III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Crime de Difamação Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Crime de Injúria Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião ou origem: (Incluído pela Lei nº 9.459, de 1997) § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003) Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997) (caso o fato não esteja enquadrado nos crimes acima, consulte o Código Penal Brasileiro) Este(s) crime(s) têm sido perpetrado(s) a partir da utilização indevida da estrutura e dos serviços prestados pela (Colocar aqui o nome da empresa prestadora do serviço) e vem causando danos irreparáveis a minha (honra, e/ou imagem e/ou reputação). Com esta notificação, Vossa Senhoria passa a tomar conhecimento formal destes fatos criminosos perpetrados através do (colocar o nome do serviço), sob sua responsabilidade, e qualquer omissão e/ou negligência na tomada de providências imediatas ensejará a adoção das medidas cabíveis para apuração das responsabilidades cíveis e criminais.

DO PEDIDO

Considerados os fatos narrados, sem prejuízo de outras medidas extrajudiciais e judiciais cabíveis, em conjunto com o que dispõe o direito invocado, pretende o Requerente ver reconhecidas e adotadas pela (indicar aqui o nome da empresa prestadora do serviço) as seguintes providências:

1) Retirada imediata do conteúdo ilegal e/ou ofensivo do (serviço onde o material está hospedado, incluindo o(s) link(s) pertinentes), sob pena de ajuizamento da competente ação de responsabilidade.

2) Preservação de todas as provas e evidências da materialidade do(s) crime(s) e todos os indícios de autoria, incluindo os logs e dados cadastrais e de acesso do(s) suspeito(s), necessários para subsidiar a instrução do inquérito policial criminal e a competente ação judicial.

(Narrar aqui as demais providências pretendidas, caso seja necessário ao seu objetivo) São os termos em que pede imediata providência.

(Local, data e ano).

(Nome e assinatura)

As notificações podem ser enviadas por serviços de e-mail autenticado, como o que é oferecido pela empresa Comprova.com. Link: http://www.comprova.com/

Decisão

A **Terceira Turma do Superior Tribunal de Justiça (STJ)** definiu em 24 horas o prazo para que o provedor de internet retire do ar mensagens postadas em redes sociais e denunciadas como ofensivas, sob pena de responder solidariamente com o autor direto do dano. O prazo deve ser contado a partir da notificação feita pelo usuário ofendido e a retirada tem caráter provisório, até que seja analisada a veracidade da denúncia.

Se o prazo não for cumprido, o provedor irá responder à ação juntamente com o autor da postagem ofensiva. A determinação afeta também serviços de redes sociais como Facebook, Orkut e Twitter.

No capítulo **8** você poderá conferir todos os provedores de serviços e seus respectivos endereços.

Como denunciar estelionato na internet

Os golpes de estelionato na internet são frequentes. Geralmente o estelionatário oferece preços sugestivos para atrair a vítima. Uma dica fundamental na hora da compra é dar preferência ao pagamento via cartão, pois lojas falsas não fazem convênios com cartões de crédito, já que a vítima pode sustar a compra.

No capítulo **Como se proteger de ataques e crimes virtuais** expliquei os riscos e deixei dicas para que o usuário possa fazer compras com mais segurança e tranquilidade.

O procedimento para quem foi vítima de estelionato é o mesmo: imprima e preserve todas as provas e procure a delegacia mais próxima para registrar a ocorrência caso não exista uma especializada.

Como denunciar extorsão pela internet

Vítimas de extorsão via internet devem procurar imediatamente a delegacia mais próxima de sua residência, sendo esta especializada em crimes eletrônicos ou não. É muito comum a vítima aceitar as exigências do chantagista acreditando que resolverá o problema, porém quando o criminoso percebe que a vítima se rendeu às suas chantagens, volta a ameaçar para obter mais vantagem.

Casos concretos

Os casos a seguir foram recebidos no e-mail do meu blog "crimes pela internet".

1. "Conheci uma moça de 28 anos pela internet, tornou-se costume através do MSN nos encontrarmos toda noite. Em algumas ocasiões ela me convenceu a me exibir através da câmera do computador, totalmente nu, eu aceitei, pois estava interessado nela, mas para minha surpresa a menina era uma golpista que agora está exigindo dinheiro e me ameaçando dizendo que vai colocar minhas imagens em sites de

relacionamento e blogs de pornografia. O que faço?”

Neste caso a orientação foi procurar a delegacia mais próxima para registrar a ocorrência.

2. “Olá, quero uma ajuda, pois tem um amigo me ameaçando, ele me gravou vestindo o vestido e disse que se eu não fizer o que ele quer ele vai postar em redes sociais e YouTube. Estou desesperada não posso falar para os meus pais. Tenho medo, o que faço? Nunca pensei que ele faria isso, por favor, ajude-me”

Neste exemplo a orientação foi que primeiro ela contasse para os pais e depois juntos eles procurassem a delegacia para registro da ocorrência.

Em novembro de 2012 policiais do DEIC de Santa Catarina prenderam, após dois meses de investigação, um homem que se passava por **Neymar** em programas de bate-papo, inclusive usando uma foto do jogador do Santos. Ele atraiu uma jovem de 23 anos, moradora de Florianópolis, para o MSN e o Skype, programas de conversação via web. As conversas em programas de bate-papo se transformaram em chantagens, exigências e extorsão assim que a jovem aceitou se exibir em fotos sensuais. O chantagista começou a ameaçá-la dizendo que iria divulgar as fotos se ela não enviasse mais imagens ou não cumprisse exigências. O autor das ameaças chegou a pedir R$ 50 mil para não divulgar fotos sensuais da garota. Ele foi preso em Volta Redonda (RJ), após a vítima denunciá-lo à polícia.[51]

Fraudes com cartões de crédito

A maioria das fraudes com cartão de crédito envolve falsificação. Segundo dados da VISA, cerca de 60% das fraudes mundiais e 52% das fraudes no Brasil são causadas pela falsificação de cartões. Os dados não deixam dúvida de que a primeira medida de segurança que você deve adotar para evitar as fraudes é proteger seus dados pessoais.

Quando uma pessoa compra algo usando o cartão, seu nome e número ficam armazenados na empresa que efetuou a venda. Se alguém conseguir invadir o sistema dessa empresa, poderá ter acesso aos dados e com isso assumir sua identidade.

As instituições financeiras e empresas que atuam no varejo on-line estão investindo cada vez mais em tecnologia para garantir a segurança do consumidor. Tanto que já são capazes, através de ferramentas específicas, acompanhar o perfil do usuário e detectar quaisquer atitudes fora do padrão normal de uso, o que permite a rápida identificação do uso indevido do cartão.

Como proceder nos casos de fraudes com cartões

Alerte a instituição para não autorizar qualquer crédito sem a sua aprovação. Leia as faturas com atenção e comunique qualquer transação irregular.

Em caso de cobrança indevida, o consumidor deve entrar em contato imediatamente com a administradora do cartão, fazer um boletim de ocorrência e registrar todo o processo através de documentos. Guarde cópias do relatório policial para apresentar à instituição financeira responsável se for preciso, pois, com isso, ficará claro que você foi vítima de um crime.

Em São Paulo este tipo de ocorrência também pode ser feito através do sítio da Polícia Civil já citado anteriormente (http://www2.policiacivil.sp.gov.br.) Se a instituição financeira não estornar lançamentos indevidos, o consumidor deverá formalizar reclamação em um órgão de defesa do consumidor, no Juizado Especial Cível ou Justiça Comum.

Como denunciar lojas virtuais que não entregam os produtos

No caso de problemas com compras feitas pela internet, a

reclamação pode ser registrada diretamente no site do Procon-SP pelo endereço**: http://www.procon.sp.gov.br/atendimento_texto.asp**. O endereço eletrônico também está aberto para orientação sobre qualquer outro problema de consumo, sendo o horário do canal de atendimento das 10:00h às 16:00h, de segunda a sexta.

Desde 2011, o Procon-SP mantém lista de sites não recomendados na sua página, no link "**Evite esses sites**", contendo endereço eletrônico em ordem alfabética, razão social da empresa e número do CNPJ ou CPF, além da condição de "**fora do ar**" ou "**no ar**". A lista atualizada em 12/07/2013 já contava mais de 270 lojas. O Procon-SP recebe reclamações desses sites por irregularidades na prática de comércio eletrônico, principalmente por falta de entrega do produto adquirido pelo consumidor e não obtém resposta deles para a solução do problema.

Essa lista pode ser acessada através do Link: http://www.procon.sp.gov.br/pdf/acs_sitenaorecomendados.pdf

Como posso ter certeza de que o site é confiável ou de que está registrado

Busque referências de amigos ou familiares e dê preferência a estabelecimentos que informem seu endereço físico e outras maneiras para que o consumidor o localize como: a razão social, CNPJ, e-mail e telefone. Cuidado com os sites que fornecem número apenas de celular e que oferecem preços baixos demais.

No site **www.registro.br**, o consumidor tem acesso aos dados dos responsáveis pelo endereço do site, seja Pessoa Jurídica (CNPJ, endereço, telefone) ou Pessoa Física (CPF, endereço, telefone do responsável pelo site). Veja como é fácil: Se o site for .**com.br** entre no site *www.registro.br* e logo no início verá o campo **PESQUISAR**. Basta digitar o

endereço neste campo sem o *www* e pesquisar.

No próximo passo será informado se o domínio já esta registrado e abaixo terá um link escrito MAIS INFORMAÇÕES, clique neste link e aparecerá a informação dos servidores DNS e outros. Logo abaixo você verá a seguinte frase: caso necessite obter mais informações sobre este domínio, consulte pelo **Whois**.

Pronto! Até aqui você já conseguiu saber em nome de quem está registrado. Se precisar de informações mais detalhadas, como endereço e telefone, clique no link **Versão com informações de contato** no box superior e será pedido para preencher os caracteres. Após isso, aparecem todos os dados da pessoa responsável.

Whois é um serviço público que permite visualizar informações sobre um domínio. Ele verifica se um domínio está disponível ou não e também pode retornar as informações pessoais sobre o proprietário do domínio. Trata-se de um protocolo que é capaz de realizar buscas dentro do banco de dados do serviço responsável.

Todos os domínios com finalização ***.com.br*** são de responsabilidade do Registro.br. Já os domínios internacionais são administrados pelo site Icann.

Como denunciar perfis roubados ou clonados

Se o seu perfil for subtraído ou clonado, você pode denunciar no próprio prestador do serviço, pois normalmente ele possui um mecanismo próprio que analisa o conteúdo e retira do ar assim que solicitado.

Passo 1: **coletar e preservar as evidências**, como já foi dito anteriormente.

Passo 2: denunciar ao próprio administrador do serviço. Os canais para denunciar perfil falso são:

No Facebook

A melhor maneira é usar o link Denunciar que aparece ao lado do próprio conteúdo. Veja como: 1.

Entre no perfil falso do usuário que roubou sua foto ou nome (ou ambos).

2. Na parte superior da Timeline, clique na setinha do lado direito de "Mensagem" e escolha "Denunciar/Bloquear".
3. Na janela que abrir, marque a opção "Este perfil está fingindo ser alguém ou é falso", escolha o "Motivo" da sua denúncia, como: "Tentando se passar por mim", mas tem também "Fingiu ser alguém que eu conheço" (será preciso copiar o endereço do Facebook da pessoa que está sendo copiada) e outras três opções de denúncia. Quando terminar, clique em "Continuar".
4. Pronto, sua denúncia foi enviada. O Facebook irá verificar as informações fornecidas.

Para acompanhar o andamento da denúncia feita, acesse este link: **https://www.facebook.com/settings?tab=support/**

ATENÇÃO!! No caso de alguém estar copiando uma pessoa que você conhece, é importante digitar o endereço URL do PERFIL VERDADEIRO (não é o endereço URL do perfil falso!), porque se você não colocar isso, eles não poderão verificar se as informações são verdadeiras ou não.

Para qualquer outro tipo de denúncia no Facebook, acesse o endereço **http://www.facebook.com/report/** e siga os passos da tela.

No Twitter

A central de ajuda do Twitter oferece uma lista bem completa para denunciar violações. Acesse: **http://support.twitter.com/groups/33-report-abuse-**

or-policy-violations e escolha qual melhor lhe atende.

O Twitter possui também um e-mail exclusivo para denúncias de contas com conteúdo sexual infantil, o cp@twitter.com.

Como denunciar vídeos impróprios no YouTube

Com a nova interface do YouTube disponível desde 07/12/2012, para denunciar um vídeo como impróprio deve-se clicar no botão "Report". O botão está situado por baixo de cada vídeo, na respectiva página de visualização.

Vídeos e usuários denunciados são analisados pela equipe do YouTube 24 horas por dia, sete dias por semana, para determinar se eles violam as diretrizes da comunidade. As contas são penalizadas por violações dessas diretrizes, sendo que violações graves ou repetidas podem levar ao encerramento da conta.

Outros canais importantes para denúncias

mail-abuse@cert.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) – Para encaminhamento de denúncias de mensagens fraudulentas, deve ser enviada uma cópia do e-mail original e também comunicar a instituição que está sendo utilizada no golpe.

phishing@cais.rnp.br – Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) – Para encaminhamento de denúncias de mensagens fraudulentas deve ser enviada uma cópia do e-mail original e também comunicar a instituição que está sendo utilizada no golpe.

artefatos@cais.rnp.br – Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino

e Pesquisa (RNP) – Para encaminhamento de denúncias de aplicativos suspeitos (cavalos de troia e outros programas maléficos usados nos golpes on-line).

crime.internet@dpf.gov.br – Mensagens que se refiram aos crimes de internet devem ser reportadas ao novo canal centralizador dessas denúncias na Divisão de Comunicação Social da Polícia Federal **Digi Denúncias** – **www.prsp.mpf.gov.br/noticias-prsp/aplicativos/digi-denuncia** - Canal de denúncia de crimes eletrônicos do **Ministério Público.**

denunciar.org.br – SaferNet Brasil – É uma organização não governamental que reúne especialistas para combater crimes digitais. O que denunciar? Pornografia infantil, racismo, xenofobia e intolerância religiosa, neonazismo, apologia e incitação a crimes contra a vida, homofobia, apologia e incitação a práticas cruéis contra animais e tráfico de pessoas.

reclameaqui.com.br – Site para quem costuma fazer compras ou usar serviços pela internet. Bom para tirar dúvidas, fazer reclamações ou pesquisar empresas fraudulentas.

ic3.gov- Internet Crime Complaint Center – Site para denunciar crimes digitais internacionais.

Como investigar e apurar judicialmente a autoria de crimes digitais

Descobrir o IP da máquina que gerou o suposto crime é a única maneira de identificar quem é o culpado. Este procedimento só é efetuado, porém, após uma solicitação de quebra de sigilo telemático feita pela polícia. Quando este IP, que é o número que identifica cada computador, for descoberto, basta encontrar, junto ao provedor, onde ele está instalado.

O primeiro passo é acionar o provedor de serviços, para que

este informe os dados de conexão **(IP, data, hora, GMT)** envolvendo um suposto crime.

Na sequência, acionar o provedor de acesso, para que este informe os dados físicos **(nome, RG, CPF, endereço, telefone etc.)** do titular da conta de Internet que estava conectado no momento exato identificado pelo provedor de serviços.

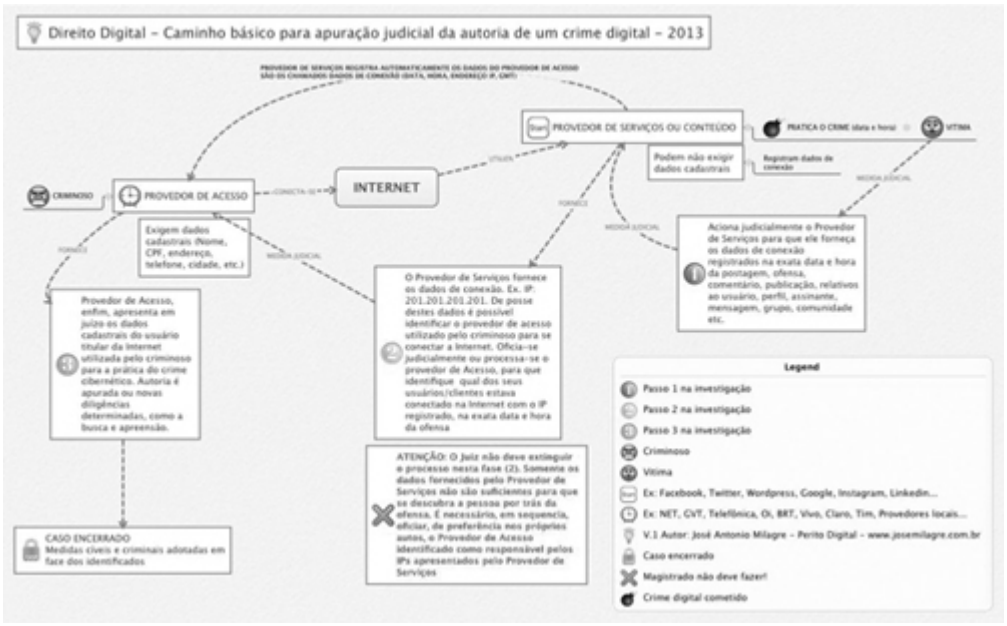
Pronto! É através desta correlação envolvendo provedor de serviços e provedor de acesso é possível chegar à autoria de crimes na internet.[52]

É bom saber que quem instala uma linha é responsável pelo seu uso. Sendo assim, a princípio o titular é o responsável pelos crimes cometidos no computador.

O Dr. José Antonio Milagre[53] criou e disponibilizou para download um gráfico ilustrativo e legendado denominado "**Caminho básico para apuração judicial da autoria de um crime digital – 2013**". Pelo gráfico, advogados, promotores, acadêmicos, vítimas e membros do judiciário poderão rapidamente compreender de forma básica como um delito digital é praticado, via de regra, e como é possível apurar a autoria, na grande maioria dos casos.

O documento é liberado para uso em requerimentos, petições e quaisquer outros pleitos judiciais envolvendo crimes informáticos, e o endereço para o download é: Versão PDF – http://josemilagre.com.br/blog/wp-content/uploads/2013/07/Mapa-Apurac%CC%A7a%CC%83o-Autoria-Crimes-na-Internet-v1.pdf

Versão JPG – http://josemilagre.com.br/blog/wp-content/uploads/2013/07/Mapa-Apurac%CC%A7a%CC%83o-Autoria-Crimes-na-Internet-v1.jpg)


Direito Digital – Caminho básico para apuração judicial da autoria de um crime digital – 2013
PROVEDOR DE SERVIÇOS REGISTRA AUTOMATICAMENTE OS DADOS DO PROVEDOR DE ACESSO
SÃO OS CHAMADOS DADOS DE CONEXÃO (DATA, HORA, ENDEREÇO IP, GMT)
PROVEDOR DE SERVIÇOS OU CONTEÚDO
PRATICA O CRIME (data e hora)
VITIMA
Podem não exigir dados cadastrais
Registram dados de conexão
CRIMINOSO
PROVEDOR DE ACESSO
CONECTA-SE
INTERNET
UTILIZA
FORNECE
MEDIDA JUDICIAL
Exigem dados cadastrais (Nome, CPF, endereço, telefone, cidade, etc.)
Aciona judicialmente o Provedor de Serviços para que ele forneça os dados de conexão registrados na exata data e hora da postagem, ofensa, comentário, publicação, relativos ao usuário, perfil, assinante, mensagem, grupo, comunidade etc.
Provedor de Acesso, enfim, apresenta em juízo os dados cadastrais do usuário titular da Internet utilizada pelo criminoso para a prática do crime cibernético. Autoria é apurada ou novas diligências determinadas, como a busca e apreensão.
O Provedor de Serviços fornece os dados de conexão. Ex. IP: 201.201.201.201. De posse destes dados é possível identificar o provedor de acesso utilizado pelo criminoso para se conectar a Internet. Oficia-se judicialmente ou processa-se o provedor de Acesso, para que identifique qual dos seus usuários/clientes estava conectado na Internet com o IP registrado, na exata data e hora da ofensa
ATENÇÃO: O Juiz não deve extinguir o processo nesta fase (2). Somente os dados fornecidos pelo Provedor de Serviços não são suficientes para que se descubra a pessoa por trás da ofensa. É necessário, em sequencia, oficiar, da preferência nos próprios autos, o Provedor de Acesso identificado como responsável pelos IPs apresentados pelo Provedor de Serviços
CASO ENCERRADO
Medidas cíveis e criminais adotadas em face dos identificados
Legend
Passo 1 na investigação
Passo 2 na investigação
Passo 3 na investigação
Criminoso
Vitima
Ex: Facebook, Twitter, Wordpress, Google, Instagram, LinkedIn...
Ex: NET, GVT, Telefônica, Oi, BRT, Vivo, Claro, Tim, Provedores locais...
V.1 Autor: José Antonio Milagre – Perito Digital – www.josemilagre.com.br
Caso encerrado
Magistrado não deve fazer!
Crime digital cometido

Capítulo 8. Endereços Úteis

Conforme determinado pela **Lei 12.735/12**, órgãos da polícia judiciária deverão criar setores especializados no combate a crimes virtuais. Alguns estados brasileiros já possuem essas estruturas. Se você foi vítima de um crime virtual, veja se o seu estado já possui uma delegacia especializada; caso contrário, você pode e deve registrar a ocorrência na Delegacia de Polícia mais próxima. O que não pode acontecer é você deixar de buscar orientação policial. Veja os endereços atualizados: **São Paulo:**

DIG-DEIC – 4ª Delegacia – Delitos praticados por Meios Eletrônicos. Presta atendimento presencial, por telefone e via web. Endereço: Av. Zack Narchi, 152, Carandiru – São Paulo (SP) Fone: (11) 2224-0721 ou 2221 – 7030. Para denunciar qualquer espécie de delito virtual anonimamente, utilize o e-mail: 4dp.dig.deic@policiacivil.sp.gov.br.

Rio de Janeiro: **Delegacia de Repressão aos Crimes de Informática (DRCI) –** Rua Professor Clementino Fraga, nº 77 (2º andar), Cidade Nova (prédio da 6ª DP), Rio de Janeiro/RJ (CEP: 20230-250), telefones (0xx21) 2332-8192, 2332-8188 e 23328191 e e-mail drci@pcivil.rj.gov.br.

Espírito Santo: **Delegacia de Repressão a Crimes Eletrônicos (DRCE)** – Av. Nossa Senhora da Penha, 2290,

Bairro Santa Luiza, Vitória/ES (CEP: 29045-403), telefone (0xx27) 3137-2607 e e-mail: drce@pc.es.gov.br.

Minas Gerais: **DEICC – Delegacia Especializada de Investigações de Crimes Cibernéticos** – Av. Nossa Senhora de Fátima, 2855 – Bairro Carlos Prates – CEP: 30.710-020, telefone (33) 3212-3002, e-mail: dercifelab.di@pc.mg.gov.br.

Paraná: **Nuciber da Polícia Civil do Paraná** – Rua José Loureiro, 376, 1º andar – sala 1 – Centro – 80010-000 – Curitiba-PR, Tel:(41) 3323-9448 – Fax: (41) 3323-9448, e-mail cibercrimes@pc.pr.gov.br.

Rio Grande do Sul: **Delegacia de Repressão aos Crimes Informáticos (DRCI/DEIC**) – Av. Cristiano Fischer, 1440, Bairro Jardim do Salso em Porto Alegre, na mesma sede do DEIC. O telefone de contato é (0xx51) 3288-9815, e-mail drci@pc.rs.gov.br.

Distrito Federal: **Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT) –** Não atende diretamente ao público. Neste caso, a vítima pode procurar a delegacia mais próxima para efetuar registro de ocorrência. A DICAT é uma **Divisão** especializada em crimes tecnológicos que tem como atribuição assessorar as demais unidades da Polícia Civil do Distrito Federal. O telefone é (0xx61) 3462-9533 e o e-mail é dicat@pcdf.df.gov.br.

Goiás: **Gerência de Inteligência da Polícia Civil** – Setor de Análise (0xx62) 3201-6352 e 6357).

Pará: **Delegacia de Crimes Virtuais –** Rua Oliveira Belo

nº 807, Belém-PA. CEP: 66.050-380, com telefone de contato (91) 3222-7567. Entre a Trav. Nove de Janeiro e a Av. Alcindo Cacela.

Mato Grosso: Gerência de **C**ombate a **C**rimes de **A**lta **T**ecnologia – **GECAT** – Av. Cel. Escolástico Nº, Bandeirantes – Cuiabá – Cep: 78.010-200 – Telefone: (65) 363-5656.

Sergipe:

Delegacia de Repressão a Crimes Cibernéticos (DRCC) – Rua Laranjeiras, nº 960, Bairro Centro - Aracaju – Cep: 4900-000, telefone: (79) 3198-1124.

Piauí:

Delegacia de Repressão a Crimes Tecnológicos (DERCAT). Endereço: Delegacia Geral da Polícia Civil do Piauí – Rua Barroso, nº 241, Centro – Teresina – telefones: (86) 3216-5212 (recepção); (86) 3216-5225 (plantão geral).

Endereços dos principais provedores de serviços

Um provedor de serviço ou **ISP (Internet Service Provider)** é uma empresa que fornece utilidades e serviços como: *hospedagem, e-commerce, serviços de e-mails, comunicadores, chats, jogos on-line, redes sociais, dentre outros*. Exemplos: Google, Facebook, MercadoLivre, Yahoo e Hotmail.

Se você está sendo vítima de algum crime relacionado a algum dos prestadores de serviços listados a seguir, envie uma carta registrada pedindo para preservar todas as provas da materialidade e os indícios de autoria do(s) crime(s). A carta modelo você encontra disponível no ***Capítulo 7***.

MICROSOFT CORPORATION/MICROSOFT INFORMÁTICA LTDA Av. Nações Unidas, 12 901 - 27º andar - Torre Norte, CEP: 04578-000, São Paulo/SP

Universo Online S.A Av. Brigadeiro Faria Lima, 384, 6º andar, CEP: 01452-002 – São Paulo, SP

Yahoo! do Brasil Internet Ltda.

R. Fidêncio Ramos, 195 – 12º andar, Fone: (11) 3054-5200 - CEP: 04551-010, São Paulo - SP

Terra Networks Brasil S.A.

Centro Empresarial Nações Unidas, 12.901 – 3º andar, CEP: 04578-000, São Paulo - SP

Google Brasil Internet Ltda.

Av. Brigadeiro Faria Lima, 3900, 5º andar, CEP 04538-132, São Paulo - SP

Internet Group do Brasil S.A (IG-OI) Rua Amauri, 299 – Itaim, Fone: 0800 770-7839 - CEP: 01448-901, São Paulo – SP

Facebook

Rua Leopoldo Couto de Magalhães Júnior, nº 700, 5º andar, Edifício Infinity, Itaim Bibi, CEP: 04542-000, São Paulo – SP

Provedores de acesso

Os provedores fornecem acesso de usuários à rede mundial de computadores, possuindo o cadastro daquele que utiliza os seus serviços.

Exemplos: Telefônica, Embratel, Net, GVT, Brasil Telecom, Claro, *etc.*

Como rastrear um IP utilizando a geolocalização

O rastreamento de um endereço IP é realmente muito simples, e mesmo que nem sempre seja possível rastrear um indivíduo específico, você pode obter informações suficientes para agir e fazer uma denúncia.

O que você pode obter a partir do endereço IP

1. Qual provedor de serviços de internet (ISP, do Inglês "Internet Service Provider") o usuário está usando.
2. A localização física aproximada do usuário (por exemplo: São Paulo, SP).
3. Normalmente você não vai saber o nome real da pessoa que está usando o endereço IP. Os **ISPs** (provedores de serviços) normalmente só liberam tais informações sob ordem judicial.

Entendendo o que é o IP

Para o uso de computadores em rede, é necessário que cada computador tenha um endereço, uma forma de ser encontrado. O **IP (Internet Protocol)** é uma tecnologia que permite a comunicação padronizada entre computadores, mesmo que estes sejam de plataformas diferentes, identificando-os de forma única em uma rede.

Existe o IP *estático* (ou fixo), que é um número IP dado permanentemente a um computador, ou seja, seu IP não muda, exceto se tal ação for feita manualmente. Como exemplo, há casos de assinaturas de acesso à internet via ADSL, onde alguns provedores atribuem um IP estático aos seus assinantes. Assim, sempre que um cliente se conectar, usará o mesmo IP.

Essa prática é cada vez mais rara entre os provedores de acesso, por uma série de fatores, incluindo problemas de segurança. O IP *dinâmico*, por sua vez, é um número dado a um computador quando este se conecta à rede, mas que muda toda vez que há conexão. Como você deve imaginar,

existem poucos números de IP possíveis (comparado ao imenso número de computadores no mundo), por isso eles são distribuídos pelas organizações competentes, como a IANA e a LACNIC. Cada país pode usar uma determinada faixa de IP, e é assim que a geolocalização ou o GeoIP descobre, por exemplo, o seu país: verifica em que faixa de IP o seu endereço se encaixa.

Endereço IP de um E-mail Para encontrar o IP de um e-mail enviado para você, investigue o cabeçalho da mensagem. (Veja no Capítulo 7 como fazer).

Vá para um site que permita busca por informações sobre o endereço IP. Procure no Google, "Procurar ou Localizar IP" ou "**Geolocalização de IP**" para obter uma grande lista de sites que oferecem este serviço gratuitamente. Já testei vários e achei alguns bem práticos.

http://geoip.flagfox.net/ (GeoTool)
http://whois.domaintools.com/

http://www.maxmind.com/app/lookup_city

Vamos usar como exemplo o primeiro link que sugeri, o **GeoTool**. Assim que for acessado, a tela inicial já mostrará o número do IP que você está usando.

Nome do servidor 189-69-93-150.dsl.telesp.net.br Provedor DE SÃO PAULO S/A – TELESP Continente América do Sul – País Brasil Código do país BR (BRA) Região São Paulo Hora local 02 Jan 2013 12:07 Cidade São Paulo Latitude -23.5333 Endereço IP 189.69.93.150 Longitude -46.6167

Essas informações são referentes ao IP que eu estava usando no momento em que estava escrevendo este tópico (você perceberá que os dados referentes ao seu IP são diferentes). Para exibir mais detalhes, clique em Endereço IP e o site o direcionará para uma página com mais detalhes. Se você precisa pesquisar outro IP (como o retirado de um cabeçalho de e-mail) basta inserir no campo: Endereço IP/Nome do servidor e enviar, que o

redirecionamento lhe trará as informações referentes ao IP solicitado.

O que o endereço IP revela sobre você

A única informação que o endereço IP revela é o provedor de acesso (**ISP**). A partir dessa informação é possível determinar, em alguns casos, a localidade aproximada da conexão. Isso porque muitos provedores usam endereços IPs específicos para determinadas regiões ou, às vezes, são provedores locais que atuam somente em uma cidade ou estado.

Não existe, necessariamente, qualquer ligação do endereço IP com o local geográfico do internauta. Por exemplo, um internauta pode usar uma conexão discada para se conectar a um provedor europeu e terá um IP na Europa, independentemente do lugar físico do computador.

Para obter outras informações é preciso que a polícia obtenha uma ***ordem judicial*** para que o provedor revele os dados do assinante que estava com um endereço IP em uma determinada hora e dia. O detalhe da hora e data é importante porque é comum receber um novo endereço IP a cada vez que se conecta. Logo, sem uma informação precisa sobre a data e hora não é possível determinar quem pode estar usando um endereço.

Vale a pena se preocupar?

As coisas sempre funcionaram dessa forma. Alguém pode obter seu endereço IP apenas iniciando uma chamada no Skype, enviando um arquivo ou dando um link. Mas o endereço IP não serve para nada sozinho. Ele não permite uma invasão (para isso, é preciso usar uma brecha de segurança, o que se resolve por meio da atualização do sistema). Ele não vai permitir que alguém relacione seu IP a outros dados sem informações sobre **data e hora**.

Da mesma forma, também não será possível saber quem você é apenas pelo endereço IP.

Quem registra seu endereço IP

Praticamente todos os sites que você visita registram seu endereço IP e guardam-no em um banco de dados por períodos que variam de trinta dias a dois anos. Às vezes, o período é indeterminado, como, por exemplo, nas postagens de fóruns on-line e comentários.

Em muitos casos, o endereço IP fica registrado no cabeçalho das mensagens de e-mail, apesar de o e-mail ser um meio de comunicação intermediado.

Capítulo 9. Novas Leis Reforçam a Luta Contra Crimes Virtuais

Leis de Crimes Informáticos

Entraram em vigor em 02 de abril de 2013 as leis ***12.735/12*** e ***12.737/12***, que alteram o Código Penal para tratar de crimes cibernéticos.

A primeira, ***Lei 12.735/12***, tipifica condutas realizadas mediante uso de sistemas eletrônicos, digitais ou similares, que sejam praticadas contra sistemas informatizados. O projeto original dessa lei tramitou no Congresso desde 1999 (PL 84/99, na Câmara). O texto original era bastante abrangente e criou polêmica, por exemplo, no que se refere à responsabilidade dos provedores de internet. Durante a longa tramitação, no entanto, foi reduzido a quatro artigos e, na sanção, a presidente Dilma Rousseff vetou dois. Portanto, a lei traz somente duas mudanças: a) Determinação para que as polícias civis dos estados brasileiros criem setores especializados no combate a crimes virtuais conforme descrito no artigo 4º.

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Em resumo, o artigo 4º determina que as polícias civis de

todo o Brasil terão que se adaptar para esta nova realidade, o que não vem acontecendo. As forças policiais no Brasil não estão estruturadas e treinadas adequadamente para enfrentar, com eficiência, os crimes virtuais. Pelo contrário, alguns estados estão extinguindo os serviços que possuem.

No dia 28 de junho de 2013, a Polícia Civil do Rio Grande do Norte extinguiu o Núcleo de Investigação dos Crimes de Alta Tecnologia (**Nicat**). A portaria normativa que pôs fim ao Núcleo que investigava os crimes virtuais no estado foi assinada pelo delegado geral Ricardo Sérgio Costa de Oliveira e publicada no Diário Oficial daquele estado, onde ele admite que o **Nicat** "carece de organização, estruturação, pessoal e disciplina de gestão administrativa permanente para alcançar a eficiência de resultados na prestação dos serviços públicos".[54]

b) O artigo 5º altera o inciso II do § 3º do art. 20 da Lei no 7.716, de 5 de janeiro de 1989, sobre racismo, dando autorização para que juízes determinem a interrupção de conteúdos racistas em qualquer meio de comunicação. Para esse crime, a pena vai de dois a cinco anos de prisão e multa.

A segunda, ***Lei 12.737/12***, criminaliza as condutas cometidas através da internet, tais como: invasão de computadores, roubo e/ou furto de senhas e de conteúdos de e-mails e a derrubada intencional de sites, inclusive oficiais, o que tem ocorrido em todo o mundo. Esta lei ganhou o apelido de ***Lei Carolina Dieckmann*** porque o projeto (PL 35/12) foi elaborado na época em que as fotos da atriz foram espalhadas pela internet.

Muitas são as opiniões formadas em relação a esta lei **12.737/12**. Uma das criticas é em relação às punições previstas, que são muito brandas, pois no Brasil pena de até quatro anos de reclusão para crime sem violência se transforma em restrição de direitos. Portanto, na prática ninguém sofrerá perda de liberdade, porque a nova lei

prevê no máximo um ano de detenção. Os principais pontos alterados pela nova lei são: a) Passa a ser crime o simples ato de interromper (os conhecidos **DDoS**) os serviços de utilidade pública em mídias disponíveis na internet. Mas atenção: se sua empresa for atacada, você deve provar que o serviço prestado é de utilidade pública.

b) Os cartões de crédito e débito passam a ser um documento particular. Ações como roubo, adulteração ou falsificação passam a ser regidas por lei já existente.

c) O simples fato de invadir um dispositivo e obter informações privadas, com ou sem intenção de utilizá-las de forma ilícita, passa a ser crime também. Assim, senhas, documentos sigilosos, conversas particulares e correspondência, se forem encontrados de posse de terceiros, sem autorização, já são indicados como crime, independente de serem ou não utilizados para algo ilícito.

d) Desenvolver e distribuir softwares de grampo, escutas ou controle remoto para fins ilícitos também passam a ser considerados crime.

Uma regulamentação mais completa é esperada com o Marco Civil, que vem sendo discutido na Câmara. Ele pretende definir responsabilidades e deveres de **provedores e usuários**.

O Marco Civil da Internet

Marco Civil da Internet é o nome pelo qual ficou conhecido o Projeto de ***Lei nº 2.126/2011***, que pretende regulamentar a internet no Brasil, estabelecendo princípios, direitos e deveres para provedores e usuários brasileiros da web e se tornar uma espécie de "Constituição da Internet".

A proposta, até a conclusão desse livro, já havia entrado na pauta de votações da Câmara dos Deputados por seis vezes e ainda não tinha sido aprovada. Ela foi elaborada em conjunto com a população, que pôde fazer observações no texto por meio da internet. Foram recebidos mais de 2,3 mil

comentários, que resultaram no texto enviado pelo poder executivo ao Congresso em 2011.

Quais são os direitos e garantias estabelecidos pelo Marco Civil?

Remoção de conteúdo Segundo o Marco Civil, os provedores de conexão à internet não serão civilmente responsáveis por danos relacionados ao conteúdo gerado por terceiros (essas empresas não responderão na Justiça pelo conteúdo publicado por seus usuários). Isso só acontecerá caso, após ordem judicial, a empresa não tome as providências para tornar o conteúdo indisponível. Atualmente a remoção pode ser feita de forma extrajudicial – quando o usuário faz uma reclamação ao provedor via e-mail, por exemplo.

Dados pessoais O Marco Civil assegura ao internauta o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros de conexão e acesso; informações claras e completas sobre coleta, uso, tratamento e proteção de dados pessoais; garantia de direito à privacidade e à liberdade de expressão. Os provedores deverão manter os registros de conexão por um ano, e autoridades policiais ou administrativas poderão requerer de forma cautelar que esse período seja maior. No caso de aplicações de internet (programas on-line), a guarda dos registros é opcional.

Neutralidade da rede Este item propõe que o responsável pela transmissão do conteúdo deve tratar de forma igual quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino. É a chamada neutralidade da rede.

Em resumo, os destaques do projeto são: o direito à privacidade, o sigilo das comunicações (salvo em casos de ordem judicial), direito a não suspensão da conexão, a

manutenção da qualidade contratada da conexão e informações claras e completas sobre coleta, uso, tratamento e proteção de dados pessoais Em um quadro publicado no portal **IDGNOW** a advogada especialista em Direito Digital ***Patrícia Peck*** mostra o que poderá ser o Marcos Civil.

O QUE É HOJE	O QUE PODERÁ SER
Direito à Liberdade de Expressão com vedação ao anonimato.	Direito à Liberdade de Expressão com mecanismo legal válido que permitirá o anonimato na prática.
Não existe obrigação de guarda de dados de conexões ou aplicações de internet.	Haverá guarda obrigatória de registro de conexão por pelo menos um ano e será facultativa a guarda de registro de acesso á aplicação de Internet.
Conteúdo enviado por terceiro responsabiliza civilmente o provedor de conteúdo, caso não retire o material a pedido de interessado em prazo breve (24h – 72h)	Só haverá responsabilização do provedor de conteúdo caso exista Ordem Judicial e não seja cumprida.
Não há obrigação expressa de diretrizes para o uso de dados.	O uso de dados pessoais terá de atender às destinações informadas a ser realizado em conformidade com a boa-fé e com as legitimas expectativas dos usuários.
Sem obrigação de informar o motivo do armazenamento de dados.	O armazenamento de informações pessoais que vão além dos previstos no registro de acesso a aplicação de internet será descrito com informações claras e completas sobre a sua finalidade, o modo como que serão usados, as hipóteses de eventual divulgação a terceiros e outros detalhes relevantes sobre seu tratamento.
Não existe disposição sobre privilégios de	A neutralidade da rede será garantida a todos, sem privilégios ou preferência de trafego.

tráfico.	
Sem obrigação expressa para oferecer a exclusão dos dados pessoais.	O provedor de aplicação de internet deverá oferecer ao usuário a opção de solicitar a destruição definitiva dos dados pessoais que este tiver fornecido a determinada aplicação, a qualquer tempo.

O quadro está disponível em: http://idgnow.com.br/blog/digitalis/2013/02/15/impactos-do-marco-civil-da-internet/

Decreto Federal 7.962/13

Entrou em vigor a parir de 14/05/2013 o Decreto Federal nº 7.962/13, que objetiva suprir as lacunas por parte do **Código de Defesa do Consumidor (Lei nº. 8.078/90)** em relação ao processo de compra e venda pela internet, já que não há uma legislação exclusiva para o e-commerce.

Com as novas regras, as empresas que atuam no comércio eletrônico terão que dispor em suas páginas informações sobre produtos, fornecedores, serviços e aperfeiçoamento do atendimento ao consumidor.

Veja o que passou a vigorar a com o novo decreto: ➢

Informações claras e precisas. Os sites devem disponibilizar, em local de destaque e de fácil visualização e de forma clara e objetiva, o nome da empresa e número do CNPJ, ou do CPF (caso a venda seja feita por pessoa física), além do endereço físico e eletrônico do fornecedor.

□

Atendimento ao consumidor. Deve haver um canal de atendimento ao cliente de fácil acesso (chat, e-mail ou telefone) para as vendas e o pós-venda e estabelecer procedimentos claros sobre o direito de

arrependimento para a desistência da compra (de até sete dias). O decreto determina ainda que em todos os casos deve haver a confirmação imediata do recebimento das solicitações do consumidor, mesmo que de forma automática. Não havendo resposta, poderão ser aplicados eventuais ônus para a empresa.

□

Compras coletivas. Pela primeira vez, foram criadas regras específicas para ofertas em sites de compras coletivas. A partir do decreto, esses sites deverão informar a quantidade mínima de clientes necessária para valer a promoção, o prazo para utilização da oferta, além de dados para localização do fornecedor do produto ou serviço ofertado.

□

Direito dos Consumidores. As empresas ficam a partir de agora obrigadas a disponibilizar o contrato, ou pelo menos o sumário do contrato, antes da finalização da compra. O documento deve oferecer as informações necessárias ao consumidor antes de confirmar a aceitação da oferta.

Será obrigatório também que as empresas do e-commerce respeitem os direitos do consumidor, como, por exemplo, o de se arrepender da compra no prazo de até sete dias úteis, sem a necessidade de apresentar alguma justificativa. Nesses casos, a retirada do produto na casa do consumidor e o estorno do valor pago ficam a cargo da empresa.

Há também os casos de não arrependimento, mas em que há um defeito no produto ou este não está adequado para o consumo. Nesses casos, a medida prevê o prazo de trinta dias para o consumidor reclamar quando se tratar de bens não duráveis e noventa dias no caso de bens duráveis.

Capítulo 10. Estudos de Casos

Recebo diariamente dezenas de mensagens de pessoas procurando algum tipo de informação referente a crimes virtuais. Em quase dois anos da existência do meu blog, é fácil perceber que a maioria das vítimas tem em comum os mesmos problemas. Pesquisando a melhor resposta para essas dúvidas elaborei o **Capítulo 7** deste livro. Foi pensando nisso que tomei a liberdade de reproduzir algumas dessas mensagens. Classifiquei por assunto, coloquei respostas e algumas dicas para prevenção.

Todos os e-mails estão em sua configuração original apenas sem o nome dos remetentes para preservar suas identidades.

Lembrando que, se você foi ou está sendo vítima de qualquer tipo de crimes pela internet, siga os primeiros passos descritos no **Capítulo 7** para coletar provas e procure a delegacia mais próxima de sua residência e registre a ocorrência. Você também pode ir a uma delegacia especializada em crimes virtuais, caso exista uma no seu estado.

Golpes

Empréstimo fácil

- "Fui vítima de um golpe pela internet que o golpista me passou oferecendo um determinado

empréstimo da qual eu depositei uma quantia em dinheiro como garantia da liberação do empréstimo, perdi o dinheiro depositado na conta do golpista. Gostaria de saber a quem eu devo denunciar, tenho os comprovante de depósitos, tem como chegar aos golpistas. Alguém poderá me ajudar."

- "Fiz um empréstimo no qual foram exigidos vários depósitos no final nem recuperei o dinheiro depositado nem o empréstimo. Fiquei a ver navios"
- "Solicitei um empréstimo de **dez mil reais** e obtive resposta via e-mail mediante um contrato pra empréstimo e documentos necessários para a realização do mesmo. Após mandar o contrato junto com comprovante de residência e documento de identidade, retornaram a ligação no dia seguinte solicitando um deposito de **três mil reais**, pois o contrato foi aprovado, mas houve um engano no deposito do cheque que foi de treze mil e quinhentos, sendo então necessário que devolvesse os três mil e quinhentos. Então me mandaram duas contas para depósito uma no Bradesco e outra no Itau,sendo que ao mesmo tempo recebi notificação de um depósito de treze mil e quinhentos reais em meu celular.Então parti para o deposito. Depositei R$ 500,00 em dinheiro no bradesco via cheque transferência de um amigo e mil reais em dinheiro.Novamente ligaram dizendo que o cheque estava bloqueado e só iriam desbloquear mediante deposito do restante! Só então que caiu a ficha e descobri q estava sendo enganada!"
- "Fui vitima de um golpe, mas infelizmente quando fui pesquisar e vi o site com essas informações valiosas já

era tarde. Como estou lidando com despesas medicas e estou precisando de dinheiro achei tentador a facilidades do empréstimo, no primeiro contato telefônico um atendente pediu e-mail para enviar o formulário de proposta e preenchido meus dados reenviei uma hora mais tarde o atendente retornou avisando que meu cadastro estava aprovado e era para entrar em contato para definir valores do empréstimo optei por valor de 15.000,00 porem para liberar este valor eu teria que depositar **5% do valor** devido ao seguro fiador de um advogado deles mesmos, fiz o deposito de **750,00** o atendente garantiu que após uma hora o dinheiro estaria em minha conta, mas nada apareceu na conta. Além de estar precisando de dinheiro gastei mais e com golpistas. Ajudem-me”

Resposta: Este tipo de golpe é conhecido como “**empréstimo fácil**” e segue um padrão: as falsas instituições financeiras anunciam uma forma de “empréstimo pessoal” rápido, fácil, sem burocracia e com juros muito abaixo do mercado. De forma geral, solicitam que o cliente faça um depósito antecipado de 5% a 10% do valor do empréstimo ou outra forma de pagamento, que seria um seguro avalista ou fiador. Assim que o depósito é feito, a pessoa simplesmente não consegue mais contato e o empréstimo jamais é depositado na conta. Essas falsas instituições financeiras sempre utilizam telefones clonados e contas laranja abertas com documentações falsas, dificultando o trabalho da policia.

Existem casos em que os estelionatários chegam a depositar um valor acima do solicitado e pedem para a pessoa depositar a diferença a título de devolução. Por exemplo, a vítima solicitou R$ 10.000, eles depositaram um cheque de R$ 13.000 e pedem para que seja depositado R$ 3.000 a título de devolução. Como o depósito foi feito por cheque, o valor consta na conta, mas aparece bloqueado. Isso porque o banco precisa verificar se o cheque possui fundo, mas o atendente fala que para desbloquear é

necessário fazer o depósito de devolução e é aí que está o golpe, pois a pessoa ingênua ou mal informada faz o depósito caindo no golpe.

Dica: Fique sempre alerta e lembre-se de que nenhum banco, instituição ou agente de crédito que seja sério e verdadeiro solicita qualquer tipo de taxa ou antecipação de valores para conceder empréstimo.

Nunca envie seus documentos ou dados pessoais por fax ou e-mail para esse tipo de empréstimo fácil. Procure sempre instituições financeiras conhecidas e que tenham referências para realizar seu empréstimo. Jamais faça empréstimo por telefone, procure sempre realizá-los pessoalmente.

Ofertas de emprego

"Bom dia, há dois dias eu encontrei um site na web oferecendo um emprego para trabalhar em casa com rendimentos de até R$ 1.200,00 por semana. Eu só tinha que comprar um produto ou serviço oferecido por R$ 257,90, que por ventura estava na promoção, sendo oferecido por R$ 149,00. Este "pacote" oferecia uma espécie de software e com ele teria apenas que inserir links em sites da web. Porém comecei a desconfiar após perceber que só estava sendo aceito pagamento mediante cartão de crédito, mas as informações contidas no próprio site ofereciam o pagamento por outros meios principalmente via boleto bancário, mas quando entrei na página para fazer o pedido do "pacote (software e uma senha de conexão á um servidor ou banco de dados)" percebi que só por cartão de crédito poderia realmente efetuar o pagamento. Mesmo desconfiado preenchi todos os dados em um formulário para concluir a compra, e para minha surpresa clonaram meu cartão. O que fazer para recuperar meu dinheiro?"

Resposta: Basta uma simples busca na internet para achar milhares de sites com a oferta: **Trabalhe em casa e**

ganhe muito dinheiro pela web. Em muitos casos, podemos conhecer histórias de donas de casa que resolveram trabalhar na internet e atualmente ganham mais de R$ 10.000 por mês.

Todos os sites possuem quase sempre as mesmas características: ➢

Mostram alguns logotipos de emissoras de TV para dar mais credibilidade.

□

O texto é escrito com letras maiúsculas e/ou com trechos em destaque.

□

Exibem uma reportagem de um jornal da TV sobre o trabalho em casa.

□

Contam a história de uma mãe e/ou dona de casa que resolveu trabalhar em casa.

□

Mostram cheques dos pagamentos recebidos.

□

Exibem vários depoimentos de pessoas que já se deram bem com o "curso".

□

Possuem um texto cheio de falhas e erros.



Não há nenhum link para contato.

É claro que há maneiras lícitas de ganhar dinheiro na web, e para todas elas é necessário que se trabalhe muito.

Existem centenas de programas de afiliados sérios, com os quais o internauta pode ganhar comissões por cada venda realizada. Mas saiba que são necessárias muitas vendas para se gerar uma boa receita.

Dicas: ➢

Desconfie sempre que a esmola for muita.



Nada vem fácil.



Pesquise sempre antes de adquirir esses métodos milagrosos.



Nenhuma empresa séria exige pagamentos para contratar funcionários.



Denuncie os golpistas.

Troca de mercadorias

"Bem na verdade eu fui um tolo, pois foi uma negociação de troca via correio. Vi um anuncio na internet e percebi que ele tinha outros anúncios com telefones e foi aí que enviei um e-mail perguntando sobre a troca. Eu tinha um

galaxy note em perfeitas condições e queria trocar por um **galaxy s3** novo dando uma volta se fosse necessário.

Eu tenho mais de 100 e-mails comprovando esta negociação. Eles disseram que enviariam por sedex e me mandariam o número de rastreamento e que eu deveria mandar o meu enviando o número de rastreamento. Pedi o cnpj e eles me deram, mas creio ser de outra empresa. Foi o que eu fiz, mandei o meu aparelho e recebi uma fita de silicone em troca. Na verdade fui muito tolo e aprendi com a lição, e sei que é muito difícil recuperar o aparelho, mas a minha intenção é pará-lo para que não roube mais ninguém".

Resposta: Os golpistas agem sempre no ponto fraco da vítima, eles são rápidos e muito criativos. A regra é estar atento, desconfiando de ofertas absurdas e muito boas.

Phishing

- "Prezados, moro em São Gonçalo, e estou enviando este e-mail para pedir o socorro de vocês. Sofri um débito de quase cinco mil reais em minha conta no Banco Itaú. O fato se deu sexta-feira (18/01/2013). Eu acessei minha conta corrente e dentro do ambiente da conta surgiu uma pequena janela solicitando meu código (itoquem) para atualização de segurança. Após a informação o site informou que aguardasse enquanto processava. Saí normalmente do site. Mais tarde ao solicitar um saque num caixa eletrônico, estranhei a informação de que estaria usando o meu limite de cheque especial. Ao solicitar o extrato na tela, observei uma espécie de pagamento de título no valor aproximado de cinco mil reais. Por favor, me instruam como proceder para reaver o meu saldo. Muito obrigado."
- "Eu caí em um golpe na internet para roubo de dados pessoais e de cartão de crédito. Consegui imprimir o e-mail, as páginas que foram

direcionadas e os códigos-fonte das mesmas. Cheguei a ser debitado nos cartões de crédito várias vezes. Tenho medo dos meus dados pessoais nas mãos de pessoas mal intencionadas. Elas possuem todos os meus dados, incluindo CPF data de nascimento e identidade. Como proceder?"

- "Prezados, estou recebendo um email com diferentes abordagens. Já falará sobre nota fiscal, agora mensagem de voz pelo facebook o que pode ser?"
- "Bom dia, gostaria de saber se é considerado crime (pela internet) quando alguém envia e-mails, dizendo ser de algum cartório, sobre comunicado extra-judicial e cobrando o pagamento de algum boleto? Isso seria estelionato? Eu sei que estes e-mails são falsos, só não sei se é algum tipo de vírus ou golpe de alguém. Recebi e-mails de pessoa desconhecida com esse conteúdo. Só quero saber se é crime ou não.Obrigada."

Resposta: Todos esses são exemplos de engenharia social praticada por criminosos para tentar aplicar golpes estimulando a vítima a acessar páginas (sites) fraudulentas, preencher formulários com seus dados privados ou despertar curiosidade fazendo com que o usuário clique em um link para fazer download de um arquivo malicioso (malware) capaz de transmitir para o atacante as informações em que tenha interesse.

Dica: Desconfie mesmo se o e-mail vier de alguém que você conhece. É muito comum abrir uma mensagem e confiar em seu conteúdo quando se vê que a mensagem partiu de um conhecido seu. Mas não se esqueça de que conhecidos também estão sujeitos a terem suas máquinas

infectadas e que muitos malwares se autoenviam para a lista inteira de contatos. *Reveja o Capítulo 5 - Cuidado com os e-mails.*

Perfil falso

- "Olá estou precisando de ajuda, pois já é a terceira vez que alguém faz uma conta falsa no facebook usando meu nome e minhas fotos,esta pessoa fica me difamando e injuriando,me deixando constrangida pois sou casada e estudante fico sem graça diante da minha família e amigos não sei mais o que fazer a primeira vez me dirigi até a delegacia mais próxima e fiz um BO mas de nada adiantou essas vezes só denunciei a pagina mas ate agora nada,não sei mais o que fazer .Me ajudem."
- "boa tarde, eu queria saber como localizar uma pessoa que hackeou meu face e fica se passando por mim para as outras pessoas. Manchando minha imagem."
- "Uma pessoa se passou por mim em um chat sobre sexo na internet, divulgou fotos minhas e links de minhas redes sociais através de uma conta de e-mail criada em meu nome. Creio que essa mesma pessoa cadastrou meu e-mail em sites pornográficos e é possível que tenha mandado fotos minhas para esses sites também. Não tenho ideia de como proceder. Preciso de ajuda, por favor. Estou com medo de tudo na internet agora, é muito perigoso."
- "Boa noite, publicaram fotos dos meus dois filhos menores de idade no facebook sem minha autorização. Essas fotos foram copiadas do álbum de outras pessoas. Já solicitei que a pessoa

retirasse, mas ela nada fez. Como devo proceder?"

- "Oi, Vi uma foto de meu filho em uma comunidade do facebook, a foto está completamente mudada e acredito que é bullyng, essa foto foi roubada do meu álbum não sei quem é o dono da comunidade, mas acredito saber quem a enviou, como devo proceder? Posso fazer um boletim de ocorrências? Contra quem?"

Resposta: Vimos no **capítulo 4** que quem cria perfil falso usando a imagem de outra pessoa viola o previsto na Constituição Federal em seu artigo *5º, inciso X,* bem como o direito de personalidade previsto pelo Código Civil, além de cometer crime de **falsa identidade** quando for para obter vantagem, em proveito próprio ou alheio, *ou para causar dano a outrem*.

Os procedimentos são os mesmos: coletar provas e denunciar à polícia. Se o perfil falso foi criado no Facebook e você quer apenas retirá-lo, basta denunciá-lo. Esse procedimento é feito acessando o perfil falso através de uma conta legítima. Logo abaixo da foto do perfil, clique em "**Denunciar/Bloquear**", marque a opção "**Este perfil está fingindo ser alguém ou é falso> Escolha um tipo> Tentando se passar por mim**", e clique em "**Continuar**". Após a denúncia, a equipe do Facebook irá verificar a veracidade dos fatos e, se for o caso, remover o perfil denunciado como falso.

Para acompanhar o andamento da denúncia feita, acesse este link: https://www.facebook.com/settings?tab=support

Dica: Tenha cuidado com os conteúdos publicados na rede, pois eles são facilmente replicados, ou seja, as pessoas que tiveram acesso a fotos, vídeos ou textos podem facilmente copiá-los e redistribuí-los.

Furto de identidade

Olá, ano passado comprei um note sony vaio na ALPHA INFORMÁTICA por 545 reais, era uma loja virtual, o site sumiu e a encomenda nunca chegou, agora estão usando meu nome, criaram uma conta no Santander e pelo que entendi estão usando essa conta em meu nome para receber dinheiro das pessoas que compram nesse outro site que criaram a JIM INFORMÁTICA, que também está fora do ar. Não cheguei a fazer B.O. da encomenda que nunca chegou, porque me disseram que nunca iria conseguir meu dinheiro de volta, mas agora estão usando meu nome para essas atividades ilícitas. Descobri tudo isso hoje, quando uma das pessoas que comprou nessa loja online me ligou, e agora estão me ligando direto, sendo que eu não fazia ideia do que estava acontecendo, quero também tirar meu nome desse site de reclamações que tem meus dados mas não sei como prosseguir, se puderes me dar uma luz, estou muito preocupado com toda essa situação.

Resposta: Como já foi dito, o furto de identidade é um dos crimes mais praticados na internet. De posse dos seus dados, os criminosos podem abrir empresas ou contas bancárias e quem arca com consequências como perdas financeiras, perda de reputação e falta de crédito é você. Além disso, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

Dica: A primeira orientação que dou para qualquer pessoa que me procura solicitando ajuda por ter sido vítima de um crime virtual é procurar a polícia para registrar boletim de ocorrência. Neste exemplo fica claro o porquê da minha insistência, pois, se a vítima tivesse sido corretamente orientada a fazer o B.O. seria muito mais fácil resolver o problema. Outra orientação é agir com rapidez. De acordo com a Comissão de Comércio Federal, as chances de

sofrer uma grande perda financeira em detrimento de um roubo de identidade diminuem significativamente se você descobrir a violação dentro de seis meses contados da data em que ela ocorreu.

Se puder procure formas de pagamento que estejam menos sujeitas a fraudes, como os boletos bancários, evitando, assim, preencher formulários que pedem seus dados.

Crimes contra a honra

- "A dois meses atrás um rapaz me adicionou no Facebook se apresentando como um amigo de infância.mantivemos contatos até eu perceber que ele não é quem ele diz ser.E ele expôs fotos minha intimas em sua pagina do Facebook e enviou emails com essa fotos para outras pessoas de minha família e em um desses email ele declara que tem a senha do meu email também. Gostaria de uma orientação pois tenho filhas pequenas e ele está me expondo."
- "Solicito a gentileza do contato de vocês urgente, estou em fase de separação e meu ex-marido esta expondo minhas fotos intimas na Internet. Preciso de orientação."
- "Venho por este meios adquirir algumas informações de como devo proceder perante a uma postagem, contendo fotografias e vídeos não autorizados além de alguns comentários maldosos, ofensivos referente a minha pessoa,já que estou sabendo quem foi que postou como devo proceder para denunciá-lo? Preciso ir até uma delegacia? Devo contratar um advogado?Como vocês poderia estar me orientando a solucionar este problema? Aguardo uma resposta,e desde já agradeço."

- “ola estou sofrendo ofensas em um perfil criado no facebook. Como faço para dar um fim a isso? aonde posso denunciar? em qualquer delegacia?”
- “Boa tarde. Estamos sendo vítimas de crimes virtuais como injuria, difamação, violação de privacidade, dentre outros crimes, por meio do FACEBOOK. Nós salvamos as telas, as URLs e tudo mais, também denunciamos ao FACEBOOK, salvando todas as telas. As mensagens que ele mandou também salvamos. Registramos BO e tudo. O que eu quero é localizar a pessoa para processá-la. Como fazer? Você tem algum caso em que a pessoa foi localizada? Se a pessoa excluir o perfil ainda pode ser localizada? Grato.Diga não à impunidade!”

Resposta: Se você foi vítima de um dos crimes contra a honra ou de ameaça, de posse das provas coletadas, procure a delegacia mais próxima de sua residência e registre a ocorrência. Você também pode ir a uma delegacia especializada em crimes virtuais.

Dica: Vítimas que tiveram fotos ou vídeos íntimos divulgados na internet têm seus casos analisados através do **artigo de crimes contra a honra**, como difamação (o ato de disponibilizar imagens íntimas de uma pessoa) ou injúria (ofensas realizadas em meio digital). Mesmo que a pessoa tenha admitido que seu parceiro tirasse as fotos, não é permitido que tais imagens sejam repassadas. Portanto, quem teve a integridade manchada na internet possui total respaldo judicial.

Retirada de conteúdo

- “vou contar o que houve, sei que fiz a maior

besteira da minha vida, mas já ta feito então o que resta e correr atrás pra ve se resolve.. conheci uma pessoa pela internet em um site de relacionamento badoo, conversamos vários dias, esta pessoa falou que gostaria de ver umas fotos mais sensuais minhas e perguntei porque já que não tínhamos nenhuma intimidade, hesitei por muitos dias, porque um pressentimento me avisava que não ia dar certo, então ele me ofereceu uma quantia em dinheiro somente pelas fotos, então cai nessa e enviei, para um email que na verdade era um fake dele, então alguns dias depois ele me contou toda a verdade e me falou de onde era realmente como era e apareceu na Webcam pra mim ter a certeza de quem ele era, vi que tudo era uma farsa fiquei furiosa e o denunciei, consegui bloquear as contas dele, fazendo com que ele não fizesse isso com outra garota, porque ele me enviou várias fotos de meninas que ele já tinha conseguido, ele ficou muito bravo comigo, eu não lembrava no momento que ele tinha minhas fotos exclui minha conta e deu no que deu, ele postou minhas fotos todas na internet. Como fazer para retirar as fotos da Internet?"

- "um vídeo feito em câmera fotográfica no ano de 2008,apareceu agora em inúmeros sites pornográficos,desde então venho lutando,relatando abuso nos sites,muitos retiraram,porem outros recebem minhas denuncias e relatos de abuso mas não retira o vídeo,nem me da nenhuma resposta, tenho filha pequena ,estou sem poder voltar na minha cidade por que o vídeo alem de mostrar minha imagem informa minha cidade e estado onde nasci."

Resposta: Se suas fotos ou vídeos íntimos foram postados

em sites ou blogs de conteúdo adulto, a melhor coisa a fazer é entrar em contato diretamente com o administrador da página solicitando que retire o material o mais rápido possível sob pena de se acionar a justiça.

Informe ao administrador da página que quem mantém as fotos ou vídeos sem a autorização da vítima responde solidariamente com o autor do dano.

Dica: Tome cuidado ao deixar-se fotografar ou filmar. Não acredite na promessa de "depois eu apago" e, mesmo que você veja apagando o arquivo na sua frente, não se esqueça de que quando se apagam fotos e vídeos de um cartão de memória ou pendrive é muito fácil de recuperar. Lembre-se dos perigos de se exibir na webcam, principalmente para estranhos. Uma imagem parar na internet é muito fácil, mas quando se quer removê-la a coisa fica mais complicada.

"O par perfeito"

- "Existe uma quadrilha que tenta seduzir para depois extorquir dinheiro de mulheres brasileiras. Eu mesma já fui assediada pelo menos 3 vezes, com a última é a 4ª. Esta última ainda está acontecendo. Por que já digo que é um meio de extorsão? Porque a estória que contam é sempre a mesma. Um viúvo, solitário, pai de uma ou duas crianças que busca uma companhia. Um dado momento, dando como certo o enlace emocional, eles pedem dinheiro ou para remédio, ou para mandar para seus filhos que estão só com a babá, e eles como dizem ter seu local de trabalho longe, não conseguem enviar o dinheiro necessário para eles. O último ainda está na internet, no facebook, e acaba de me abordar. Em

sua segunda mensagem já veio contando a mesma estória. O que eu faço?

- "Bom dia! gostaria de saber como devo agir nesse caso. Outro dia uma pessoa pediu para que eu a aceitasse como amigo no meu facebook, à partir desse dia ele passou a fazer galanteios, mas todos com muito respeito, depois desse dia passamos a conversar pelo msn, onde ele compartilhou fotos de um filho que disse ser adotivo,foram muitas conversas em um determinado dia ele pediu para que eu enviasse uma mensagem a seu filho por que ele estava em zona de guerra na **Líbia** e não tinha como falar com o menino e me deu um numero e o que eu deveria falar, enviei a mensagem e tive a resposta, que deixei no face para ele, dai por diante todos os dias ele deixava uma mensagem ou falava comigo sempre cheio de amor. Quando foi ontem recebi uma mensagem pela manha que supostamente seria do menino, porem nessa mensagem veio com outro nome, em seguida respondi dizendo que não conhecia ninguém com aquele nome. Mais tarde entrei no meu face ele tinha deixado outra mensagem, eu deixei ali a mensagem que tinha recebido do numero que ele tinha me dado pra falar com o filo dele, logo ele ficou online e conversamos ele perguntou o que eu tinha respondido eu falei, e nesse momento recebi uma outra mensagem pelo celular do suposto menino que deveria enviar para o pai a mensagem dele. Foi ao que começou o **golpe**. Nesse momento ele começou a lamentar por não poder estar junto do filho e o menino estar sofrendo de estar sozinho em um País estranho, ele veio com a conversa que não tinha como enviar para o filho o dinheiro

para as despesas do mês e que o menino ainda precisava de um computador portátil, ai ele me falou que eu poderia ajudar, já bem desconfiada perguntei como eu poderia ajudar, foi ai que ele falou que eu poderia enviar o dinheiro para o suposto menino e o computador que assim que conseguisse vir ao Brasil ele me reembolsaria tudo. Neguei e a partir daí ele ficou off-line e não mais me enviou mensagens pelo face e nem msn. Gostaria muito de saber se devo denunciar essa pessoa porque ele de tentar me dar um golpe, tenho todas as conversar em meu face e msn, por favor me responda o mais rápido possível para que possa saber o que faço. Porque eu não cai na conversa dele mas outras mulheres podem cair. Obrigada aguardo uma resposta."

Resposta: Aqui os golpistas na maioria das vezes são homens e as vítimas, mulheres. Não se deve esperar que um golpista tenha cara de golpista ou se apresente como tal; ele sempre será bonito ou sensual, carinhoso, gentil, atencioso e disponível, ou seja, ele molda seu perfil para melhor atender às expectativas e desejos da vítima. Depois de ganhar a simpatia da vítima, ele conta uma história trágica e comovente para pedir dinheiro.

Dica: Desconfie! Pedir dinheiro a alguém que acabou de conhecer é uma atitude no mínimo estranha.

Compras pela internet

- "Fui lesado por um site de compras via internet tenho todos os dados desde o inicio da compra. Qual o caminho que devo seguir?"
- "Comprei um tênis no site em 6x e já vou pagar a

4 parcela e não recebi até hoje. Descobri no site Reclame aqui, que mais de 100 pessoas foram enganadas igual a mim eles não respondem a email e o telefone so cai na caixa postal não tem cnpj, estou indignado por ate hoje não ter fechado esse site.”

- “Gostaria de saber como proceder neste caso. Comprei uma capa de colchão Impermeável a quase um mês. A duas semanas depois de muita dificuldade consegui me comunicar com os funcionários, e um deles me disse que iriam me reembolsar, até agora nada. Onde denuncio? Na própria Policia Federal?”
- “ Por favor preciso de ajuda, fiz um pedido de compra de alguns produtos e efetuei o pagamento dos mesmos depositando o dinheiro na conta do vendedor como indicado, mas esse produto nunca chegou, faz mais de um mês tentei entrar em contato diversas, inúmeras vezes mas, nunca recebi nenhuma resposta ou qualquer tipo de satisfação,o vendedor usou de má fé e a consequência é que fui enganado,como faço para reaver meu dinheiro? desde já agradeço a atenção,obrigado.”
- “comprei um celular smartphone em 08/09, no site Lojas Vergueiro, o prazo de entrega venceu e não enviaram o produto. Mandei vários e-mails e só responderam o 1º dizendo que o produto seria postado na semana seguinte, já faz mais de um mês e não entendem o telefone e nem respondem os e-mails. Só agora descobri que há varias pessoas na mesma situação. Podem me orientar sobre como proceder?”
- “Fiz a compra de um produto (Tablet) pela internet, já se passou 11 dias que fiz o

pagamento e ate agora nada do produto, ligo para atendente, que diz : O produto já esta em São Paulo, mas devemos aguardar o código de rastreamento, já por e-mail, quanto mais cobro do site menores as informações do produto. O que devo fazer? Tenho medo de perder o dinheiro que paguei pelo produto, não sinto firmeza nos esclarecimentos. Caso seja necessário, tenho o código do produto, boleto pago, e os e-mails enviados."

- "Boa noite!Efetuei uma compra de uma TV pela internet. Fiz isto depois de averiguar qualificações do vendedor as quais estavam propicias para negociar. Apos alguns dias observei que o status no site não muda, continua até hoje como "aguardando pagamento". Já se passaram 7 dias. Procurei novamente referencias do vendedor na internet onde para minha surpresa observei várias reclamações de pessoas também lesadas pelo tal site. O que eu posso fazer? O vendedor não responde os meus e-mails, os telefones de contato não funcionam.

Resposta: Com as novas regras estabelecidas através do Decreto Federal 7.962/13 as empresas que atuam no comércio eletrônico terão que dispor em suas páginas informações sobre produtos, fornecedores, serviços e aperfeiçoamento do atendimento ao consumidor. As informações terão que estar disponíveis em local de destaque e de fácil visualização, e de forma clara e objetiva, o nome da empresa e número do CNPJ, ou do CPF (caso a venda seja feita por pessoa física), além do endereço físico e eletrônico do fornecedor.

Dica: Tenha cuidado especial ao comprar itens populares,

como MP3 players, câmeras digitais, smartphones, TVs LCD, notebooks, tablets e navegadores GPS. Itens mais desejados são mais explorados, o que pode tornar a compra mais arriscada. Pesquise bem antes de comprar, fazendo uma consulta sobre a loja no site **Reclame Aqui** (www.reclameaqui.com.br) ou no **Confiometro** (www.confiometro.com.br) para saber se existem reclamações contra ela. Uma busca rápida pode revelar resultados sobre atrasos na entrega, problemas com trocas, produtos danificados *etc.* Pesquise também nos sites de busca. Veja o que aparece sobre a empresa quando você digita o nome dela no *Google*, por exemplo. Você pode encontrar tanto reclamações quanto boas indicações. Consulte no **Capítulo 5** o item: ***Cuidado ao fazer compras pela internet*** para conhecer outras dicas.

Ameaças

- "Estou sendo chantageada por uma pessoa pela internet ele tem vídeos íntimos meus e disse que postará na rede se eu não fizer o que ele manda. Gostaria muito de acabar com isso. Preciso que me orientem como agir, a quem devo recorrer. Pelo amor de Deus! Estou desesperada"
- "Como faço com imagens divulgadas sem minha autorização. Estou sendo ameaçada, por um ex ele diz que vai publicar minhas fotos sensuais no facebook. O que eu faço"
- "Por favor me ajudem to sendo ameaçada, tive um namorinho virtual, e o cara me gravo na webcam pelada e ta ameaçando jogar na net o que devo fazer me ajudem desde de já muito obrigada"
- "como posso descobrir quem está ameaçando minha família com ameaças de morte pelo facebook. são ameaças horríveis, e essa pessoa troca de nomes

para enviar mensagens a todos nós.ameaças até contra a vida de nossas crianças. por favor me ajudem.estamos sofrendo muito."

- "Ando recebendo ligações com número desconhecido e também de um número identificado com ameaças. Posso registrar queixa em delegacia comum ou tenho que ir a uma delegacia especializada em crimes eletrônicos?"

Resposta: A primeira coisa a fazer é coletar e preservar as evidências. No caso de ameaças através de e-mail, além de preservar o conteúdo da mensagem, é preciso identificar o cabeçalho do e-mail e imprimi-lo como prova - **Leia o Capítulo 7**. O segundo passo é prestar queixa na polícia. Procure na página oficial da Polícia Civil do seu estado se existe a opção de registrar queixa eletronicamente; caso contrário, vá pessoalmente à delegacia mais próxima e registre a ocorrência. O que não pode é deixar de denunciar.

Caso o ameaçador seja uma pessoa conhecida, basta prestar queixa contra o sujeito no Juízo Criminal e Cível para solicitar uma "ordinária de ressarcimento pelos transtornos ocasionados". Não sendo o ameaçador conhecido, se a ameaça foi através de e-mail, com o cabeçalho e informações internas do e-mail será possível identificar a origem, e se foi através de algum provedor de serviços como, por exemplo, o Facebook, será preciso uma ordem judicial para liberar as informações do ameaçador. Procure o item *Como investigar e apurar judicialmente a autoria de crimes digitais na internet* – **no Capítulo 7.**

Dica: Se você recebeu qualquer tipo de ameaça pela internet, não se deixe intimidar; denuncie o mais rápido possível para que as provas necessárias para a sua proteção não sejam perdidas.

Outras dúvidas

- "Um vírus ou uma pessoa consegue entrar no meu computador e dele mesmo mandar email no meu nome da minha maquina e depois a pessoa que foi prejudicada entrar o meu IP? Mesmo não sendo eu que enviei? Eu estou sendo acusado de enviar um email para uma pessoa e não fui eu quem enviou."

Resposta: É possível sim um vírus disparar e-mails a partir do seu computador. São os chamados *vírus de e-mail***.** Reveja no **Capítulo 3** o item *Tipos de Vírus*.

- "Olá! Primeiramente, parabéns pelo site, muito útil. Gostaria que me tirasse uma dúvida: No meu trabalho, alguns colegas foram denunciados por um e-mail anônimo, e sabemos que tem como descobrir de onde foi enviado, mas a dúvida é a seguinte: se esse e-mail foi enviado por uma lan house e a pessoa que mandou, fez um endereço eletrônico falso, apenas para enviar a denúncia, como seria possível identificar quem foi a pessoa que mandou? Aguardo sua resposta. Um grande abraço e obrigada desde já."

Resposta: Alguns estados já possuem leis que obrigam as *lan houses* a manter um cadastro com nome do usuário, identidade, endereço, telefone, o equipamento e o horário em que foi utilizado, inclusive com imagens do usuário para confrontarem com informações passadas no cadastro.

[1] A palavra "computador" foi escolhida para se referir a todos os dispositivos passíveis de invasão e/ou de infecção por códigos maliciosos, como aparelhos celulares, smartphones, tablets, computadores e todos os dispositivos informáticos.

[2] http://www.em.com.br/app/noticia/internacional/2013/10/07/interna_internacional,457110/para-onu-internet-tera-2-7-bilhoes-de-internautas-ate-o-fim-do-ano.shtml. Acesso em: 07 out. 13.

[3] http://idgnow.com.br/internet/2013/08/13/acesso-mobile-cresce-e-brasil-alcanca-105-milhoes-de-internautas/. Acesso em: 07 out. 13.

[4] http://tecnologia.terra.com.br/noticias/0,,OI5754472-EI12884,00-Brasil+e+campeao+em+atividade+hacker+na+America+Latina.html. Acesso em: 16 mai. 12.

[5] http://www.d24am.com/noticias/amazonas/site-da-sepror-e-atacado-por-crackers-em-manaus/68010. Acesso em: 07 jul. 12.

[6] http://www1.folha.uol.com.br/folha/informatica/ult124u15159.shtml. Acesso em: 14 dez. 10.

[7] STALLINGS, Willian. Criptografia e Segurança de rede. 4 ed. São Paulo: Pearson Prentice Hall, 2008, p. 427.

[8] http://www.al.rn.gov.br/site/noticias.php?id=1577&titulo=especialista-diz-que-crimes-na-internet-superam-o-narcotrafico. Acesso em: 16 mar. 12.

[9] http://olhardigital.uol.com.br/noticia/crimes-eletronicos-podem-comprometer-o-crescimento-economico/28616. Acesso em: 26 ago. 13.

[10] http://www.cert.br/stats/incidentes/#2012. Acesso em: 03 set. 12.

[11] http://www.techlider.com.br/2010/07/sequestro-de-dados-e-cada-vez-mais-uma-realidade/. Acesso em: 06 set. 12.

[12] http://www.crimespelainternet.com.br/a-nova-arma-do-anonymous-contra-sites-e-voce/. Acesso em: 07 set. 12.

[13] http://www.bbc.co.uk/portuguese/videos_e_fotos/2013/03/130321_click_golpe_dg.shtml. Acesso em: 23 mar. 13.

[14] http://idgnow.com.br/internet/2013/07/02/a-cada-15-segundos-brasileiro-e-vitima-de-fraude-na-internet-diz-serasa/. Acesso em: 08 jul. 13.

[15] http://idgnow.com.br/internet/2013/01/23/quase-30-milhoes-de-brasileiros-entraram-no-facebook-em-2012/. Acesso em: 31 jan. 13.

[16] http://www1.folha.uol.com.br/tec/1179545-pornografia-infantil-domina-denuncias-de-crime-na-internet-no-brasil.shtml. Acesso em: 08 jan. 12.

[17] http://www.cetic.br/usuarios/kidsonline/2012/index.htm. Acesso em: 05 out. 12.

[18] http://www.estadao.com.br/noticias/impresso,professora-

universitaria-e-presa-por-pedofilia-,922506,0.htm. Acesso em: 06 out. 12.
[19] http://blogbr.ecglobal.com/comunidade-ecglobal/resultados-sexting-uma-ameaca-desconhecida/. Acesso em: 10 mai. 13.
[20] http://blog.telasamigas.com/2012/10/quase-todas-as-fotos-e-videos-de-sexting-acabam-em-sites-de-pornografia/. Acesso em: 10 mai. 13.
[21] http://www.emol.com/noticias/internacional/2012/10/12/564492/conmocion-en-canada-por-suicidio-de-joven-victima-de-bullying.html. Acesso em: 14 out. 12.
[22] http://www.crimespelainternet.com.br/traficante-e-preso-apos-postar-fotos-com-armas-em-rede-social/. Acesso em: 06 out. 12.
[23] http://fantastico.globo.com/Jornalismo/FANT/0,,MUL1610463-15605,00-SEQUESTRADORES+ESCOLHEM+VITIMAS+ATRAVES+DE+PERFIS+NA+INTERNET.html. Acesso em: 04 out. 12.
[24] Adolescente vítima de bullying na internet vai receber indenização por danos morais – Jornal Hoje – Catálogo de Vídeos. Acesso em: 05 out. 12.
[25] http://www.crimespelainternet.com.br/presidente-da-microcamp-e-vitima-de-crime-virtual/. Acesso em: 29 set. 12.
[26] http://www.passeiaki.com/noticias/cpi-para-investigar-minha-relacao-sexual-carlinhos-cachoeira-indaga-denise-leitao-rocha. Acesso em: 13 out. 12.
[27] http://www.crimespelainternet.com.br/mulheres-sao-maiores-vitimas-da-chamada-pornografia-da-vinganca-ou-vinganca-do-mouse/. Acesso em: 03 dez. 12.
[28] http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=110340. Acesso em: 08 jul. 13.
[29] http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=574247. Acesso em: 15 mai. 13.
[30] http://www.ebc.com.br/tecnologia/2012/10/denuncias-contra-perfis-e-postagens-preconceituosas-aumenta-em-periodo-eleitoral. Acesso em: 21 out. 12.
[31] http://www.crimespelainternet.com.br/justica-condena-estudante-preconceito-contra-nordestinos-twitter/. Acesso em: 16 set. 12.
[32] http://esporte.uol.com.br/futebol/campeonatos/paulista/ultimas-noticias/2012/03/25/tiros-barras-de-cano-e-pancadaria-em-posto-marcam-batalha-entre-corintianos-e-palmeirenses.htm. Acesso em: 30 set. 12.
[33] http://http://www.crimespelainternet.com.br/eleitores-cometem-crime-ao-postar-fotos-de-votacao-na-internet/. Acesso em: 21 out. 12.
[34] http://http://noticias.terra.com.br/educacao/enem. Acesso em: 03 nov. 12.

[35] http://g1.globo.com/brasil/noticia/2012/11/tj-sp-nega-recurso-condenado-por-vender-abortivo-na-internet.html. Acesso em: 19 nov. 12.
[36] http://noticias.r7.com/minas-gerais/justica-federal-aceita-denuncia-contra-neonazistas-presos-em-bh-06062013. Acesso em: 15 abr. 13.
[37] http://imirante.globo.com/imperatriz/noticias/2013/07/22/justica-federal-condena-25-galaticos.shtml. Acesso em: 27 jun. 13.
[38] http://www.crimespelainternet.com.br/crimes-de-odio-na-internet-sao-mais-comuns-no-brasil-afirma-especialistas-em-direito-eletronico/. Acesso em: 16 set. 12.
[39] http://www.crimespelainternet.com.br/no-brasil-16-dos-pcs-tem-protecao-zero-contra-ameacas-diz-estudo/. Acesso em: 10 nov. 12.
[40] http://idgnow.com.br/internet/2012/11/09/microsoft-anuncia-primeira-correcao-de-seguranca-para-windows-8-e-rt/. Acesso em: 09 nov. 12.
[41] http://idgnow.com.br/internet/2012/11/09/quase-25-dos-internautas-usam-browsers-desatualizados-e-correm-riscos/. Acesso em: 09 nov. 12.
[42] http://www.crimespelainternet.com.br//?s=ware&x=0&y=0. Acesso em: 10 nov. 12.
[43] http://revistawindows.com.br/noticias/firma-de-seguranca-lista-as-senhas-fracas-mais-comuns/. Acesso em: 11 nov. 12.
[44] http://www.nic.br/imprensa/releases/2012/rl-2012-26.htm. Acesso em: 14 nov. 12.
[45] http://www.institutotelecom.com.br/index.php?option=com_content&view=article&id=3905:crimes-na-web-bancos-responsabilizam-correntistas-por-acao-de-hackers&catid=1:latest-news&lang=pt. Acesso em: 24 nov. 12.
[46] http://info.abril.com.br/noticias/seguranca/virus-em-e-mail-aumentou-56-no-primeiro-semestre-25092012-38.shl. Acesso em: 01 fev. 12.
[47] http://www.crimespelainternet.com.br/encontro-marcado-pelainternet-acaba-em-desespero/. Acesso em: 19 nov. 12.

[48] http://oglobo.globo.com/rio/para-as-vitimas-crimes-na-internet-ainda-estao-longe-de-ter-castigo-merecido-6821835. Acesso em: 25 jan. 12.
[49] http://indicadores.safernet.org.br/. Acesso em: 22 jul. 13.
[50] http://www.mp.mg.gov.br/portal/public/interno/repositorio/id/3941. Acesso em: 10 fev. 12.
[51] http://www.crimespelainternet.com.br/homem-usou-um-perfil-falso-de-neymar-para-extorquir-um-juovem-de-23-anos-em-sc/. Acesso

em: 03 jan. 13.
[52] http://www.crimesinternet.com.br/3-1-como-se-chega-a-autoria-de-um-crime-na-internet/. Acesso em: 10 mar. 13.
[53] José Antonio Milagre - Consultor, professor, advogado e perito especializado em tecnologia e segurança da informação. Blog: josemilagre.com.br/blog, Facebook: http://www.facebook.com/josemilagre e Twitter@periciadigital.
[54] http://www.crimespelainternet.com.br/policia-civil-do-rn-extingue-nucleo-que-investigava-crimes-virtuais/. Acesso em: 28 jun. 13.