From the Editors of **Bottom Line Personal**

Stop Facebook from Spying on You

and Other Ways to Protect Your Online Privacy



Stop Facebook from Spying on You…

and Other Ways to Protect Your Online Privacy

From the Editors of *Bottom Line Personal*

BONUS:

As a thank you for buying *Stop Facebook from Spying on You…*
we have a Special Gift for you… click here for a **FREE** digital issue of

Bottom Line PERSONAL

A $5 value, it's yours absolutely ***FREE!***

Bottom Line PERSONAL is today's best personal magazine for money, health, consumer and lifestyle news, in a concise format designed just for you. With easy-to-use information from the country's best experts, you¹ll learn how to have greater wealth, better health, and more happiness in every area of your life.

Click here now to get this thank-you bonus FREE.



Stop Facebook from Spying on You

Six Ways Facebook Is Invading Your Privacy

Online Privacy and Theft Protection Q and A

How to Keep Your Movements, Your Purchases and Your Past Private

Beware of Invisible Stalkers

How to Stop Online Spies

This Tricky ID Scam Is Spreading

Cloud Hackers: Could They Steal Your Photos, Too?

Block Annoying Internet Ads

Best Privacy Defense When Using Wi-Fi

How Stores Are Spying on You

Protect Your Privacy at Work

Don’t Let the FBI Read Your E-Mail!

Ways to Block Unwanted Calls

How to Create the Best Password

The Safest Password Today

Take Charge of Your Medical Privacy

The Other Side of Health Privacy Laws

Copyright © 2015 by Boardroom® Inc.

All rights reserved. No part of this publication may be reproduced, scanned, distributed or transmitted in any form, by any means, electronic or mechanical, without permission in writing from the publisher.

Bottom Line Personal® publishes the advice of expert authorities in many fields. These opinions may at times conflict as there are often different approaches to solving problems. The use of this material is no substitute for health, legal, accounting or other professional services. Consult competent professionals for answers to your specific questions.

Telephone numbers, addresses, prices, offers and websites listed in this book are accurate at the time of publication, but they are subject to frequent change.

Bottom Line Personal® is an imprint of Boardroom® Inc., publisher of print periodicals, e-letters and books.

Bottom Line Personal® and Bottom Line Publications® are registered trademarks of Boardroom® Inc., 281 Tresser Boulevard, Stamford, CT 06901



Please let us know your thoughts on this Kindle book:

Click here to write a review.

Thanks for reading!

About Bottom Line Publications

For more than 40 years, Bottom Line Publications has provided millions of customers with practical answers to life's difficult questions by tapping our extensive network of leading experts in all areas of life. Whether you have a question about your health, your money, your career (or anything else), we provide the expert perspective that goes beyond the simple news that you'll find in other media outlets. Our bottom line is all about your bottom line—what you can do to solve your problems and how you can do it…today!

Through our *Bottom Line/Personal* publications, we help readers enjoy more wealth, better health, enriched personal relationships and greater happiness by providing easy-to-use, need-to-know information from the best experts and insiders in every area of your life.

Whether in print or online, via videos and more, Bottom Line's clear, concise answers make it easy for you and your loved ones to take action. Visit our website to learn more and to get a taste of what Bottom Line can do for you: http://www.BottomLinePersonal.com.

Six Ways Facebook Is Invading Your Privacy

A billion people worldwide use Facebook to share details of their lives with their friends. Trouble is, they also might be unintentionally divulging matters they consider private—to friends…coworkers, clients and employers…marketing companies…and even to competitors, scammers and identity thieves.

Six ways Facebook could be compromising your private information and how to protect yourself…

1. The new Timeline format exposes your old mistakes. Timeline, introduced in late 2011, makes it easy for people to search back through your old Facebook posts, something that was very difficult to do in the past. That could expose private matters and embarrassing photos that you've long since forgotten posting.

What to do: To hide Timeline posts that you do not wish to be public, hold the cursor over the post, click the pencil icon that appears in the upper-right corner, then click "Hide from Timeline" or "Delete."

2. Facebook apps steal personal details about you—even details that you specifically told Facebook you wished to keep private. Third-party apps are software applications available through Facebook but created by other companies. These include games and quizzes popular on Facebook such as *FarmVille* and *Words with Friends*, plus applications such as *Skype*, *TripAdvisor* and *Yelp*. Most Facebook apps are free—the companies that offer them make their money by harvesting personal details about users from their Facebook pages, then selling that information to advertisers.

Many apps collect only fairly innocuous information—such as age, hometown and gender—that probably is not secret. But others dig deep into Facebook data, even accessing information that you may have designated private, such as religious affiliation, political leanings and sexual orientation.

What to do: Read user agreements and privacy policies carefully to understand

what information you are agreeing to share before signing up for any app. The free Internet tool Privacyscore is one way to evaluate the privacy policies of the apps you currently use (www.Facebook.com/privacyscore). You also can tighten privacy settings by clicking the lock icon in the upper-right-hand corner. Select "See More Settings," then choose "Apps" from the left menu. Under "Apps You Use," click "Edit" to see your privacy options.

3. Facebook "like" buttons spy on you—even when you don't click on them. Each time you click a "like" button on a website, you broadcast your interest in a subject not just to your Facebook friends but also to Facebook and its advertising partners.

But if you're a Facebook user and you visit a web page that has a "like" button, Facebook will record that you visited that page even if you don't click "like." Facebook claims to keep web-browsing habits private, but there's no guarantee that the information won't get out.

What to do: One way to prevent Facebook from knowing where you go online is to set your web browser to block all cookies. Each browser has a different procedure for doing this, and you will have to reenter your user ID and password each time you visit certain websites.

Alternatively, to eliminate cookies created during a specific browser session, you can use the "InPrivate Browsing" mode (Internet Explorer), "Incognito" mode (Google Chrome) or "Private Browsing" mode (Firefox and Safari).

There also are free plug-ins to stop Facebook from tracking you, such as Facebook Blocker (www.Webgraph.com/resources/facebookblocker).

4. "Social readers" tell your Facebook friends too much about your reading habits. Some sites, including *The Washington Post* and *The Huffington Post*, offer "social reader" Facebook tools. If you sign up for one, it will tell your Facebook friends what articles you read on the site.

Problem: The tools don't share articles with your Facebook friends only when you click a "like" button—they share everything you read on the site.

What to do: If you've signed up for a social reader app, delete it. Click the lock

icon in the upper-right-hand corner, select “See More Settings,” then choose “Apps” on the left. Locate the app, click the “X” and follow the directions to delete.

5. Photo and video tags can hurt you. They could let others see you in unflattering and unprofessional situations. If you work for a straitlaced employer or with conservative clients or you are in the job market, you already may realize that it’s unwise to post pictures of yourself in unprofessional and possibly embarrassing situations. But you may fail to consider that pictures that other people post of you also can hurt you.

A Facebook feature called photo tags has dramatically increased this risk. The tags make it easy for Facebook users to identify by name the people in photos they post, then link these photos to the Facebook pages of all users pictured.

What to do: Untag yourself from unflattering photos. Hold your cursor over the post, and click the pencil icon. Select “Report/Remove Tag,” then follow the directions to remove the tag. Enable review of all future photos you’re tagged in before they appear on your Timeline. Click the lock icon in the upper right, then “See More Settings” and select “Timeline and Tagging.” Then click “Edit” next to “Review posts friends tag you in before they appear on your Timeline,” and click “Enabled” on the drop-down menu.

6. Your Facebook friends—and those friends’ friends—may reveal too much about you. Even if you’re careful not to provide sensitive information about yourself on Facebook, those details could be exposed by the company you keep.

Example: A 2009 Massachusetts Institute of Technology study found it was possible to determine with great accuracy whether a man was gay. This was based on factors such as the percentage of his Facebook friends who were openly gay—even if this man did not disclose his sexual orientation himself.

If several of your Facebook friends list a potentially risky or unhealthy activity, such as smoking or barhopping, among their interests—or include posts or pictures of themselves pursuing this interest—an insurer, college admissions officer, employer or potential employer might conclude that you likely enjoy this pursuit yourself.

What to do: Take a close look at the interests and activities mentioned by your Facebook friends. If more than a few of them discuss a dangerous hobby, glory in unprofessional behavior or are open about matters of sexual orientation or political or religious beliefs that you consider private, consider removing most or all of these people from your friends list or at least make your friends list private. Click your name in the upper right, then click “Friends,” then “Edit” and select “Only Me” from the drop-down menu.

Expert Source: John Sileo, president, The Sileo Group, a Denver-based identity theft prevention consulting and education provider that has worked with the Department of Defense, the Federal Reserve Bank and many other clients. He speaks internationally about online privacy, social-media exposure and digital reputation. He is author of *Privacy Means Profit: Prevent Identity Theft and Secure Your Bottom Line* (Wiley). www.Sileo.com

Online Privacy and Theft Protection Q and A

Identity theft expert John Sileo answers common questions about online privacy and theft protection…

Q: Is it safer to make bill payments through your online banking account versus logging in to the website of the company that is billing you to make payments? (Online banking can take up to seven to 10 days to process a payment, while a direct payment to a vendor's site is immediate.)

A: I prefer to log in to the bank and use its bill pay option. That way, only the bank has your information and when it sends out a check or ACH on your behalf, it is the bank's account number, not yours. But yes, you have to be a bit more prepared to do it.

Q: If someone hacks my e-mail address and sends spam to people in my address book, is it enough to just change my password, or should I obtain a totally new e-mail address?

A: This is a hard question, as that address has forever been tainted and will often trigger the junk mail feature on the accounts of your acquaintances. If it's not a ton of trouble (I know it is), change the account, otherwise, change the password to something longer than 13 characters, using alphanumeric characters and symbols. *Example:* Th3H1ll$areAl!v3 (The Hills Are Alive). Easy to remember, tough to crack.

Q: I heard that many smartphone apps, including many popular ones, actually have viruses embedded within them. How can I tell if an app is safe to download? What do I do to make sure my smartphone remains virus (and hacker) free?

A: Oftentimes they are apps that mimic the real ones but that intercept all of your private information. My rule of thumb is to only load what you absolutely need, only use the approved app store (e.g. Apple) and change the privacy settings in your mobile phone to restrict the apps access to your contacts, etc.

Q: Is it best not to shop at retailers that have announced they had breaches in security?

A: Actually, it's only after a retailer has had a breach that it starts to take the security precautions it should have taken in the first place. Over time, Target will be safer than most retailers. Isn't it ironic? That said, I am done with Target, at least with a credit card. It ended up losing data that was more than 10 years old—That's bad practice keeping that information around for so long.

Q: My daughter said someone gained access to her debit card account via her PayPal account. The bank had her file an "investigation" request and nothing more…shouldn't it change her account and/or her debit card before the person who has her information takes more money from her—while they investigate? I don't understand them not being more proactive to protect her money!

A: *Absolutely the bank should change her account!* If the bank doesn't do that, find another bank. The chances of someone breaching the account again are very high.

Q: I want to discontinue my Facebook account. How do I unsubscribe?

A: That is probably the most popular question I get these days, and I show you how to do it (without shooting yourself in the foot) here: http://www.sileo.com/how-do-i-delete-my-facebook-account/. 1. Backup your data. 2. Deactivate your account for a week or two first to see if you really want to live without it. 3. Alert your friends if you do decide to permanently delete your account. The intention is to protect your privacy, not anger your friends. 4. Delete your account.

Q: What is the "safest" web browser and which do you use?

A: I use two separate browsers—one for private and one for public. For private, I have built a much more secure browser using Firefox. There are a bunch of items you can lock down on a browser to make it safer. But, of course, performance suffers. So, when I'm browsing non-private stuff like sports I use my regular browser (Chrome). And when I go to my bank or other financial company websites, I use my protected Firefox browser.

Q: I've been reading about bitcoins. Is it a legitimate currency? Would you recommend using them?

A: While there are a lot of supporters of bitcoins (mostly drug users and criminals who want to launder money), I am not one of them. Remember when they said that Cabbage Patch Kids would be worth a fortune in 10 years (or Pet Rocks, or Furbies)? Well, the bitcoin will be worth about as much.

Q: Can you give us some of the best ways we can protect ourselves from identity theft?

A: Some of the most popular suggestions from my book, *Privacy Means Profit* (Wiley), include freezing your credit (more here: http://www.sileo.com/2) and opting out of junk mail (http://www.sileo.com/1). I also recommend you take your Social Security card out of your purse or wallet and only take it when you need it.

Q: I've heard about web browsers such as Tor that would allow me to browse the web anonymously—and more securely. Are there different risks to my computer's security than if I were to use a traditional browser such as Safari or Google Chrome?

A: Tor is actually not a browser, but a program that hides your IP address (makes it look like it's coming from another country). This is great for people who want to avoid the Great Firewall of China or to mask their behavior (usually Spamming), but it does little to keep you anonymous. For that, I like the software Cocoon or www.getcocoon.com.

Q: I've heard that some US credit card issuers are thinking of switching from the traditional swipe-and-sign cards to the chip-and-pin technology that is common in Europe and Asia. Would this improve security?

A: Yes, and let's hope they do switch. By no means is it a perfect technology, but in the first five years in Britain, it lowered credit card fraud by more than 70%. You see, it's so easy to replicate the magnetic strip on the back of the card, but much harder to clone a digital chip and also have the PIN or password. I am totally behind this technology.

Q: I've been hearing about apps to transfer money quickly and easily such as *Venmo*. Are these services safe? If not, what is the most secure way to transfer money to friends or family members?

A: I do not use my mobile phone or iPad for any financial transactions at this point, as they are so compromised by rogue apps. I use the old fashioned method and get on my laptop or give the bank a call. Much more work, but much safer. In two to three years, these apps will be safe because the mobile operating systems will have done a better job locking down the important apps and locking out the rogue apps.

Q: When I enter a commerce site on my computer these days, the browser, or perhaps my computer, asks me if I would like to save my password, so that the next time I visit the site from the same computer device, I will not have to enter it. I normally answer no. Is it safe to answer yes?

A: I don't like to use the password keychains, as they are called, that are in the browser. They are so easy to hack. I prefer to use a program like 1Password so that they are well encrypted, and so that you are forced to use long, strong and varied passwords.

One question that hasn't come up that is so important is how to keep hackers out of your online accounts (bank, investment, dropbox, Gmail, etc.). There is a simple answer called two-factor authentication (it's not as scary as it sounds), and you can watch a quick video on how it works here: http://www.sileo.com/two-factor-authentication/.

Expert Source: John Sileo, president, The Sileo Group, a Denver-based identity theft prevention consulting and education provider that has worked with the Department of Defense, the Federal Reserve Bank and many other clients. He speaks internationally about online privacy, social-media exposure and digital reputation. He is author of *Privacy Means Profit: Prevent Identity Theft and Secure Your Bottom Line* (Wiley). www.Sileo.com

How to Keep Your Movements, Your Purchases and Your Past Private

People have the right to hide their pasts—as long as they are European. That essentially was the ruling of the European Union's highest court in May 2014, which said Google must grant requests by individuals to delete certain links to information about themselves. However, even people in Europe will continue to find it difficult to hide in an increasingly exposed world.

Much of our private personal lives—including embarrassing remnants of the past, our spending habits, even our location at any given time—will continue to be available for corporations, the government, former spouses, our neighbors, scammers, stalkers and anyone else to uncover.

But there are steps you can take to reduce their ability to invade your privacy. *Here, Frank Ahearn, an expert on hiding, describes some of those methods…*

Hide Your Past

Even an honest, respectable person may have something in his/her past that he would prefer to keep private. For some, it's an old relationship…for others, an ill-considered comment in a speech or to a reporter…or even an old arrest for an embarrassing infraction. An employer who learns of someone's past mistake might decide not to hire or promote the person…a civic organization might decide not to accept or affiliate with the person…even new neighbors might be wary. Unfortunately, the Internet can prevent our old mistakes from ever fading away. You could ask a website to take down private details from your past, but the site might not agree to do so, and even if it does, the information might just pop up elsewhere on the Internet. The truth is that there is no realistic way to completely erase information from the Internet. To really protect yourself from your past, you might have to take somewhat extreme measures.

What to do: If you cannot make troubling information disappear, make it appear that the information is not about you. To do this, you create an imaginary person who has the same name as you. You set up phony Facebook and LinkedIn pages

for this person and perhaps a blog as well. Include details that strongly link this person to the event from your past that you wish to escape. Use keywords on these pages that someone is likely to search for if that pursuer wants to know more about you.

Example: If you're trying to hide the fact that you belonged to an extreme political movement back in college, use the name of that political movement prominently in the fake person's Facebook and LinkedIn pages. Add personal details that clearly establish that this fake person is not you. (Don't add a fake photo—you could get sued for using a stranger's photo without permission, and modern technology makes it possible for people to figure out that the photo is of someone with a different name.) Set the privacy settings as low as possible on these social-media pages so that anyone can access them.

Meanwhile, remove any details from your own social-media pages and blogs that connect you to the old misstep. Employers or acquaintances who stumble upon the misstep likely will conclude that you weren't the one who was involved. This technique can be effective as long as the troubling information mentions only your name and perhaps your hometown but does not include a photo of you or mention something that clearly establishes that it was you.

Real-life example: A very successful Wall Street banker appeared in a tasteless low-budget movie many decades ago. To hide this fact, he created social-media pages for an imaginary man in Cincinnati who shared his name and had this fake man brag about an interest in porn and the movie role. If people watch this old movie, they might recognize the banker, but if they just stumble across a cast list and do some digging online, they might conclude it is someone else.

Hide Your Spending

Your spending is being watched. Retailers sell information about what you buy to data-tracking companies, which in turn sell reports about your purchasing history and habits. Insurance companies might use the information to check whether you have healthy habits—and raise your premiums or deny coverage if you don't. An employer might use it to keep tabs on your behavior. Most people consider this a serious invasion of privacy.

What to do: Wherever you shop, pay in cash or with prepaid gift cards, which can be purchased anonymously at many major retail, supermarket and pharmacy chains. Some of these prepaid cards are good only with a specific retail or restaurant chain or a website such as Amazon.com, while others, such as those issued by Visa, MasterCard and American Express, are good wherever debit cards are accepted.

Hide Your Location

In TV shows such as *NCIS* and movies such as the Bourne films, bad guys—and good guys—often are tracked down through their cell phones.

This is possible and common in real life, too. Law-enforcement agencies and even high-tech criminals increasingly have the ability to track people using their cell phones. Cell towers keep track of where we are, and many smartphone apps do so, too. They even can track phones that are turned off.

What to do: Use a very inexpensive so-called "burner" phone and prepaid cell-phone service. The phones cost as little as $15. These can be obtained without a contract—and even without a requirement that you provide your name and Social Security number. That makes it harder for anyone to track you, especially if you pay with cash. These phones can be bought at retail chains such as Target and Walmart along with prepaid talk "minutes."

If you are willing to pay for even greater cellular privacy, dispose of your burner phone and purchase a new one each time you use it to speak to a friend or relative, as in the TV shows and movies. Otherwise, someone tracking the friend's or relative's phone records might figure out that the prepaid phone belongs to you and use it to track you.

Hide Your Online Activities

The things you do on the Internet reveal more about you than you might realize. If a con man learns what topics you research online, he could pretend to have similar interests to get close to you. If he learns what clubs you belong to, he can check when those clubs meet to determine where to bump into you…or when your home might be vacant and easier to rob.

What to do: Stop reporting details about your life online. Do not post anything on social-media pages or blogs that you wouldn't feel comfortable putting on a billboard. Ask family members and friends to not include your name or photo on their pages, either.

Consider falsifying your hometown on your social-media pages and/or blog. Once someone has your name and hometown, it's usually fairly easy for him to find your phone number, address and much more through a site such as ZabaSearch.com.

If you wish to keep certain Internet activity truly private, buy a low-end laptop or tablet for only this purpose and connect to the Internet using public Wi-Fi, not your home network. Do not save personal files on this device…do not access your e-mail with it…and never access your home Internet service with it or enter your name into it for any reason. If you visit a website that requires you to register, use a fake name.

Also: Never include private information in e-mails. E-mail messages are never 100% secure, and you never can be certain that they are truly gone after you delete them. There are "private e-mail" services that claim to keep e-mail messages secure, but they're often not as secure as they claim and these services frequently go out of business—taking clients' e-mail addresses and old messages with them. Besides, even if you use the world's most secure e-mail service, there is no guarantee that the recipients of your e-mail messages will keep your e-mails secure. Secure texting apps such as *Wickr* provide additional security for text messages, but even with these, texts aren't 100% secure.

How to Totally Disappear

If you wish to truly disappear, perhaps to evade a dangerous person who is trying to find you…

Before relocating, leave a false trail leading somewhere you have no intention of hiding. Use your computer to search for information about a city where you have a trusted friend. Apply to rent an apartment in this city (don't actually rent one), and open a bank account there. Give the bank your current mailing address, which you will soon leave. Deposit a few hundred dollars in

this account, then take the debit card that the bank gives you and give it to a friend with instructions to use it to make occasional small purchases. Close the account when these funds are depleted. If someone skilled at finding people is tracking you, he will try to access your credit report and your computer's search history for clues about where you went. If you feed him fake clues, you could keep him busy looking in the wrong place. (The friend should not be in any danger, because this searcher is looking for someone who looks like you.)

Set up a shell company. For less than $1,000, you can set up a company that cannot easily be connected to you. This company can pay your bills and rent you an apartment. Speak with a CPA or tax attorney about the potential tax consequences of forming a business.

Helpful: Wyoming Corporate Services, Inc., and Companies Incorporated are two services that set up shell companies.

Warn friends and family members not to give away your location. Professional pursuers who may be looking for you know how to trick your loved ones into divulging your whereabouts.

Corrupt the information that utility companies have on file for you. People who find people for a living sometimes do so by gaining access (illegally) to utility-company records. Visit your utility's website or call to "correct" your name to something slightly inaccurate—replace your first name with your middle name, for example, or adjust your last name slightly.

Use Internet message boards to communicate with friends and family. Plant a coded message on a specific site when you need to get in touch.

Example: You might tell your most trusted family member to place an ad for a 1999 gold Chevy Silverado on the Kansas City Craigslist site when this person needs you to call. Set a high asking price to cut down on would-be buyers who call. The phone number listed in this ad should be for a new prepaid cell phone.

Expert Source: Frank Ahearn, a consultant who helps people disappear. He previously worked as a "skip tracer," helping private detectives, investigators and attorneys track down people in hiding. He is author of several books about hiding and privacy, including *How to Disappear* (Lyons) and *How to Disappear from BIG BROTHER* (CreateSpace). He does not reveal his location. www.FrankAhearn.com

Beware of Invisible Stalkers

Identity thieves aren't the only prying eyes on the Internet. Mainstream websites and their advertising partners track our digital doings as well. Some of this tracking is innocent and even beneficial—for example, an Internet merchant might record which items we browse so that it can suggest related products the next time we visit. Unfortunately, online tracking can cross the line from welcome feature to worrisome invasion of privacy. Sites often sell information about us to other companies…install tracking files onto our computers without our permission…and allow ad-tracking companies to lurk unseen on their sites, gathering information about us.

Who's Doing It

It isn't just shopping sites that are tracking us. Media companies sell information about which articles we read online. Charities sell information about the causes we seem interested in. Even government sites might share information about visitors.

Example: A man who registered to visit the Grand Canyon on the National Park Service site was immediately deluged with advertisements from companies selling hiking gear.

Much of this information is recorded, analyzed and shared with anyone willing to pay for it, all without our consent. If it falls into the wrong hands, such data potentially could be used for ID theft. Even if that doesn't happen, it's likely to be used to determine whether we are approved for loans and insurance and to target us with solicitations designed to take advantage of our opinions and weaknesses.

Examples: If we visit the site of a political organization or charity, disreputable companies that want our business might portray themselves as sympathetic to this cause in the online ads we see, even if they are not. If you buy a book from an Internet merchant about overcoming gambling addiction, you might receive a flood of ads from poker websites.

The sharing of our private data also could cause us embarrassment if a friend or family member who uses our computer sees that we receive an unusually large number of ads for dating sites, debt-reduction services or treatments for potentially embarrassing health conditions.

What to Do

There are many ways to make your online activities more private. Some are complex, expensive or inconvenient—but there are some simple, free online privacy options that most Internet users find worth the trouble…

1. Make an intermediate stop at Yahoo.com. Generally, each website we visit knows which site we were visiting before we dropped in and which site we head to when we leave. Unfortunately, a disreputable site could use this information for nefarious purposes. What we can do to help prevent this is visit a safe, innocuous site such as Yahoo.com both before and after we visit any site that we would prefer to keep private, such as the site of a financial company with which we do business. The fact that we visit Yahoo.com tells others almost nothing about us.

2. Use an ad-tracker tracker. These programs don't stop the online spies, but they do warn us when we are being watched by them, so you can make an informed decision regarding whether you want to visit certain sites.

Example: TrackerScan is available for free at www.PrivacyChoice.org/trackerscan.

3. Opt out of ad tracking. Many online advertisers and companies that sell data to online advertisers allow Internet users to opt out of Internet tracking by signing up with opt-out services.

Examples: Opt-out services include www.AboutAds.info… www.PrivacyChoice.org… and www.NetworkAdvertising.org.

Also, several Web browsers, including Mozilla Firefox and Google Chrome, are beginning to offer users ways to permanently opt out of ad tracking. However, less ethical advertisers do not participate in these opt-out programs.

4. Periodically clear your cookie cache. Cookies are computer files stored by websites on our computers that remind the sites who we are when we return or that track our movements around the Internet. As a result, marketers may know more about us than we want to share. We can delete most of these cookies from our computers in a few simple steps—but be aware that doing so will cause some sites to lose information that we want them to have. We might have to retype passwords, mailing addresses, user profiles and other information the next time we visit. *Examples of how to clear your cookies…* *

In Internet Explorer 8: Select "Internet Options" from the "Tools" menu, select the "General" tab, then click "Delete." Next, select "Cookies," then click "Delete" again.

In Mozilla Firefox: Select "Options" from the "Tools" menu, click "Privacy," then "Show Cookies," followed by "Remove All Cookies."

5. Adjust your browser settings for greater privacy. In addition to deleting the cookies that already are on our computers, we can instruct our browsers to permit fewer cookies in the future.

Most browsers also have a "Private Browsing" option (Internet Explorer calls it "InPrivate Browsing") for when we want our browsing to be especially private.

6. Avoid sites that do a poor job protecting user privacy. Don't use a site if its "Privacy Policy" or "Privacy Terms" states that information about you can be shared with third parties. Avoid a site if a security-rating program, such as MacAfee's *SiteAdvisor*, warns you that the site could expose your computer to malicious software, which could put your personal information at high risk. For a free version of MacAfee's *SiteAdvisor*, go to www.SiteAdvisor.com.

**For more details on removing cookies and adjusting privacy settings on various browsers, see your browser's "Help" file.*

Expert Source: Linda Criddle, president, Safe Internet Alliance, a nonprofit group that encourages websites to improve user privacy, Kirkland, Washington. She also is president of LookBothWays Inc., an online safety software and consulting company that works with corporations and law-enforcement agencies. She previously spent 13 years with Microsoft as an online safety expert. www.ilookbothways.com

How to Stop Online Spies

It is not a secret that your online activity is not very private. Cyber criminals and government agencies have ways of reading your e-mails and discovering where you go on the Internet. websites you visit can figure out who you are, where you live and what your interests are, then sell that information to marketing companies or anyone else who wants to know. *Two of the latest options for improving online privacy…*

• **Safeplug.** This device keeps your Internet activity private. Plug Safeplug ($49, PogoPlug.com/safeplug) into your Internet router, and it can conceal your IP address—a unique number that can be used to identify your computer. It also can route your Internet traffic through random computers around the globe, making it extremely difficult for high-tech snoops to figure out where you live.

This added security can slow down your Internet speeds, however, sometimes noticeably. Consider loading more than one web browser onto your computer—both Chrome and Firefox, perhaps—and activating Safeplug with only one of these. Use the browser that is not Safeplug-enabled when fast Internet speeds are more important than privacy, such as when streaming a movie from Netflix or another reputable site.

• **ShazzleMail.** This service keeps your e-mails private. When you send a regular e-mail, your e-mail provider stores a copy of the message on its computers. Those stored messages could later be read by a government agency or a cyber criminal who hacks the e-mail provider's system. Your e-mail provider itself might examine your e-mails in order to target advertisements to your interests. You would never tolerate eavesdropping on your phone calls—but that's what this is like.

ShazzleMail lets you send e-mails from your smartphone or tablet to your e-mail recipients. These messages are never stored on an e-mail provider's computers, increasing the odds that they will remain private (free, iOS or Android, *ShazzleMail.com*). You have to use a special ShazzleMail e-mail address to send these messages, however, and using this service won't keep your e-mails secure if a criminal has loaded spyware onto your device or onto the phone or computer

of the person who receives the message. ShazzleMail works best if both sender and recipient have ShazzleMail accounts. You can send messages to non-ShazzleMail users, too, but they will have to take a few extra steps to access them.

Expert Source: Robert Siciliano, security analyst, CEO, IDTheftSecurity.com. He has more than 30 years of experience in cyber- and real-world security and is author of *99 Things You Wish You Knew Before…Your Identity Was Stolen* (99 Series). www.RobertSiciliano.com

This Tricky ID Scam Is Spreading

Scammers have become proficient at stealing just a little piece of your identity and using that to create a fake person to buy things. The crime, called "synthetic" identity theft, now accounts for more than 80% of the 16 million identity-theft cases in the US, according to the federal government.

How it works: Instead of stealing your basic credit card information and posing as you to run up charges on your credit card, thieves steal a sliver of your ID, typically your Social Security number, and combine that information with another person's name or a fake name, a phone number and an address they can access. Remarkably, many of the applications with mismatched information slip past the credit bureaus and credit card providers. This is partly because Social Security numbers are not meant to be universal identifiers, though they often are used that way. Sometimes scammers even use the new ID to get a job, which further enhances their ability to get credit. And you don't realize what has happened to your ID information, because nothing unusual shows up on your statements.

When creditors eventually do investigate because the scammer stops paying the credit card bills for a prolonged period, some of the identifying information gets traced back to you. While you won't be responsible for the financial losses, creditors still may freeze your credit accounts and/or add negative marks to your credit rating until they determine that you are an innocent victim.

Self-defense: Make sure that your reported income on your annual Social Security statement for the year is not overinflated, and monitor your credit reports for any unauthorized accounts.

Expert Source: Andrew Gerry, senior vice president of operations for the identity risk management company Intersections Inc., Chantilly, Virginia. www.Intersections.com

Cloud Hackers: Could They Steal *Your* Photos, Too?

Few people seem to fully understand "the cloud," yet hundreds of millions of people use it to store their digital photos, videos, e-mail and other data in cyberspace. *The appeal:* You effortlessly create a backup in case your smartphone is lost or your computer crashes…you free up storage space on all your devices…and you can access the data from almost anywhere. However, the publication of nude celebrity photos obtained by hackers from Apple's iCloud put a spotlight on the vulnerabilities of cloud storage. *Strategies to safeguard your cloud storage…*

Turn off automatic backup. Many cloud services come with a convenient feature that automatically sends every photo and video you create to the cloud. If you don't want to take a chance of these files being hacked and distributed on the Internet, disable the backup feature. For step-by-step directions, go to the following support pages for the four major cloud providers: For Apple, Apple.com/support…for Google, Support.Google.com…for Amazon, Amazon.com/clouddrive…for Dropbox, Dropbox.com/help. (Or go to "Support" for any other cloud service you use.)

Look at your files that already are stored in the cloud—and delete sensitive ones. Deleting these files from your smartphone, tablet and/or computer does not necessarily remove them from your cloud account. Go to your cloud account, and delete such files directly there.

Store and back up your most confidential files off-line. Save these items to one or more portable USB flash drives in your home and/or place of business. Then delete the files from your computer's hard drive so that the data can't be accessed over the Internet.

Use a stronger password and two-step verification, which requires not just your password to access your accounts but also a special onetime-only code that is sent to your phone each time you log on.

Expert Source: John Sileo, president, The Sileo Group, a Denver-based identity theft prevention consulting

and education provider that has worked with the Department of Defense, the Federal Reserve Bank and many other clients. He speaks internationally about online privacy, social-media exposure and digital reputation. He is author of *Privacy Means Profit: Prevent Identity Theft and Secure Your Bottom Line* (Wiley). www.Sileo.com

Block Annoying Internet Ads

Internet advertising can be invasive and annoying. Some ads suddenly expand in size, blocking the Web page we're reading. Others blast audio messages without warning. Pop-up ads appear in new windows that we are forced to close. And "targeted" ads follow us around the Internet pushing products related to topics that we previously looked into online—an invasion of privacy that many people find creepy.

Web browsers have settings that allow us to opt out of targeted ads, but these settings tend to be confusing to use and not especially effective.

Better ways to block annoying Internet ads…

1. Download *AdBlock Plus.* This free "browser extension" prevents the vast majority of invasive, annoying Internet ads from appearing on your computer screen. Many, but not all, of the relatively unobtrusive ads that don't move, make noise or otherwise disrupt still will appear, though you can eliminate these, too, by adjusting the settings in *AdBlock Plus's* "Filter preferences" or "Options" menu. *AdBlock Plus* isn't the only ad blocker available, but it's probably the most effective and easiest to use—just click a button or two to install it, and it will do the rest. AdBlockPlus.org

Important: Ad-blocking filters also may block some pop-up videos, coupons and other features you do want to see. *Adblock Plus* adds an icon to the browser that a user can click to adjust the filtering rules for any particular website or advertiser.

2. Install a tracking blocker, such as *DoNotTrackMe*. *AdBlock Plus* has a "Disable Tracking" feature that stops advertisers from following what we do online. But if you want to ensure that Internet-ad-tracking companies aren't watching you, also download a browser extension designed specifically for this purpose. *DoNotTrackMe* (www.Abine.com) is effective, easy to use and free.

Other tracking blockers such as *Disconnect* (www.Disconnect.me) and *Ghostery* (www.Ghostery.com) also are effective, but there's no need to install more than

one.

Alternative: An even easier way to stop advertisers from tracking you is to click the turquoise triangle found in the upper-right-hand corner of certain Internet ads. Clicking this "AdChoices" icon calls up a Web page explaining how to opt out of tracking. You have to do this only once, not every time an ad appears. But don't expect this to eliminate all targeted ads. Unlike *DoNotTrackMe*, *AdChoices* will prevent tracking only by companies that have voluntarily agreed to participate in the industry's self-regulation efforts.

3. Opt out of mass e-mailings of ads sent by legitimate businesses. Ads that flood our e-mail in-baskets often claim that we can opt out of future mailings by clicking an "unsubscribe" link, likely found at the end of the message.

If the e-mail in question was sent by a legitimate company that you have done business with in the past, clicking this link likely will head off that company's future ads as promised. But do not click opt-out links in e-mails sent by companies that you do not know and trust. Doing so is likely to result in more e-mail ads, not fewer.

Expert Source: John R. Levine, PhD, founder, Taughannock Networks, an Internet infrastructure consulting company, and president, CAUCE, an Internet user advocacy organization, Trumansburg, New York. He is coauthor of *The Internet for Dummies* (For Dummies). www.JohnLevine.com

Best Privacy Defense When Using Wi-Fi

It’s important to make sure you are protected when using Wi-Fi.

How: Make sure that you have two-step verification enabled (for directions, search for “two-step verification” and the service you want to use, such as Google or Facebook). This means that signing into an account will require two forms of identity verification—usually a password you create and a code sent to you through a text message or with a special app. So, even if your user name and password are stolen, the thieves cannot get to your account because they will not receive the additional required code.

For the system to work properly, you need separate sign-ins and passwords for every online account and need to enable two-step authorization for all of them. Since this may significantly increase the number of passwords you have, consider using a password manager such as *1Password* or *LastPass*.

Source: *The New York Times*

How Stores Are Spying on You

Retailers keep track of shoppers' returns. *How*: They track individual shoppers by name—not just returns in general. Best Buy, J.C. Penney, Victoria's Secret, The Home Depot, Nike and other stores maintain return-tracking databases.

Retailers say they need the databases to fight theft and fraud. But consumer advocates say that the databases—whose existence often is not disclosed by retailers—invade consumer privacy.

To see what return information retailers have on you: Request a free copy of your Return Activity Report from TheRetailEquation.com.

Source: Round-up of experts in retailers' data practices and consumer protection, reported in *USA Today*.

Protect Your Privacy at Work

They can read our e-mails, listen to our phone calls, watch us through hidden cameras, track our movements and monitor our Facebook pages—all legally. They are not federal agents from the National Security Agency—they are our employers.

Few Americans are aware that their bosses have wide-ranging rights to look into their lives. The rapidly dropping cost of high-tech surveillance equipment, including digital cameras and GPS technology, has made such prying increasingly common.

Your E-mail and Text Messages

Any e-mail sent through your employer's computer network can be read by your boss—including not only messages in your work e-mail account but also messages in your personal e-mail accounts if you use your employer's network to send or receive them. This includes messages on your own personal laptop, tablet computer or smartphone.

The e-mails most likely to be examined are those containing words that often are used in a sexual context. Many employers use computer programs that call such messages to their attention so that they can stop workplace sexual harassment before it leads to a lawsuit. But the same keywords that appear in sexual harassment e-mails also can turn up in very private messages between sexual partners or in messages about sensitive medical matters.

Employers have a right to read text and e-mail messages sent from company-owned cell phones, smartphones and laptops, too, even if those messages are sent through personal e-mail accounts from outside the workplace. Employers can't easily monitor such messages as they are sent, but they can be uncovered later when the device is returned to the IT department for repairs or upgrade.

What to do: If you must send a private e-mail or text from the workplace, do so through your own mobile computer or cell phone…and if this device is capable of operating over both Wi-Fi and a cellular network, confirm that it currently is

accessing the cellular network, not company Wi-Fi. If you must use a company cell phone to send a private message, opt for calling the person rather than texting or e-mailing. That makes it much less likely that the company will learn the content of the message, though the company could determine what person or place you called.

Your Online Activity

Most employees realize that their employers can monitor their Internet use when they're in the office. And most job applicants understand that many potential employers now evaluate applicants' Facebook pages, blogs and other Internet postings. But some employers go even further, monitoring Internet content by and about their current employees—and occasionally firing those whose personal lives or opinions the employer considers offensive or unprofessional.

Examples: Employees have been fired for posting pictures of themselves holding a beer at a party…or wearing a bikini on a beach while on vacation. One employee was fired for expressing opinions about the Iraq war that ran counter to his employer's views.

In most states, an employer can legally fire an employee for nearly any reason, aside from reasons that are specifically prohibited by federal law (such as race, religion, sex, national origin, age or disability)…by collective bargaining agreements…or by civil service protections for government employees. Apart from laws prohibiting employers from firing employees for smoking, only California, Colorado, Montana, New York and North Dakota have laws restricting the ability of employers to fire employees for legal off-duty activities and statements.

Employers even can require employees to provide their social-media passwords to facilitate their snooping, though some states have begun passing laws to prohibit this.

What to do: Do not post anything online that you would not be comfortable saying or doing in the office. Discourage your friends and relatives from posting pictures of you doing these things as well. Even if your current employer does not monitor your online life, there's a good chance that it will be examined the

next time you apply for a job.

Tracking Your Movements

If you have a company car or company cell phone, your employer could be tracking your movements—even during your free time.

It's common and reasonable for employers to install GPS in company vehicles to make sure that their salespeople and delivery people are where they're supposed to be during the workday. But nothing legally prevents employers from also tracking company vehicles during nonworking hours to learn where employees go in their spare time.

Modern cell phones have GPS capabilities, too. For as little as $5 per phone per month, an employer can obtain a service that will use this GPS to track employees' movements.

A company might monitor how late an employee stays out on weekends, how often he/she visits bars or whether he's having an affair with a coworker.

What to do: If you don't want your employer to know about your activities outside the office, leave your company car at home or at least park it several blocks from destinations that you hope to keep private. Leave the company cell phone home.

Cameras, Laptops, Phones

Some of the following types of snooping are not as common, but it may just be a matter of time before they catch on with employers…

Digital video camera surveillance. Although the cameras are present in many workplaces as security devices, employees often don't realize that they're being observed or recorded. These aren't the obvious security cameras of old—a modern digital camera can be easily concealed. Courts generally have ruled that employers have the right to record video of their workers and workplaces, though usually not in employee bathrooms or locker rooms.

Example: The Massachusetts Supreme Court ruled that an employer was within his rights to take videos of a female employee who regularly changed into gym clothes in her cubicle after everyone else had left for the day.

Laptop surveillance. If you have a company laptop, your employer—or a rogue employee in your employer's IT department—could activate that laptop's Webcam and spy on you, possibly with no obvious sign that the camera is active. We don't yet have evidence of an employer doing this, but it was done with laptops issued to students by a Pennsylvania high school.

Audio surveillance. In most states, employers can place hidden audio recording devices in their workplaces, too, though a state law might require them to disclose to employees that they have done so.

These listening devices generally must be confined to parts of the workplace where conversations are predominantly work-related, so they typically can't be used in cafeterias, break rooms or bathrooms.

Companies can and do monitor and record employee phone conversations, however. By federal law, they must disclose that calls are being recorded. Federal laws also require them to stop listening if it becomes clear that a call is not work-related—but don't count on this rule to protect your privacy.

Employees can't know for sure that their employers are hanging up on personal calls, and employees legally can be disciplined if the call violates employer restrictions limiting personal use of the phone.

Companies legally can monitor calls made on company-owned cell phones as well, but in practice, this is difficult for them to do.

What to do: Do not do anything in your workplace that you would not want your employer to see, even if no one else is around. If you must do something private in the workplace, the bathroom or locker room is the spot least likely to be under observation. Do not say anything on an office phone that you wouldn't want your employer to hear. If you must make a private call, do so from a cell phone —ideally your personal cell phone. If you have a company laptop, turn it off or at least close it when it's not in use. If you never use your company laptop's Webcam, cover it with a piece of tape.

Expert Source: Lewis Maltby, JD, president, National Workrights Institute, a not-for-profit organization that researches and advocates on issues related to employee rights. Maltby previously served as general counsel of Drexelbrook Engineering Company and as director of employment rights with the American Civil Liberties Union. He has testified before Congress on employment issues. www.Workrights.us

Don’t Let the FBI Read Your E-Mail!

FBI officials can read messages that are more than six months old without a warrant.

To protect your messages: You can encrypt them before sending them if your e-mail provider allows this, but the recipient must have your encryption key to read the message.

Alternative: Delete older e-mails regularly. Or store them on your hard drive, which is protected by the Fourth Amendment (the right to avoid unreasonable search and seizure).

Also: Consider an e-mail service that uses servers based outside the US. Offshore e-mails are not subject to the same rules as ones within the US. But other countries have their own privacy rules—be sure you know them. And access through offshore servers may be slower than access through domestic e-mail providers.

Source: MarketWatch.com

Ways to Block Unwanted Calls

Signing up for the federal government's Do Not Call Registry was supposed to protect us from unwanted telemarketing phone calls. But a lot of unwanted calls still sneak through, and it's only getting worse. Inexpensive international Internet-based calling allows telemarketers to evade US laws by contacting us from overseas. And certain callers, including pollsters, politicians and charities, are exempt from the National Do Not Call Registry restrictions.

You still should register your landline and cell-phone numbers with the Do Not Call Registry (DoNotCall.gov) because it does reduce unwanted calls. *But here are four additional steps to further block these calls…*

Stop writing your phone numbers on forms and entering them into websites. Retailers, websites, charities and political organizations often ask for phone numbers, but that doesn't mean you have to provide them. Handing out phone numbers to such organizations increases the odds that the numbers will end up on additional call lists. An e-mail address should be sufficient when contact information is needed.

When a website won't let you proceed without entering a phone number, supply a fake one starting with "555" after the area code. (No real numbers start with 555.)

Exceptions: Do provide your real phone number(s) to doctors' offices, insurers, credit card providers and other organizations that might have a legitimate reason to contact you quickly.

Sign up for Nomorobo—if your telecom provider is eligible. This is a free service that recently won the top prize from the Federal Trade Commission for coming up with a technological solution to reduce the number of robocalls.

Incoming calls to your phone number are routed not just to your phone but also to Nomorobo's computers. These computers very quickly determine whether the call is from an automatic dialer—a tool used by many of the worst telemarketers to call several numbers quickly—and hang up on the caller after the first ring if

it is.

Nomorobo does allow legitimate automated phone calls through, such as reminders about doctor and other appointments.

Unfortunately, you can use Nomorobo only if your phone provider and/or cellular provider offers a service called “simultaneous ring,” which allows calls to one phone number to ring at a second number as well.

Most Internet- or cable-based telecom providers offer Nomorobo, but many cellular and traditional landline providers currently do not—though that could change if Nomorobo continues to gain popularity. At Nomorobo.com, click “Get Started Now” to determine whether you can sign up.

Block calls from troublesome phone numbers. Some telecom providers allow their customers to block incoming calls from specific numbers, perhaps by entering a code immediately after receiving a call from someone you don’t want to hear from again. Contact your provider(s) to see if such a feature is available to you.

Unfortunately, blocking individual phone numbers won’t stop the most unethical telemarketers—they tend to use “spoofing” technology to make their calls appear to come from a different phone number each time.

Because of this limitation, it’s usually worth blocking individual numbers only if your phone provider lets you do so for free.

Also: Some telemarketers block their own numbers so they don’t appear on your caller ID at all. Some phone-service providers offer the option of blocking incoming calls from callers that have blocked numbers—ask your provider.

Ask legitimate organizations to put you on their do-not-call list. Pollsters, politicians and companies that place unsolicited calls generally are required to maintain their own do-not-call lists. Ethical organizations comply with requests to be placed on these lists.

Exception: Prerecorded-message calls typically include instructions for opting out of future calls, usually by pressing a key on the phone’s keypad. Do not

follow these directions if the automated call is from an unknown or a potentially untrustworthy caller—doing so can lead to an increase in call frequency.

Expert Source: Edgar Dworsky, consumer attorney, founder, Consumer World, a consumer resource guide, Somerville, Massachusetts. He previously served as assistant attorney general for the state of Massachusetts and as consumer education consultant for the Federal Trade Commission. www.ConsumerWorld.org

How to Create the Best Password

The most common solutions for keeping track of your computer passwords no longer provide enough protection. Are you still doing the following?

Picking obvious passwords, such as 123456, abc123, your pet's name or your mother's maiden name.

Problem: Many people can guess these easily and break into your accounts.

Using the same password for multiple accounts.

Problem: This allows a person who knows your password to access more than one of your accounts.

Taping password reminders to your computer screen or leaving them in the top drawer of your desk.

Problem: They are easily accessible to anyone who enters your home or office.

Better strategies…

High-Security Password

The safest passwords are nondictionary words of at least eight characters that contain a combination of numbers and lowercase and uppercase letters. *This sounds like a chore, but it's actually easy if you use this three-step system…*

1. Use a mnemonic device to come up with your "core" password. Use a memorable combination, such as your spouse's initials and the month and day of your anniversary. *Example:* If your spouse's initials are ST and you were married on June 3, your core password is ST0603.

2. Create unique passwords by using variations on your core password. Take the name of the particular website you are creating a password for, and add the first letter to the front of your core password and the last letter to the end, all in

lowercase. *Examples:* If you use the Amazon.com website, your password is aST0603n… if you go to www.Vanguard.com, your password is vST0603d.

3. For added protection, add a layer of variation to your core password. For example, if your Vanguard password (vST0603d) doesn't feel secure enough, go one step further. Add another number to the end of it. Take the final letter of your password and convert it to the corresponding number on a telephone number pad. Since the letter "d" corresponds to the number "3," your new password is vST0603d3. That's nearly impossible to crack, but fairly easy to re-create should you forget it.

Note: Many sites today also require at least one special character—such as a dollar sign or an exclamation point—and it's good for your security to include one even when a site doesn't insist. An easy way to do this is to swap in a special character for a letter that reminds you of that special character—such as using a dollar sign instead of an "s" or an exclamation point instead of an "i."

Extra Security

Choose the right security question. Many websites now require you to answer a preselected personal question when you choose a password. You're usually allowed to select the question you want to use. Avoid picking one whose answer is open to interpretation or difficult to spell. *Example:* I usually use a security question that asks for the city of my birth, but not one that asks for my favorite food (which could change) or my elementary school. (Was it PS 12 or P.S. 12 or PS #12?)

Write down your passwords and security answers. Keep this information in a secure place, such as a safe-deposit box. If you die or are injured, your family still will have a way to access your website accounts.

Consider password-management software protected with encryption. You create a database of all your passwords on your computer and secure the file with a master password. *My favorite encryption software:* KeePass, http://keepass.info. *Cost:* Free. Put your master password in your safe-deposit box.

Expert Source: Gina Trapani, author of *Upgrade Your Life: The Lifehacker Guide to Working Smarter,*

Faster, Better (Wiley). Based in San Diego, she is creator of Lifehacker.com, a website that provides daily advice and links about technology and personal productivity.

The Safest Password Today

Every day, you hear of another security breach from a major retailer or other business. It's clear that hackers are all around us. What is one to do? Fight back with a secure password.

The challenge is that just about any password you can think up, the bad guys can guess with the help of password-hacking software. One common strategy—turning a memorable phrase into an obscure password by combining the first letter of each word in the phrase—has become so popular that the hacking software now can guess some of these seemingly secure passwords as well. Trouble is, people tend to gravitate to the same phrases. *Star Wars* fans use MTFBWY (May The Force Be With You)…Shakespeare fans, TBONTBTITQ (To Be Or Not To Be That Is The Question).

If you want a truly strong password for your most important accounts, use one created by the free *"Password Generator"* on Random.org or a similar site. But the challenge with truly random passwords is remembering them.

The secret is to mentally convert these random passwords into phrases. The random password RPM8T4KA might be remembered as *Revolutions Per Minute Eight-Track for KAthy,* for example. The human mind is very good at remembering phrases, even odd ones that include a lowercase letter, a number or a symbol. Keep trying the random password generator until you get a password that you can convert into a phrase that you can remember.

Expert Source: William Poundstone, author of *Rock Breaks Scissors: A Practical Guide to Outwitting Almost Everybody* (Little, Brown).

Take Charge of Your Medical Privacy

Imagine calling the hospital where your spouse or your 90-year-old mother just had major surgery and being told that you do not have the right to find out how he/she is doing. This scenario happens frequently these days. That's because people often assume wrongly that family members always have access to each other's medical information. Prior to 2004, laws were rather vague on the issue of gaining access to a person's medical status or records. But with the passage of the federal *Health Insurance Portability and Accountability Act* (HIPAA), medical privacy is now governed by voluminous and complicated rules. So unless you do your homework, situations like the one described above can happen to you. *Key points to consider…*

Who should know? Unless you designate in writing the specific family members (including your spouse) or friends you want to have access to your medical information, medical personnel are severely restricted in disclosing anything about you to nonmedical personnel. Only in real emergencies (such as an auto accident) or when a patient is unable to comprehend what is going on around him (due to such conditions as a stroke or a concussion) do doctors or nurses have the discretion to speak to a nondesignated family member or friend. But those are rare instances.

My advice: Make a list of the people you would allow medical personnel to talk to about your medical status. At the top of the list, write "permissible contacts" and include each person's phone number and address. Give your list to each of your doctors and to the hospital when you are admitted.

What's in your record? Prior to HIPAA, someone else's medical test result had been wrongly placed in my medical record. It took me three years to get the doctor to remove it. Even then, he didn't have a record of whether he had sent the test result that wasn't mine to an insurance company or another doctor. Under HIPAA, the doctor must give you access to your record and tell you where information has been sent so you can contact the party.

My advice: Every few years, review the medical records that all your doctors and any hospital to which you have been admitted have on file for you. If you find an

error, ask the doctor to correct it and to forward corrections to whomever the medical record was sent.

Appoint a personal representative. Under the HIPAA law, a legally designated "personal representative" must be treated as if he were the patient with respect to that patient's medical information, and he has the authority to make decisions about the patient's care.

My advice: Regardless of your age, complete the paperwork (ideally, with the help of an attorney) that is necessary, under the laws of the state where you reside, to name a family member or friend as your personal representative. This step can be completed through a medical/health-care power of attorney document (available from attorneys and, in some cases, state departments of health or attorney general offices).

By taking these steps now, you can avoid a lot of confusion later.

Expert Source: Charles B. Inlander, consumer advocate and health-care consultant, Fogelsville, Pennsylvania. He was the founding president of the nonprofit People's Medical Society, a consumer advocacy organization credited with key improvements in the quality of US health care in the 1980s and 1990s, and is author or coauthor of more than 20 consumer-health books.

The Other Side of Health Privacy Laws

Not long ago, I learned of a family that was heartbroken by a doctor's misguided attempts to protect their dad's privacy. These sons and daughters, in their 30s and 40s, were not told by their father's doctor that the man's condition was terminal. As a result, they kept insisting on more tests and treatment for their father, who was not strong enough to object but had told the doctor that he did not want to continue that level of care. The man knew that he was dying and wanted his family to know that, too. But the doctor never advised the man's children of this crucial fact, citing federal privacy laws. The doctor was wrong about the privacy law.

Numerous cases such as this one came to light at a recent congressional hearing on the federal privacy provisions of the *Health Insurance Portability and Accountability Act* (HIPAA). Lawmakers discovered that health-care providers often are wrongly denying family members, caregivers and friends involved with a patient's care vital information that might have life-or-death consequences. One expert suggested that some health professionals are simply using the law to sidestep difficult conversations with family members. To avoid having family members stonewalled by medical personnel, the solution is to simply make sure that you have a list that names all people (including your doctors) whom you want to have access to your health information included in your medical records —and carry a copy of that list in your wallet.

But the other side of the HIPAA laws involves cases in which your doctor determines on his/her own that certain information about your case should be disclosed to family members or others involved with your care—even if those people are not on your list. *For example…*

When you are incapacitated. If you are unconscious or in another examination room, a doctor may under the law share information if it is in "the best interest of the patient." For example, a surgeon who performed emergency surgery may inform family members not on your list about your condition while you are still unconscious. But doctors and nurses can reveal only the most basic information, such as whether you came through the surgery well or poorly and your prognosis. Anything that is not directly related to your current care, such as past

illnesses or other medical conditions, should not be discussed.

When it benefits you medically. If, according to your doctor's "professional judgment," it is to your medical benefit, he can under the law discuss certain matters with family, friends or caregivers who are not on your list. For example, your doctor may discuss with your sister your increased risk of falling if she is driving you home from the hospital.

When you bring someone into the exam room. If you bring a friend or family member into an exam room at your doctor's office, it is assumed that you have given permission for the doctor to speak freely.

For more on medical privacy rights, go to www.HHS.gov/ocr/hipaa.

Expert Source: Charles B. Inlander, consumer advocate and health-care consultant, Fogelsville, Pennsylvania. He was the founding president of the nonprofit People's Medical Society, a consumer advocacy organization credited with key improvements in the quality of US health care in the 1980s and 1990s, and is author or coauthor of more than 20 consumer-health books.



We hope this Kindle book has been helpful to you.

Would you please take a moment to write a review?

Please click here to add your review.

Thank you.

Don’t forget, you’ve got instant access to

Bottom Line PERSONAL

Click here now to get your FREE BONUS.


34 YEARS / INSIDE INFORMATION FROM THE WORLD'S BEST EXPERTS

BOTTOM LINE PERSONAL

Is it really better?

HEARD BY OUR EDITORS

Widely prescribed heart drug is dangerous for patients with atrial fibrillation (abnormal heart rhythm), warns Samy Claude Elayi, MD. There is increasing evidence that those patients taking digoxin are at increased risk for death, compared with patients treated with beta-blockers and calcium-channel blockers such as diltiazem and verapamil. About one-quarter of people with atrial fibrillation still are prescribed digoxin, partly because it has been used for so long. But do not stop taking it until you have talked with your doctor. Dr. Elayi, MD, is associate professor of medicine at UH Heart Institute of University of Kentucky, Lexington.

Interest rates on "jumbo" mortgages are making high-priced homes more attractive, we hear from loan expert Keith Gumbinger. Traditionally, rates on 30-year, fixed-rate jumbo loans (which start at $417,000 in most of the US and $625,500 in pricier areas) are higher than those on standard mortgages, but recently jumbo rates averaged 4.23%, about the same as standard rates, following five weeks in which jumbo rates were even lower than standard rates. Reason: Lenders have lowered jumbo rates to attract wealthy borrowers with high credit scores...and standard rates have risen as federal regulators have increased insurance costs.

Keith Gumbinger is vice president of HSH Associates, which publishes mortgage and consumer information, Riverside, New Jersey, HSH.com.

Colonoscopy patients with only one polyp removed may need less frequent follow-up, reports Randall W. Burt, MD. A recent Norwegian study suggested that a follow-up colonoscopy at 15 years may be enough in some cases when a polyp is small and low risk. When more or higher-risk polyps are removed, the follow-up should be in three to five years.

Dr. Burt, MD, is the gastroenterologist at Huntsman Cancer Institute, Salt Lake City.

John W. Kray, S&P Capital IQ

The Best Stocks in Europe

9 Countries to Invest in Despite the Region's Turmoil

The economic outlook for Europe is not pretty. But the outlook for investors could be quite good—maybe even better than in the US—if you know which European countries and companies to focus on.

Weighing against Europe right now: Threats of deflation and recession...mounting tit-for-tat economic sanctions with Russia over Ukraine...and double-digit unemployment in various countries. But that doesn't mean that the continent is lacking in great stock opportunities. You just have to think of Europe as 50 separate countries rather than one giant bloc that moves in a single direction.

Bottom Line/Personal asked international investment analyst John W. Kray of S&P Capital IQ to sort out the good, the bad and the ugly among European nations and the stocks that should do best, based on assessments and rankings by that research firm's analysts.

Bottom Line/Personal interviewed John W. Kray, senior investment officer and analyst covering European and Asian markets for S&P Capital IQ, which provides investment research to more than 6,000 financial-services clients. New York City, CapitalIQ.com.

The following nations should continue to see economic growth even if much of Europe stagnates or falls into recession....

Germany's economy should grow at a 2% rate this year and next. *Reasons:* It will achieve a balanced budget by next year, thanks in part to spending cuts and tax increases. German exports, third in the world behind China and the US, remain strong, especially for autos and electronic equipment and especially to fast-growing parts of Asia. *Stocks highly ranked by S&P Capital IQ:* Financial-services firm Allianz SE (AZSEY)...Beiersdorf AG (B

Secrets Inside

2 Edison's problem solver
3 Avoid Obamacare mistakes
6 Taxpayer victories (and defeats) save $$$
7 Sinusitis remedies
10 Coloring your own hair? Four common mistakes
11 Words that can transform a marriage
15 Fast and flavorful veggies