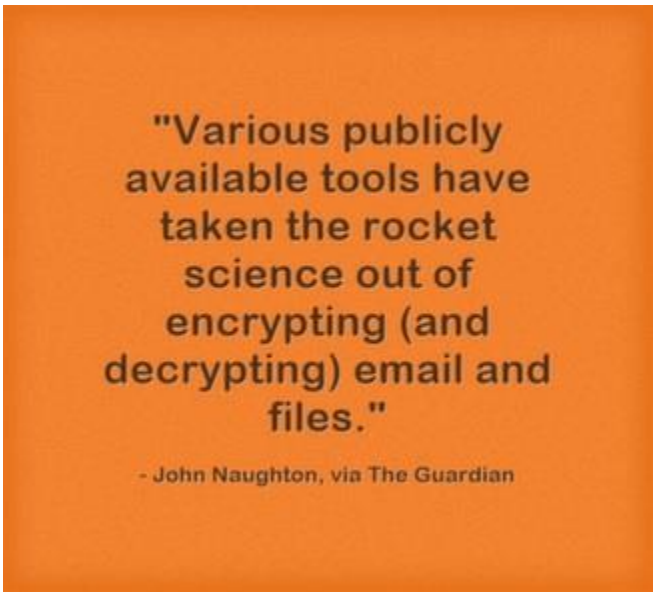
Keeping your passwords, financial, and other personal information safe and protected from outside intruders has long been a priority of businesses, but it's increasingly critical for consumers and individuals to heed data protection advice and use sound practices to keep your sensitive personal information safe and secure. There's an abundance of information out there for consumers, families, and individuals on protecting passwords, adequately protecting desktop computers, laptops, and mobile devices from hackers, malware, and other threats, and best practices for using the Internet safely. But there's so much information that it's easy to get confused, particularly if you're not tech-savvy. We've compiled a list of 101 simple, straightforward best practices and tips for keeping your family's personal information private and protecting your devices from threats.

Securing Your Devices and Networks

1. Encrypt your data.



Data encryption isn't just for technology geeks; modern tools make it possible for anyone to encrypt emails and other information. "Encryption used to be the sole province of geeks and mathematicians, but a lot has changed in recent years. In particular, various publicly available tools have taken the rocket science out of encrypting (and decrypting) email and files. GPG for Mail, for example, is an open source plug-in for the Apple Mail program that makes it easy to encrypt, decrypt, sign and verify emails using the OpenPGP standard. And for protecting files, newer versions of Apple's OS X operating system come with FileVault, a program that encrypts the hard drive of a computer. Those running Microsoft Windows have a similar program. This software will scramble your data, but won't protect you from government authorities demanding your encryption key under the Regulation of Investigatory Powers Act (2000), which is why some aficionados recommend TrueCrypt, a program with some very interesting facilities, which might have been useful to David Miranda," explains John Naughton in an article for The Guardian. Twitter: @guardian

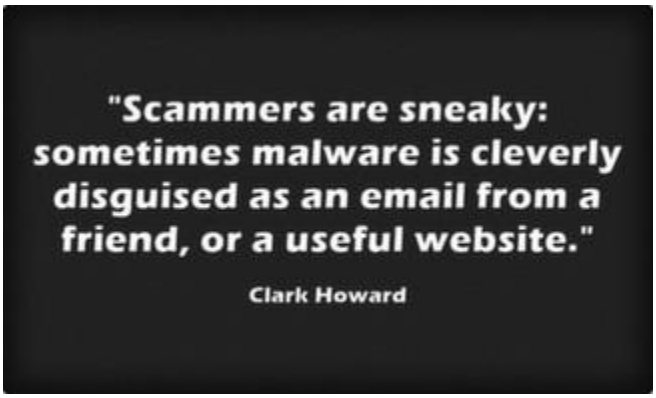
2. Backup your data.

One of the most basic, yet often overlooked, data protection tips is backing up your data. Basically, this creates a duplicate copy of your data so that if a device is lost, stolen, or compromised, you don't also lose your important information. It's best to create a backup on a different device, such as an external hard drive, so that you can easily recover your information when the original device becomes compromised.

3. The cloud provides a viable backup option.

While you should use sound security practices when you're making use of the cloud, it can provide an ideal solution for backing up your data. Since data is not stored on a local device, it's easily accessible even when your hardware becomes compromised. "Cloud storage, where data is kept offsite by a provider, is a guarantee of adequate disaster recovery," according to this post on TechRadar. Twitter: @techradar

4. Anti-malware protection is a must.



Malware is a serious issue plaguing many a computer user, and it's known for cropping up in inconspicuous places, unbeknownst to users. Anti-malware protection is essential for laying a foundation of security for your devices. "Malware (short for malicious software) is software designed to infiltrate or damage a computer without your consent. Malware includes computer viruses, worms, trojan horses, spyware, scareware and more. It can be present on websites and emails, or hidden in downloadable files, photos, videos, freeware or shareware. (However, it should be noted that most websites, shareware or freeware applications do not come with malware.) The best way to avoid getting infected is to run a good anti-virus protection program, do periodic scans for spyware, avoid clicking on suspicous email links or websites. But scammers are sneaky: sometimes malware is cleverly disguised as an email from a friend, or a useful website. Even the most cautious of web-surfers will likely pick up an infection at some point.," explains Clark Howard. Twitter: @ClarkHoward

5. Make your old computers' hard drives unreadable.

Much information can be gleaned through old computing devices, but you can protect your personal data by making hard drives unreadable before disposing of them. "Make old computers’ hard-drives

unreadable. After you back up your data and transfer the files elsewhere, you should sanitize by disk shredding, magnetically cleaning the disk, or using software to wipe the disk clean. Destroy old computer disks and backup tapes," according to the Florida Office of the Attorney General. Twitter: @AGPamBondi

6. Install operating system updates.

Operating system updates are a gigantic pain for users; it's the honest truth. But they're a necessary evil, as these updates contain critical security patches that will protect your computer from recently discovered threats. Failing to install these updates means your computer is at risk. "No matter which operating system you use, it's important that you update it regularly. Windows operating systems are typically updated at least monthly, typically on so-called 'Patch Tuesday.' Other operating systems may not be updated quite as frequently or on a regular schedule. It's best to set your operating system to update automatically. The method for doing so will vary depending upon your particular operating system," says PrivacyRights.org. Twitter: @PrivacyToday

7. Automate your software updates.

In order to ensure that you're downloading the latest security updates from operating systems and other software, enable automatic updates. "Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option," suggests StaySafeOnline.org. Twitter: @StaySafeOnline

8. Secure your wireless network at your home or business.

A valuable tip for both small business owners and individuals or families, it's always recommended to secure your wireless network with a password. This prevents unauthorized individuals within proximity to hijack your wireless network. Even if they're merely attempting to get free Wi-Fi access, you don't want to inadvertently share private information with other people who are using your network without permission. "If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router," says FCC.gov in an article offering data protection tips for small businesses. Twitter: @FCC

9. Turn off your computer.

When you're finished using your computer or laptop, power it off. Leaving computing devices on, and most often, connected to the Internet, opens the door for rogue attacks. "Leaving your computer connected to the Internet when it's not in use gives scammers 24/7 access to install malware and commit cyber crimes. To be safe, turn off your computer when it's not in use," suggests CSID. Twitter: @CSIdentity

10. Use a firewall.

"Firewalls assist in blocking dangerous programs, viruses or spyware before they infiltrate your system. Various software companies offer firewall protection, but hardware-based firewalls, like those frequently built into network routers, provide a better level of security," says Geek Squad. Twitter: @GeekSquad

11. Practice the Principle of Least Privilege (PoLP).

Indiana University Information Technology recommends following the Principle of Least Privilege (PoLP): "Do not log into a computer with administrator rights unless you must do so to perform specific tasks. Running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits. Simply visiting an unfamiliar Internet site with these high-privilege accounts can cause extreme damage to your computer, such as reformatting your hard drive, deleting all your files, and creating a new user account with administrative access. When you do need to perform tasks as an administrator, always follow secure procedures." Twitter: @IndianaUniv

12. Use "passphrases" rather than "passwords."

What's the difference? "A passphrase is simply a different way of thinking about a much longer password. Dictionary words and names are no longer restricted. In fact, one of the very few restrictions is the length - 15 characters. Your passphrase can be a favorite song lyric, quote from a book, magazine,

or movie, or something your kids said last week. It's really that easy," explains Indiana University's Protect IU. Think of a saying or series of words that is easy for you to remember, and use the first letter of each word in the phrase, along with a combination of numbers and special characters, as your passphrase. Twitter: @IndianaUniv

13. Encrypt data on your USB drives and SIM cards.

Encrypting your data on your removable storage devices can make it more difficult (albeit not impossible) for criminals to interpret your personal data should your device become lost or stolen. USB drives and SIM cards are excellent examples of removable storage devices that can simply be plugged into another device, enabling the user to access all the data stored on it. Unless, of course, it's encrypted. "Your USB drive could easily be stolen and put into another computer, where they can steal all of your files and even install malware or viruses onto your flash drive that will infect any computer it is plugged in to. Encrypt your SIM card in case your phone is ever stolen, or take it out if you are selling your old cell phone," according to Mike Juba in an article on Business2Community. Twitter: @EZSolutionCorp

14. Don't store passwords with your laptop or mobile device.

A Post-It note stuck to the outside of your laptop or tablet is "akin to leaving your keys in your car," says The Ohio State University's Office of the Chief Information Officer. Likewise, you shouldn't leave your laptop in your car. It's a magnet for identity thieves. Twitter: @OhioState

15. Disable file and media sharing if you don't need it.

If you have a home wireless network with multiple devices connected, you might find it convenient to share files between machines. However, there's no reason to make files publicly available if it's not necessary. "Make sure that you share some of your folders only on the home network. If you don't really need your files to be visible to other machines, disable file and media sharing completely," says Kaspersky. Twitter: @kaspersky

16. Create encrypted volumes for portable, private data files.

HowToGeek offers a series of articles with tips, tricks, and tools for encrypting files or sets of files using various programs and tools. This article covers a method for creating an encrypted volume to easily transport private, sensitive data for access on multiple computers. Twitter: @howtogeeksite

17. Overwrite deleted files.

Deleting your information on a computing device rarely means it's truly deleted permanently. Often, this data still exists on disk and can be recovered by someone who knows what they're doing (such as, say, a savvy criminal determined to find your personal information). The only way to really ensure that your old data is gone forever is to overwrite it. Luckily, there are tools to streamline this process. PCWorld covers a tool and process for overwriting old data on Windows operating systems. Twitter: @pcworld

18. Don't forget to delete old files from cloud backups.

If you're diligent about backing up your data and use a secure cloud storage service to do so, you're headed in the right direction. That said, cloud backups, and any data backups really, create an added step when it comes to deleting old information. Don't forget to delete files from your backup services in addition to those you remove (or overwrite) on your local devices. "If you back up your files to the cloud, remember that even though you delete them on your computer or mobile device, they're still stored in your cloud account. To completely delete the file, you'll also need to remove it from your backup cloud account," says re/code. Twitter: @Recode

---

Data Protection Tips for Mobile Devices

19. Consciously check and configure app privacy settings.

Most apps offer privacy settings for users, enabling you to determine how much and what types of information are shared or stored. Always choose the least amount of data-sharing possible. Google, for instance, offers individual permission levels and privacy settings for the mobile apps it provides: "Google offers a variety of mobile applications that you can download onto your smart phone and some of these apps, such as Search, Maps and Latitude incorporate geolocation features. Some parents may be concerned about their teen sharing their location with others. Each app allows you to adjust the privacy setting so you can share as much or little as you want." Twitter: @goinsidegoogle

20. Enable remote location and device-wiping.

"If your gadget is lost or stolen, tracking apps can tell you exactly where your phone is. These apps also let you wipe sensitive information remotely. If your phone does end up landing in the wrong hands, you can at least make sure they don't get your information," says Kim Komando. Twitter: @kimkomando

21. Take care of privacy settings immediately upon setup.

When configuring a new device or operating system, configuring privacy settings should be the first order of business. This ensures that you're not inadvertently sharing sensitive information as you set up your standard apps and services. "The minute you download and install iOS 8, the latest version of Apple's mobile operating system for iPhone and iPad, you should take note of these privacy steps in order to lock down your device. iOS 8 has a number of new features tied to your location. It also has new privacy settings, allowing users to limit how long data is stored for, such as message expiry features and new private browsing settings...Before you do anything like customizing your phone, loading new apps, or syncing your data for the first time, these first seven settings need to be checked, and if necessary, changed," explains Zack Whittaker in an article appearing on ZDNet. Twitter: @zackwhittaker

22. Use MyPermissions.com to control app permissions in one fell swoop.

While it's not all-inclusive, MyPermissions.org is a handy tool that allows you to check your permission settings across a multitude of apps, get reminders to clean your permissions with mobile-friendly apps, and get alerts when apps access your personal information so that you can remove it with a single click. Twitter: @mypermissions

23. Lock your smartphone and tablet devices.

Practically everyone has a smartphone, tablet, or both these days. All it takes is a single mishap where your device slips out of your pocket or briefcase at a restaurant or on public transportation, and your data could wind up in the hands of someone who will use it maliciously. You can take steps to protect your data in the event of a lost or stolen device, however, beginning with locking your device. When your device is locked, a thief must crack your password before gaining access to your apps or personal information, adding a layer of protection. "As soon as you get a new smartphone, set a hard to guess password to protect your device and change it on a regular basis." says CTIA, The Wireless Association. Twitter: @CTIA

24. Don't forget to backup your mobile device data.

Another data protection strategy that's often overlooked for mobile devices is the need to backup your data from your mobile device in addition to your desktop computer's or laptop's data. There are some automatic cloud-backup options, but this article on Yahoo Small Business Advisor suggests an interesting strategy: using IFTTT (If This Then That) to facilitate automatic backups of important files, such as photos or work documents. Twitter: @Yahoo

25. Disable automatic uploading.

Some devices automatically backup your data to the cloud, and some apps used on smartphones or tablets store information in remote servers. Yes, having a backup of your data is a good thing, but the backup should be accessible only by you or someone you authorize. You can prevent your devices from sharing your personal photos and other information with the cloud for the world to see by disabling automatic backup settings on your device and on individual apps. In an article on BBC, Colin Barras

explains, "As cloud services grow it's becoming common for devices like smartphones to upload user data to remote servers by default. If you're at all worried about some of your photos falling into the hands of malicious parties it's probably not a bad idea to check your phone settings to see what data is being automatically backed up to the cloud, and disable automatic uploading." Twitter: @BBC_Future

26. Disable Bluetooth when you're not using it.

Bluetooth technology has offered incredible conveniences to the mobile world, but it also opens the door for vulnerabilities. Most threats exploiting Bluetooth connectivity are dependent on the active Bluetooth connection, and while they aren't typically devastating or dangerous, they're certainly inconvenient and can be serious. "Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. Regardless of the security features on your device, the only way to completely prevent attackers from exploiting that permission request/grant process is to power off your device's Bluetooth function when you're not using it — not putting it into an invisible or undetectable mode, but completely turning it off (there are bad apps that can power your device back on, just one more reason overall app security is vital)," advises Kaspersky Lab. Twitter: @kaspersky

27. Get anti-virus or anti-malware protection for your mobile devices.

Anti-malware protection software is a given for most computer users, but many consumers still overlook the importance of protecting mobile devices from the growing number of malware programs impacting all types of mobile devices. Just a few years ago, however, security options for mobile devices offered mediocre protection against threats, at best. "Besides antivirus and malware scanning, security apps for Android also offer a full McAfee LiveSafe 2014 Android screenshot McAfee for Android security suite with features such as device location, remote wipe, backup, and suspicious-URL blocking. These extra features usually require a premium subscription, but most apps offer a minimal, basic level of protection for free, including malware scanning," according to an article on PCWorld. Twitter: @pcworld

28. Check your push notification settings on mobile devices.

Push notifications are notices posted to your device homescreen so that you don't miss important information or updates. "Many applications send proactive notifications to your phone's home screen.

In general, these notifications are valuable and make it easy to keep track of what's happening in your favorite applications. Personal health applications may send these types of notifications as well. If you are using applications that use push notifications, review them to ensure that sensitive data isn't being shared unexpectedly to your home screen. You don't want your personal health data laying out in plain site on your phone," according to an article on TrueVault. Twitter: @TrueVault

29. Enable Touch ID if you use an Apple device.

If you use an iPhone 5 or later, you can take advantage of an added security measure known as Touch ID, a technologically advanced fingerprint security tactic. "The actual image of your fingerprint is not stored anywhere, and is instead converted to a mathematical representation of a fingerprint that cannot be reverse engineered into one. This mathematical representation is stored in a Secure Enclave within your phone's chip, and is never accessed by iOS or other apps, never stored on Apple servers, and never backed up to iCloud or anywhere else."

30. Set up content filters.

If you have children who use mobile devices, check into security options such as content filters that can be activated either through your wireless provider or on the physical device. These filters restrict access to certain types of content, ensuring that your children cannot inadvertently go to websites or download apps that contain either inappropriate or malicious content. Verizon Wireless, for instance, offers a number of content filters and security options for families. Twitter: @VerizonWireless

31. Set your device to automatically lock after a period of inactivity.

Most smartphones and tablets enable you to set a specified time frame, after which the device automatically locks if it's been inactive. This means if you lose your smartphone but it wasn't locked, it will lock on its own, ideally before a thief obtains it and attempts to access your personal information. "Configure your settings to ensure that your device locks after a short period of time," says ProtectYourData.ca. Twitter: @CWTAwireless

32. Be mindful of the apps you install.

There are new apps entering the market constantly. But too many apps running in the background not only slows down your smartphone or tablet, but some of them could be sharing your personal

information, even your current location via GPS, without your knowledge. Don't install apps unless they're from trusted sources. "The problem is that many third-party app stores are not safe. If you choose to download an APK file and install it yourself, you could be putting malware on your device. You may also be sent an APK file in an email or a text message, or you could be prompted to install one after clicking on a link in your web browser. It's best not to install these unless you are certain it is safe," according to an article on Digital Trends. Twitter: @DigitalTrends

33. Prevent your smartphone from being stolen.

While remote wiping and location-tracking solutions are great for finding your device and protecting your data if it's been stolen, the ideal solution is to avoid having your smartphone or other device stolen in the first place. "One of your best 'grab-prevention' options is a wireless proximity alarm system. These handy app/device combos let you know when your phone gets more than the pre-set distance limit from the proximity device (which is usually small enough to fit on a key ring)," ComputerWorld recommends. Twitter: @computerworld

34. Use an on-device, personal firewall.

Firewalls aren't just for servers and browsers; you can get a personal firewall for your mobile device, too. MySecurityAwareness.com suggests installing "an on-device personal firewall to protect mobile device interfaces from direct attack."

35. Wipe devices and set to factory defaults before donating or discarding.

Don't just give your old mobile devices to someone else, particularly someone you don't know, without first wiping it clean and restoring it to factory settings. Otherwise, you're basically handing over all your personal data to whoever ends up with your old smartphone or tablet. "Many security experts say performing a factory reset on your old phone is exactly what you're supposed to do if you plan to sell or donate it. According to the nation's major wireless carriers, a reset will erase all personal information –

such as texts, contact lists, photos and important user data – from your phone's memory," says WTHR.com. But, this method isn't fool-proof; in fact, 13 Investigates put this very theory to the test and found that in some cases, a factory reset will wipe a device clean. In others, it won't. The solution? Do a factory reset as a precaution, but do your research and determine the best way to discard of your device or cleaning it before donating it to charity. Twitter: @WTHRcom

36. Be mindful of eavesdroppers when shopping via your mobile device in public.

If you have time to kill on your morning commute, you might browse the virtual shopping aisles, but be mindful of who is sitting beside you or behind you. Criminals can easily peep over your shoulder and watch as you enter passwords, credit card details, and other information. "A long commute on a bus or a train is the perfect time to get some holiday shopping done, but beware of that stranger sitting next to you. Your neighbors might try and read your screen and steal your credit card number or other information. Investing in a privacy screen or filter can significantly reduce the risk of peeping thieves. Screen protectors come in all shapes and sizes and at Best Buy, you can find the one that's best for your favorite tech gadget," advises BestBuy in an article offering tips for keeping your digital data safe on Cyber Monday (and really, anytime you're shopping online). Twitter: @BBYNews

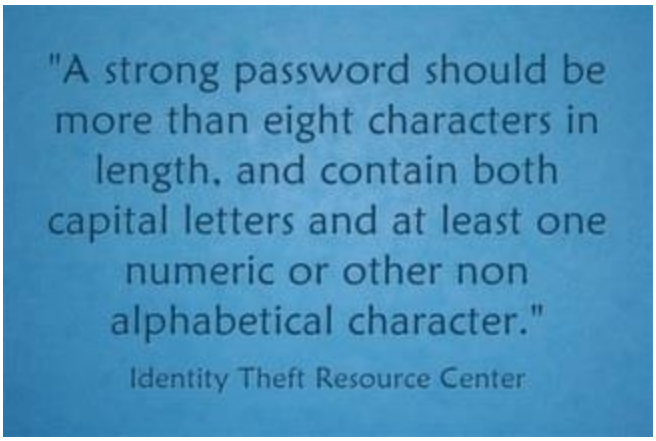
---

Protecting Your Identity

37. Decide what you define as Personally Identifiable Information (PII).

ComputerWorld asks six privacy experts for their recommendations for protecting data in the modern digital age. "'The traditional definition of personally identifying information (PII) -- health records, credit card numbers, social security number, etc. -- is so 20th century. The big data age of the Internet is upon us, and even data not previously considered to be PII can feel very personal when viewed in a broader context. 'Bits of data, when combined, tell a lot about you,' says Alex Fowler, chief privacy officer at Mozilla. Those aggregated bits, which constitute the new PII, may include such information as your email address, browsing history and search history. 'The definition of PII -- information that a person has a legitimate interest in understanding and protecting -- is going to be broadened as we move further into the information society,' says Fowler. 'It's a different footprint than what your parents ever thought about. Think about what you consider personal information,' Fowler adds. 'You need a working definition.'" Twitter: @Computerworld

38. Use secure passwords.



Passwords are easily cracked by hackers, particularly if you don't use sound password-creation practices. The best passwords contain uppercase and lowercase letters, numbers, and special characters. You should also avoid using easily guessed words or alphanumeric combinations, such as the names of children or pets, birth dates, addresses, and similar information that can be easily guessed by someone looking at your Facebook profile or through a Google search. "A strong password should be more than eight characters in length, and contain both capital letters and at least one numeric or other non alphabetical character. Use of non-dictionary words is also recommended," suggests the Identity Theft Resource Center. Twitter: @ITRCSD

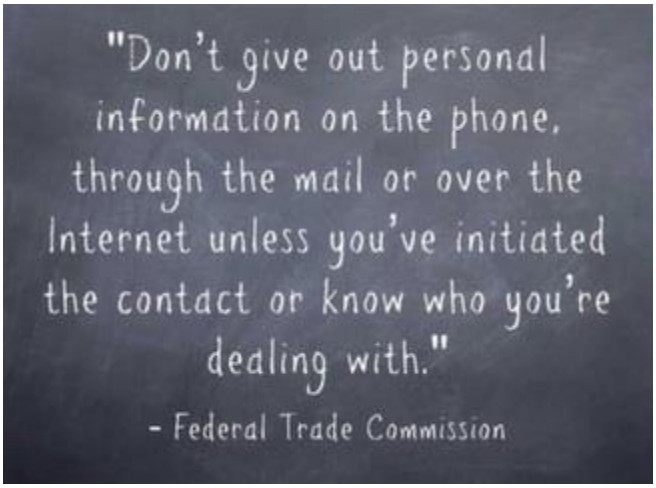
39. Don't use Social Security numbers, phone numbers, addresses, or other personally identifiable information as passwords.

Don't use numbers or combinations associated with other personally identifiable information as all or even part of your passwords. "Don't use any part of your social security number (or any other sensitive info, like a credit card number) as a password, user ID or personal identification number (PIN). If someone gains access to this information, it will be among the first things they use to try to get into your account," Bank of America advises. Twitter: @BofA_News

40. Be overly cautious when sharing personal information.

This tip applies to both the online and offline worlds: Who is asking for your personal information, such as your Social Security number or credit card information? Why do they need it? How will they use it? What security measures do they have in place to ensure that your private information remains private? Know who you're giving out information to, and don't share any information that's not necessary. When in doubt, withhold information when possible.

41. Watch out for impersonators.



Related to the previous tip, there are many impostors who attempt to trick unsuspecting consumers into giving out their sensitive personal information by pretending to be the individual's bank, credit card company, or other entity. This can happen by phone or online, via phishing emails or websites designed to mimic the authentic company's look and feel. "Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request," advises the Federal Trade Commission. Twitter: @FTC

42. Share passwords carefully.

This is a data protection tip that's been emphasized by many security experts, yet there are still many people who fail to follow this advice. The truth is, it's impractical in the modern environment. Families need to share passwords to bank accounts, credit cards, and other online services with spouses, and many share a single login to services like Netflix. In the workplace, there are abundant reasons why co-workers may need to share login credentials. You shouldn't give out passwords without concern; rather, determine when another person legitimately requires access to your personal information or account and grant access on a case-by-case basis. If another person needs access for a single, isolated purpose, change your password when the task is completed and they no longer require access. Another option, suggested in an article on PCMag, is to use a password manager that can share single login credentials with other people without them actually being able to view or interpret the login information. Twitter: @PCMag

43. Don't use the same password for more than one account or service.

A password manager seems like an even better idea when you consider the fact that you should never use the same password for more than one account or service. Think about it: If a hacker cracks your password on one website, they suddenly have cracked your password for a dozen more. But remembering the slew of passwords the average person would need to recall to access the many

accounts and services most people have these days is no simple feat, unless you have a photographic memory. In lieu of a password manager, you could follow Danny Heisner's advice at Cranking the Ranking and create your own password algorithm that makes it simple to remember all your passwords without ever using the same one twice. Twitter: @cranktherank

44. Watch out for theft of your government-issued identification numbers.

Thieves don't always go after credit and debit cards; sometimes, they steal important government-issued identification numbers, such as driver's license numbers or Social Security numbers in attempt to assume another individual's identity. "If you are notified of a breach involving your driver's license or another government document, contact the agency that issued the document and find out what it recommends in such situations. You might be instructed to cancel the document and obtain a replacement. Or the agency might instead 'flag' your file to prevent an imposter from getting a license in your name," suggests PrivacyRights.org. Twitter: @PrivacyToday

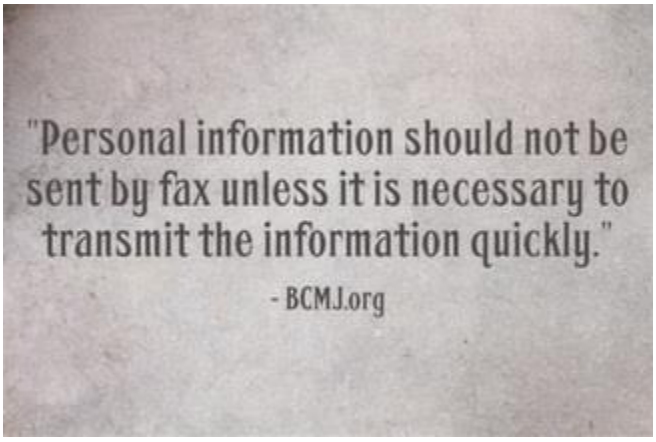
45. Don't write your passwords down.

It's tempting to keep a written list of passwords, or even a single password written down in a notebook or, worse yet, a sticky note. But this is a bad idea, as it makes it extraordinarily easy for someone else to steal your login information and access your accounts without your permission. "Writing your password on a 'sticky-note' and sticking it on your monitor makes it very easy for people who regularly steal passwords to obtain yours. Hiding it under your keyboard or mouse pad is not much better, as these are common hiding places for passwords. However if you must write something down, jot down a hint or clue that will help jog your memory or store the written password in a secure, locked place," says SANS.org. Twitter: @SANSInstitute

46. Organize your passwords in logical groupings.

By using a different system for creating passwords for different types of websites, such as social networking websites, financial institutions, and other membership sites, you ensure that should a hacker crack one of your algorithms, they won't immediately be able to crack all of your accounts' passwords. "First up, group your passwords by function — social media, financial information, work — and use a different approach for creating passwords within each group. That way, if a hacker figures out your Facebook password, he won't be just clicks away from your bank account," explains an article on Boston Globe. Twitter: @BostonGlobe

47. Avoid faxing sensitive information unless absolutely necessary.



Faxing can be a convenient way to send information quickly, but it's not possible to ensure that the intended recipient is the person who receives the document on the other end, or that the information isn't visible to someone else in the process of transporting it to another department or individual. "Personal information should not be sent by fax unless it is necessary to transmit the information quickly. It is important that sufficient precautions are taken to ensure that it is received only by its intended recipient," says BCMJ.org. Twitter: @BCMedicalJrnl

48. Shred old documents and statements.

Most consumers receive an abundance of mail largely considered junk mail. Credit card statements, bank account statements, notifications regarding other accounts, credit card offers, and more plague the mailboxes of consumers across the U.S. While online access to accounts has made printed statements practically unnecessary, many consumers simply toss these items out when they're received. But doing so without first shredding them could put your personal information in the hands of thieves. "Identity theft is the nation's number one complaint, according to the Federal Trade Commission. One of the most common methods used by thieves to steal personal information is dumpster diving, which entails rummaging through trash looking for old bills or other documents that contain personal information," explains Katie Delong, in an article for Fox 6 Now. Fellowes.com offers an informative list of documents that should be shredded, as well as best practices for document shredding to ensure adequate data protection. Twitter: @FellowesInc

49. Get rid of old data you no longer need.

Keeping your computer and mobile devices clean is a good practice to ensure usability, but it's also wise to eliminate old data you no longer need. Why give potential criminals more info than absolutely necessary? "Keep only the data you need for routine current business, safely archive or destroy older data, and remove it from all computers and other devices (smart phones, laptops, flash drives, external hard disks)," advises the Massachussetts Institute of Technology. Twitter: @mit_istnews

50. Properly dispose of electronics.

It's true that nothing is ever really deleted permanently from a computing device; hackers and technologically savvy criminals (and, of course, the FBI) are often able to recover information from hard drives if they haven't been properly disposed of. "Document shredding and electronics recycling are two of the most effective ways to dispose of sensitive records, data, documents and information. Electronic devices, even when no longer in use, often retain confidential personal information that can fall into the wrong hands if disposed of incorrectly," the Better Business Bureau says. Twitter: @bbb_media

---

Protecting Your Credit

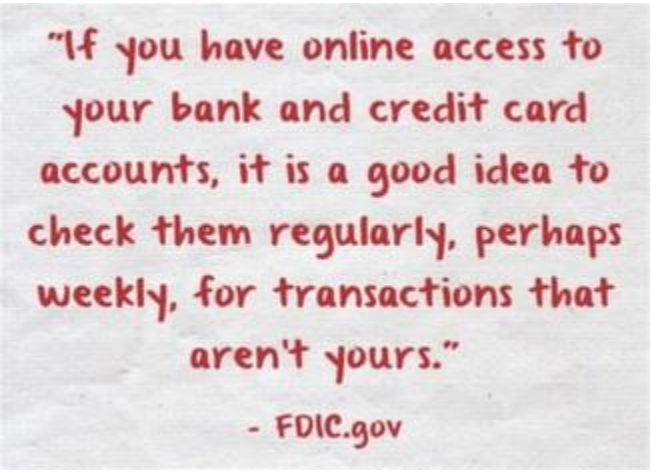
51. Sign when using debit cards, don't enter your PIN.

When possible, ask cashiers to process your debit card as a credit card transaction. Not all retail stores allow this (it results in a small processing fee to be paid by the retailer), but most do. It's often simpler just to enter your PIN, but it also makes it easier for thieves to steal all the information they need to make unauthorized purchases using your card. "Not entering you PIN into a keypad will help reduce the chances of a hacker stealing that number too, Young says. Crooks can do more damage with your PIN, possibly printing a copy of the card and taking money out of an ATM, he says. During Target's breach last year, the discount retailer said hackers gained access to customers' PINs. Home Depot, however, said there was no indication that PINs were compromised in the breach at its stores," explains Joseph Pasani in an Associated Press article appearing on USA Today. Twitter: @USATODAY

52. Sign up for email alerts for transactions.

If your bank or credit card company offers this service, sign up to receive an email alert when your card has been used for a transaction. This makes it easy to pinpoint charges you didn't make, and allows you to take rapid action to cancel cards. "Sign up for email alerts when something is charged to the account. Not all banks will offer this, but these alerts let you know when a new transaction has been made using your card," says CT Watchdog. Twitter: @ctwatchdog

53. Review your statements regularly.



"Review your bank and credit card statements regularly to look for suspicious transactions. If you have online access to your bank and credit card accounts, it is a good idea to check them regularly, perhaps weekly, for transactions that aren't yours. Contact your bank or credit card issuer immediately to report a problem. Debit card users in particular should promptly report a lost card or an unauthorized transaction. Unlike the federal protections for credit cards that cap losses from fraudulent charges at $50, your liability limit for a debit card could be up to $500, or more, if you don't notify your bank within two business days after discovering the loss or theft," advises FDIC.gov. Twitter: @FDICgov

54. Keep an eye out for small transactions.

Fraudsters don't always make major purchases with stolen cards. In fact, there have been some otherwise-legitimate companies that have scammed their own customers by charging small amounts to credit and debit cards they believed would go unnoticed by consumers. Jack Ablin, chief investment officer at BMO Private Bank in Chicago, talks with ChicagoBusiness.com about his experience: "Mr. Ablin says those who pay with credit should be vigilant about tracking their bills. He recalls after a recent online order he placed for flowers that a random charge for $1.99 appeared on his account from an unknown source. He found that the flower company he used was scamming people for this small amount. He figures the company believed most people wouldn't notice the relatively small amount. 'Don't necessarily look for the Hawaiian vacation on your statement,' Mr. Ablin says." Twitter: @CrainsChicago

55. Be wary of offers of help following a data breach.

It's an unfortunate reality that a data breach impacting a major corporation and, therefore, hundreds of thousands of its customers, spells opportunity for thieves. "Be very careful about responding to an unsolicited e-mail promoting credit monitoring services, since many of these offers are fraudulent. If you're interested in credit monitoring and it's not being offered for free by your retailer or bank, do your own independent research to find a reputable service," suggests FDIC.gov. Twitter: @FDICgov

56. Get a one-call fraud alert.

Calling one of the three major credit bureaus (Experian, Equifax, and TransUnion) and asking for a one-call fraud alert is a great way to stay on top of suspicious activity. "You only need to call one of the three credit bureaus. The one you contact is required to contact the other two. This one-call fraud alert will remain in your credit file for at least 90 days. The fraud alert requires creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. When you place a fraud alert on your credit report, you are entitled to one free credit report from each of the three credit bureaus upon request," suggests Office of Minnesota Attorney General Lori Swanson.

57. Shop on familiar websites.

There are hundreds of thousands of online retailers, known as e-commerce vendors, some more credible than others. Always opt to shop with a well-known retailer you're familiar with, rather than smaller, unfamiliar sites that could merely be a facade for credit card theft. "When it comes to online shopping, it's best to use a trusted website rather than selecting a random website with a search engine. If you're familiar with the company and website, it's easier to avoid scams. For instance, many consumer items can be bought just as easily for competitive prices using Amazon.com vs. finding boutique online shopping. Amazon has reputation and regulations to uphold," according to NENS.com. Additionally, major online retailers are more likely to offer fraud protection options and the ability to return damaged or defective merchandise. Twitter: @4NENS

58. Get a free credit report.

Secura Insurance Companies recommends getting a copy of your credit report annually. "The FACT Act of 2003 entitles you to a free credit report once a year from the three credit bureaus. The reports should be examined for fraudulent activity. To obtain your free annual credit report, either order online via www.annualcreditreport.com, or by telephone at (877) 322-8228. For the mail-in form, go to https://www.annualcreditreport.com/cra/ requestformfinal.pdf. " This allows you to pinpoint suspicious activity and identify accounts that you haven't opened. Twitter: @SecuraInsurance

59. Maintain a low-balance credit card for online purchases.

Because shopping online is one of the easiest ways to get your credit card number stolen, some experts suggest maintaining a separate, low-balance credit card specifically for online purchases. "This strategy reduces the risk of fraud, though most credit card companies have a zero liability policy if a lost card or fraudulent charge is reported promptly. Some banks and credit card companies even offer temporary card numbers you can use for online purchases or when traveling to minimize the risk if the card is lost or stolen," explains NEA. Twitter: @NEADeals

---

Protecting Your Data on Social Networking

60. Don't share too much information on social networking platforms.

Social networking has become a way of life for many individuals, but sharing too much personal information on your social media profiles can be dangerous. For instance, many hackers have successfully guessed passwords through trial-and-error methods, using combinations of common information (such as children's names, addresses, and other details) easily found on users' social media profiles. "Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be

considerate when posting information, including photos, about your connections," advises the United States Computer Emergency Readiness Team (US-CERT). Twitter: @USCERT_gov

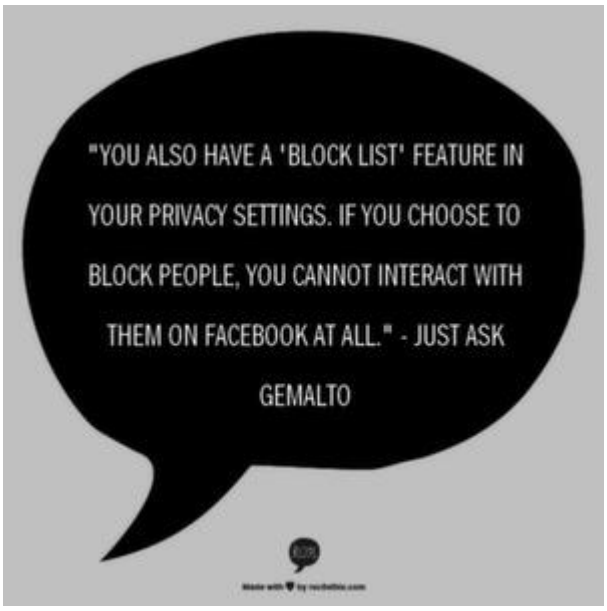
61. Customize your social networking privacy settings.

Social networks like Facebook enable users to customize their privacy settings. On Facebook, for instance, you can choose who is able to see the content you post and who is able to view information on your profile, such as your place of employment, birth date, and hometown. Always choose the highest level of privacy possible to ensure that your personal data doesn't end up in the hands of someone with malicious intent. "The content you post online will be around for a long time, but you can customize privacy settings on most social media sites. This will affect who can contact you and who can see the information you post. Be choosy: while it's fun to share information, keep your online reputation in mind. And if you over-disclose information publicly, it could be used by identity thieves to hijack your identity," suggests the Chronicle of Data Protection. Twitter: @HLPrivacy

62. Don't trust "friends" who claim to be mugged or have other unbelievable stories.

Facebook has become a dangerous platform for users who aren't careful. Scams have been attempted, some successfully, on the social network, involving thieves masquerading as users on an individual's friends list, asking for financial help after supposedly being mugged in a foreign country. Nonsuspecting users who merely want to help their friends may wire money to these criminals, failing to recognize the ploy. Never trust anyone who cannot verify they are, in fact, the person they claim to be. Ask strategic questions to which the answers are not readily available on the user's profile or easily located online. If it seems suspicious, get in touch with the person via phone or another communication method to try to verify the story.

63. Block suspicious or shady users on Facebook.



For users you don't know outside of Facebook who befriend you and then make you uncomfortable by asking repeated, personal questions or pressure you to meet them offline, blocking them is a viable option. "You also have a 'Block List' feature in your privacy settings. If you choose to block people, you cannot interact with them on Facebook at all," says Just Ask Gemalto. Blocking shady users means they cannot message you, contact you, or see that you're online. In fact, they cannot view your profile at all. Twitter: @JustAskGemalto

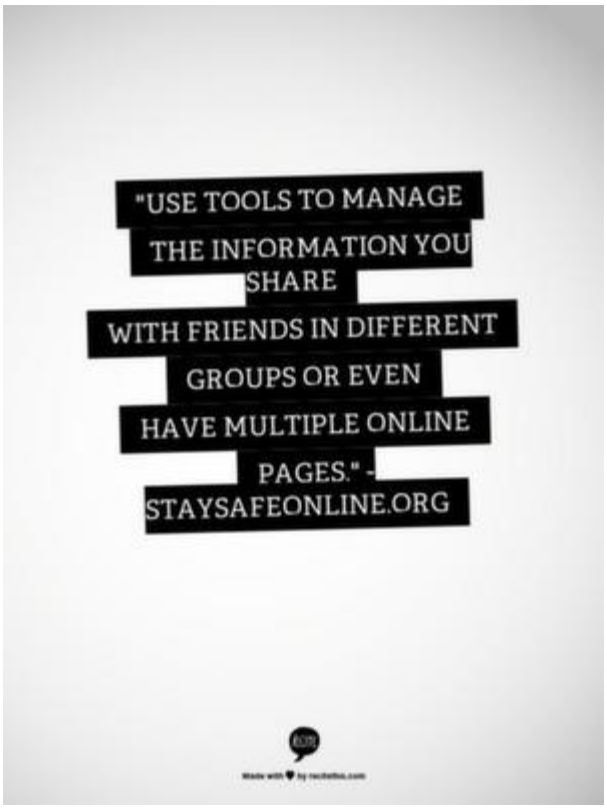
64. Protect your Tweets.

If you're using Twitter to promote your business, you might want your Tweets to be publicly available. However, if you use Twitter for personal communications, you have the option of setting your Tweets to private, meaning only approved followers are able to view your content. Read more about the difference between public and private Tweets here and how to change your settings here. Twitter: @twitter

65. Check your privacy settings regularly.

Privacy options are always changing on social networking platforms, so be sure to check your personal settings regularly and make adjustments as needed. "Content uploaded to social media platforms is not always secure, so it’s imperative to understand how to use the privacy features your social media sites have to offer," according to Social Media Examiner.Click through to the full article for a breakdown of how to update your privacy settings on each of the popular social networks. Twitter: @SMExaminer

66. Know who your friends are.



Don't accept random friend requests on Facebook from people you don't know. "Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a 'fan' page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life," advises StaySafeOnline.org. Twitter: @StaySafeOnline

67. Use two-step verification for LinkedIn.

"LinkedIn offers members the ability to turn on two-step verification for their accounts. This will require an account password and a numeric code sent to your phone via SMS whenever you attempt to sign in from a device that your LinkedIn account does not recognize," according to a post on Business News Daily. This ensures that should someone crack your account password, they will be unable to login unless they can't access your account unless they also gain access to your code -- meaning they'd have to also be in possession of your mobile device. Twitter: @BNDarticles

68. Contact the social network to regain access, and let your friends know if you've been hacked.

Sometimes, having your social networks hacked means your friends could be being conned by criminals pretending to be you. Or, you could even be blocked from your own account if they've changed the password or conducted activities that have led to your account being banned by the service. "If you're locked out of your account or blocked from accessing it, many Web services have steps in place so you

can get back in. For example, Facebook has a system where you can use a trusted source like a friend to take back your account. Search each service's help section for specific instructions. Speaking of friends, you should let your contacts know that you've been hacked, and report the issue to the site. Also, run a scan of your computer or mobile device using a trusted and up-to-date antivirus program," advises re/code. Twitter: @Recode

---

Protecting Your Data Online

69. Avoid sensitive transactions on public Wi-Fi.

Working at the local coffee shop may have some appeal, but relying on a public Wi-Fi connection means your data is interceptible by outsiders. Avoid conducting banking transactions and sending other sensitive information over a public Wi-Fi network. "Public wi-fi 'hotspots' in public places like cafés, airports, hotels and libraries are convenient but unlike your home computer, use of public hotspots involves security compromises. It is easy for other users to intercept your data, so be careful about what information you send or receive while connected. Try and limit activity when connected to a public wi-fi network to web browsing and avoid banking or any other activities that involve user password access. Avoid using hotspots that are run by people you do not know or trust. Criminals can set up hotspots known as 'evil twins' and 'rogue hotspots' to steal users' information. Always try and use encrypted (password protected) networks," advises Stay Smart Online. Twitter: @CommsAu

70. Use website privacy settings.

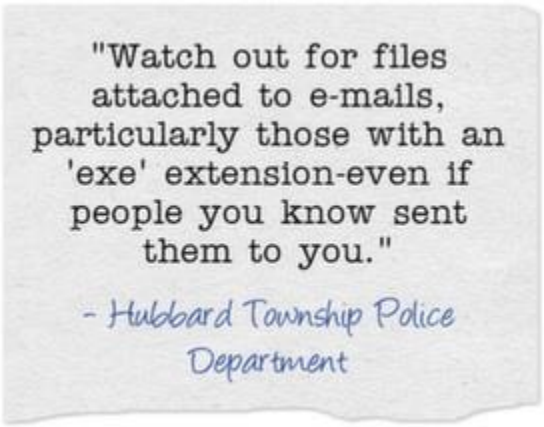
Websites other than social networking platforms also offer some privacy options. YouTube, for instance (which could arguably be considered a social networking platform, as well), allows users to make videos private or viewable only by specified persons. "You can often find privacy controls on a site by navigating to a control panel or settings menu. Sometimes, websites will draw attention to privacy controls while in other cases they will group them under broader categories like "Account Settings". Privacy controls may also be offered during the sign-up process for a new online service or account. To best protect your

privacy you should explore and understand privacy controls available to you on a given website/platform before you share personal information on or with the site," recommends TRUSTe. Twitter: @TRUSTe

71. Don't forget to sign out.

Signing in to online services is necessary when you need to access your personal accounts, but many users forget to sign out when they're finished using a service. "But when using public computers like in a cybercafe or library, remember that you may still be signed into any services you've been using even after you close the browser. So when using a public computer, be sure to sign out by clicking on your account photo or email address in the top right corner and selecting Sign out. If you use public computers often, use 2-step verification to help keep your account safe, and be extra careful to sign out of your accounts and shut down your browser when you have finished using the web," according to the Google Safety Center.

72. Don't open emails from people you don't know.



If you receive an email from a source or individual you don't recognize, don't open it, and definitely avoid clicking any links or file attachments. The Hubbard Township Police Department in Ohio suggests, "Delete email from unknown sources. Watch out for files attached to e-mails, particularly those with an 'exe' extension-even if people you know sent them to you. Some files transport and distribute viruses and other programs that can permanently destroy files and damage computers and Web sites. Do not forward e-mail if you are not completely sure that any attached files are safe."

73. Use two-factor authentication.

Two-factor authentication is an additional layer of security that provides protection in the event that a hacker guesses or cracks your password. Two-factor authentication requires a second verification step, such as the answer to a secret question or a personal identification number (PIN). You should opt for two-factor authentication when given an option. "Some websites, such as Google, will text you a code when you login to verify your identity, while others have small devices that you can carry around to generate the code. Authenticator apps are also available on all major smartphone platforms. Other

types of two-factor authentication do exist as well, so look in the settings of your banking, shopping, and e-mail hosts for the option," explains the Webroot Threat Blog. Twitter: @Webroot

74. Don't believe everything you read.

This tip is important for much beyond data protection, such as protecting your financial assets, your reputation, and perhaps most importantly, your personal confidence or self-worth. Too many people have fallen victim to scams online, by buying into false claims and promises of vast accumulation of wealth. Michael Daniel, on The White House Blog, advises, "Be cautious about what you receive or read online – if it sounds too good to be true, it probably is." Best-case scenario is you lose a few bucks buying into a pyramid scheme that will never net you any profits; worst-case, your personal information is sold and your identity stolen. Twitter: @WhiteHouse

75. Use secure websites, especially for sensitive transactions.

When you're conducting a financial transaction or sharing other sensitive information, always use a secure website to do so. Secure Socket Layers (SSL) is a commonly used website security protocol that provides additional protection for data as it's transmitted through the Internet. You can tell if you're using a secure website by looking at the beginning of the URL. Those beginning with https:// are secure. "Web browsers such as Internet Explorer and Firefox display a padlock icon to indicate that the website is secure, as it also displays https:// in the address bar. When a user connects to a website via HTTPS, the website encrypts the session with a Digital Certificate," explains Instant SSL. Twitter: @Comodo_SSL

76. Avoid clicking on links in emails.

Most everyone gets the occasional email from their bank, financial institution, or similar accounts and services. But to be safe, you should always open a browser window and type the URL in the address bar, rather than click on links in emails. Why? Phishing emails are one of the most common ways hackers obtain personal information, tricking users into inadvertently handing over their login credentials to bank accounts, credit cards, and other accounts where they can glean further information, make unauthorized purchases, or even steal your identity. "Don’t get caught by phishers. Phishing is when you get an email or a social media message that looks like it’s coming from a legitimate place such as a bank or social networking site. If you click on a link in the message, you're taken to a website that looks

legitimate but could be run by criminals trying to trick you to sign in with your username and password so they can capture that information. Your best bet is not to click on the link but rather type the web address (such as mybank.com) into your browser window and go to the site that way," the Google Safety Center recommends.

77. Be mindful of your online reputation.

Any information you enter on social networking websites, accounts, or any other website could potentially be up for grabs in the event of a data breach. In general, the information you put online contributes to your online reputation, which can impact your chances of securing employment, getting into your college of choice, and create many problems if the information is unfavorable. Monitoring your online reputation can also help you pick up on sensitive information that shouldn't be publicly available so you can take action to have it removed. Microsoft suggests searching all variations of your name, avoiding searching for personal identification numbers (such as your driver's license number or Social Security number), and asking website owners to remove this information if you find it published. You should also check sites you frequent, as well as social networking websites, so that you can clean up your profiles if necessary. Twitter: @MSFTnews

78. Don't download files from untrustworthy websites.

Websites like peer-to-peer file-sharing platforms are not only illegal, but they're often rife with malware. Avoid downloading files from any website that you don't trust completely. "According to a press release released this morning, the research found that of the 30 top pirate sites, '90% contained malware and other 'Potentially Unwanted Programmes' designed to deceive or defraud unwitting viewers.' The 'Potentially Unwanted Programmes' category is rather broad, and includes popups and ads that link to download managers. In addition, the report links one-third of the sites to credit card fraud. 'The rogue sites are also rife with credit card scams, with over two-thirds (67%) of the 30 sites containing credit card fraud,' the press release states," per a May 2014 report on BeforeItsNews.com.

79. Consider using a disposable email.

A disposable email account is one created solely for a specific purpose that you'll never use again or for any other account or purpose. "We live in a world where there are so many things that are disposable and email addresses can be added to that list. With the many free online email accounts that take just a few minutes to set up, it's easy to create an email address that can be disposed of after it has served its purpose. There are many instances where such a disposable email will make sense. Examples include short-term projects, an email address specific to one online application (such as Facebook or Twitter,) for testing purposes, etc; basically, anytime you are unsure of the period of use, like when you decide to take on numerous free software trials," GetApp explains. Twitter: @GetApp

80. Take advantage of secure mobile access options.

Some online services offer secure mobile access options, enabling users to access services without exposing login credentials. "Keep sensitive personal information and bank account numbers/passwords off your phone. Some banks offer secure mobile access without having to expose your account information or passwords," says Bank of America. Twitter: @BofA_News

81. Opt out of ad tracking.

An article on MakeUseOf addresses the issues that arise from ad tracking online: "Advertising is a huge business. We've written before about how online ads are used to target you and this goes even further with social media ads. You have to expect a level of this behavior while using the Internet, but there are ways to limit how much information is collected about you." For tips on how to opt out of ad tracking on Windows devices, click here. Twitter: @MakeUseOf

82. Don't save passwords in your browser.

Another useful tip from MakeUseOf, this advice suggests that the common practice of 'remembering passwords' in browsers is a dangerous practice. Indeed, should someone gain access to your computer

or mobile device, they'd be able to easily access any accounts for which you've stored login credentials in your browser. While it may make logging in more convenient, it's a risky habit in terms of data protection. "Keep an eye out for these pop-ups and be sure to deny them." Twitter: @MakeUseOf

83. Use more than one email address for different contexts.

Much like using the same password for multiple accounts, using the same email address for every account is a recipe for disaster. That's not to say that you can't use the same email address more than once, but a good strategy is to use a different email address for different contexts, such as one for personal accounts, one for business-related accounts, one for online retail accounts, and so on. Rich from Securosis says, "One of my favorites is to use different email accounts for different contexts. A lot of security pros know this, but it's not something we have our less technical friends try. Thanks to the ease of webmail, and most mail applications' support for multiple email accounts, this isn't all that hard. Keeping things simple, I usually suggest 4-5 different email accounts: your permanent address, your work address, an address for buying online when you don't trust the store, an address for trusted retailers, and an address for email subscriptions." For more suggestions on the types of accounts to use with each email account, click here. Twitter: @securosis

84. Create a dedicated email address for long-term projects.

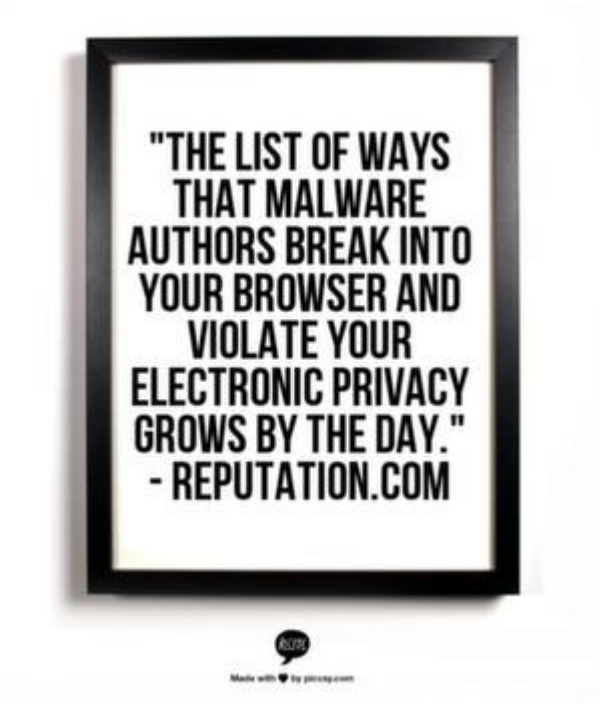
GetApp.com also offers a list of compelling reasons for maintaining multiple email accounts, suggesting creating a dedicated email account for a long-term project. That way, should you need to hand over the work or the position to someone else, you can simply pass along the login credentials rather than worry about forwarding emails for weeks and months to come. "If you are engaged in a long-term contract or project, having an email address dedicated to that specific project makes sense if you are ever transferred or move jobs. You can just hand over the email address and password to your replacement." Twitter: @GetApp

85. Take stock of your digital footprint.

Akin to evaluating your online reputation, taking stock of your digital footprint involves investigating your online presence, but to find old accounts that you no longer use. "With your digital information scattered everywhere over the course of a lifetime, it's important to think about what valuable

information you have where. For example, how many web sites are storing your credit card information? How many have up-to-date card numbers and expiration dates? Where do you have important documents, files and videos across the web? You can start by making a list and noting the types of sensitive data associated with each site. If there are sites you no longer use, you might want to consider deleting your account profiles," explains Unisys. Twitter: @unisyscorp

86. Protect your browser with sandboxing.



"In the past most viruses targeted your operating system, but nowadays the browser is the bigger prize for hackers. The list of ways that malware authors break into your browser and violate your electronic privacy grows by the day. One of the scariest is the “drive-by download,” where malicious code installs itself automatically when you visit a compromised website. However, a foolproof defense against browser exploits like drive-by downloads does exist: sandboxing. When a browser is sandboxed, it can only access the few resources necessary to do its job. Any other piece of software that tries to install itself, such as a virus, will be blocked. To date, only one browser includes sandboxing by default: Google Chrome. The Chrome browser also sandboxes the ubiquitous Flash plugin, providing yet another level of protection. For other browsers, you need to take sandboxing precautions into your own hands. For Windows users, the Sandboxie program allows you to sandbox anything running on your machine, and you should sandbox both your browser and your Flash installation," explains ReputationDefender. Twitter: @ReputationDef

87. Be careful when searching in categories known for malware.

This is a difficult tip to adequately describe in a relatively small number of words, but use caution anytime you're searching for any topic known for spam or malware. This often happens with extremely

popular search topics, such as pharmaceuticals, celebrities, and adult-oriented content. Because so many people search for these topics, it's easy for hackers to set up websites that are essentially fake, designed solely to elicit clicks and execute malicious files. "Googling your favorite celebrities can be a dangerous business if you don't recognize the sites you are clicking on. Many Google results of famous celebrity names lead to infecting your PC with malware and viruses," according to this article on PopSugar. Twitter: @POPSUGARTech

88. Don't send passwords or account login credentials over public or unsecured Wi-Fi networks.

"Never, ever send account and password information over an open (unsecure) wireless connection.You are broadcasting to everyone within the radius of your wireless signal, which can be several hundred feet, all of your personal information and account information. They can use this to compromise your accounts (e.g. email, financial, system/application access), steal your identity, or commit fraud in your name," warns the Office of the Chief Information Officer at The Ohio State University. Twitter: @TechOhioState

89. Store your most sensitive data locally.

Instead of backing up all your data in the cloud, particularly a cloud storage provider with security measures you're not completely confident in, consider backing up your most sensitive information locally or on a removable storage device you can keep under tight wraps. "I doubt there's such a thing as real privacy on the internet, so personally I wouldn't trust storing my top secret files in the cloud. Call it paranoia, but identity theft is on the rise and I just don't want to risk any of that. In any case, we probably don't have to look at our most sensitive data through the cloud on a 24/7 basis. My advice is to keep only those files which you need to access frequently and avoid putting up documents containing

passwords for your various online accounts or personally identifiable information (PII) such as your credit card numbers, national identification number, home address, etc. If you must include these information in your files, make sure to encrypt them before you upload," says Michael Poh in an article on Hongkiat. Twitter: @hongkiat

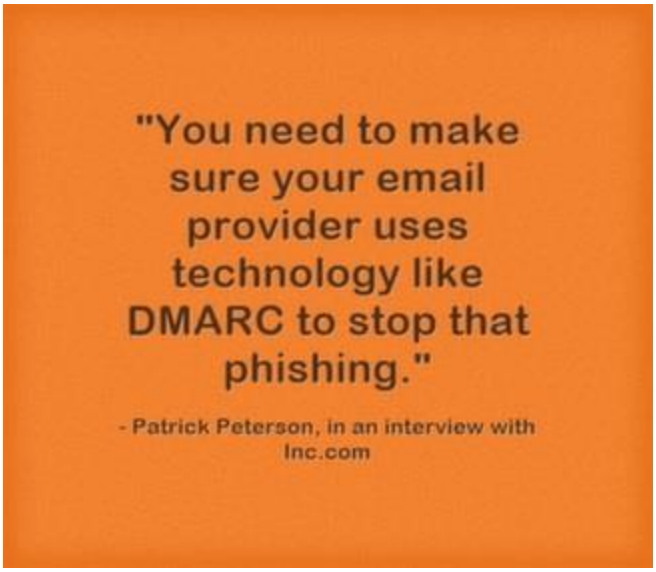
90. Regular password changes might not actually be necessary.

Frequent password changes has long been advice offered in security circles, but the practice's efficacy has come into question in recent years. "Security expert Bruce Schneier points out that in most cases today attackers won't be passive. If they get your bank account login, they won't wait two months hanging around, but will transfer the money out of your account right away. In the case of private networks, a hacker might be more stealthy and stick around eavesdropping, but he's less likely to continue to use your stolen password and will instead install backdoor access. Regular password changes won't do much for either of those cases. (Of course, in both instances, it's critical to change your password as soon as the security breach is found and the intruder blocked.)," says an article on NBC News. Twitter: @NBCNews

91. Use an encrypted cloud service.

While cloud storage makes for an ideal backup solution, it can also be more prone to hackers if you're not careful about the cloud services you choose. Victoria Ivey, in an article on CIO.com, suggests encrypting the data you store in the cloud or using a cloud provdier that encrypts your data for you. "There are some cloud services that provide local encryption and decryption of your files in addition to storage and backup. It means that the service takes care of both encrypting your files on your own computer and storing them safely on the cloud. Therefore, there is a bigger chance that this time no one -- including service providers or server administrators -- will have access to your files (the so called "zero-knowledge" privacy). Among such services are Spideroak and Wuala." Twitter: @CIOonline

92. Choose a safe, reputable email provider.



Much like not all cloud storage providers are created equal, neither are email providers. Inc.com interviews Patrick Peterson, Patrick Peterson, the founder and CEO of San Mateo, California-based email security firm Agari, about data protection, password management, and choosing safe service providers. "Be sure yours provides proper security. 'There's been technology development that stops people from impersonating your ISP, your bank, or your travel site," Peterson says. "You need to make sure your email provider uses technology like DMARC to stop that phishing. The good news is that Google does it, Yahoo does it, Microsoft supports it, AOL supports it, so if you're on one of those, you're on your way to minimizing your risk.'" Twitter: @WillYakowicz

---

Data Protection Following a Data Breach

93. Immediately change your passwords following a data breach.

If a company through which you have an account has suffered a data breach, immediately change your password. An article on ConsumerReports.org discusses the JPMorgan Chase data breach, offering tips for consumers to take steps to protect their data after a breach. "We still recommend online and mobile banking, because it allows you to watch your account in real time from almost anywhere. Yes, it's now clear that Internet banking is not impervious to hacking, but 'the convenience you get from banking digitally greatly supercedes any security risk,' said Al Pascual, head of fraud and security research at Javelin Strategy and Research, a California-based financial services industry consulting firm. As part of your monitoring, watch out for changes to your debit card PIN." Twitter: @consumerreports

94. Verify that a breach has, in fact, occurred.

There are many opportunists who use the likelihood of a data breach to trick unassuming consumers into actually handing over their passwords and other information, when a data breach hasn't actually occurred. Before responding to any requests to update your login info through a link sent to you in an email, visit the company's website by typing the URL into your address bar and confirming the breach occurred, or call the company to verify the information. "First, make sure that your card information has actually been compromised. If you receive a notification via email requesting 'confirmation' of your card information, don’t respond – it could be an opportunistic fraudster. Check the merchant’s website for news about a breach or reach out to customer support for details," says the Electronic Transactions Association (ETA). Twitter: @joxman

95. Request a new card, if applicable.

If a data breach has affected a company that has issued you a card, such as a bank-issued or retail store-issued credit card, cancel your existing card and request a new one. This action makes the previous card number invalid, so if it has been stolen by hackers, it is no longer usable and your finances are secure. "You may be able to do this through your issuer's customer service department, or through the lost and stolen card department. Some companies will charge a small fee for a replacement card, but most will swap cards for you for free. When you request a new credit card, your old card and its number are destroyed. That means that if a thief tries to use your card in the future, the card will be declined. You will have to wait for the new card to arrive in the mail, so make sure you have money to pay for your purchases during this time," says CT Watchdog. Twitter: @ctwatchdog

96. Consider a credit freeze.

This is a major step, but one that can be especially helpful if you suspect or know your identity has been stolen. It's possible to restrict access to your credit reports, meaning that thieves who are assuming your identity and attempting to open accounts in your name won't be able to do so. "Also known as a security freeze, this tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to look at your credit report before approving a new account. If they can't see your file, they may not extend the credit. To place a freeze on your credit reports, contact each of the nationwide credit reporting companies: Equifax, Experian, and TransUnion. You will need to supply your name, address, date of birth, Social Security number and other personal information. Fees vary based on where you live, but commonly range from $5 to $10," according to a Consumer Information article from the Federal Trade Commission. Twitter: @FTC

97. Take advantage of free credit monitoring.

If a major corporation suffers a data breach and your account information has been compromised, the company may offer affected consumers with free credit monitoring services. "If your personal information is hacked, the company that was victimized will probably offer you credit monitoring. (Although a Chase bank spokeswoman told CNBC that credit monitoring would not be provided to customers affected by this week's breach because no financial information was compromised.) If it does, go ahead and take it," says Bob Sullivan in an article on CNBC. Twitter: @CNBC

98. Don't ignore reports from friends about mysterious emails coming from your accounts.

One of the most common ways people learn they've been hacked is when their friends or family members report receiving an odd email or social media message, or even seeing strange updates posted on social media profiles. It's easy to ignore these warnings and assume it's some sort of fluke or someone who simply changed the "reply-to" when sending a spam email, but this is often a sure indicator that your account has been compromised. Don't ignore these tips.

99. Know the warning signs that your data has been breached or that you've been hacked.

There are many possible indications that an account has been hacked, your identity stolen, or your data breached in some other way. Educate yourself on the warning signs of a potential breach and create positive habits for monitoring your personal data security to identify potential attacks or breaches before they escalate to devastation. Read up on data protection tips (such as the guide you're reading right now) and on information outlining the common warning signs of a data breach or hack, such as this list of "11 Sure Signs You've Been Hacked" from InfoWorld. Twitter: @infoworld

100. Regain control over your compromised accounts.

All too frequently, if one account has been hacked, your data is no longer secure on other accounts using the same login information, particularly if you use the same password for multiple services. "Regaining control of a hacked email account can be tougher. You'll have to contact the email provider and prove that you're the true account holder. Of course, if the hacker changes your password, you can't use your regular email to contact the provider. It's important to have more than one email address, and make each the alternate contact address for the other. Did you use your email address as a username on other sites? That's certainly a common practice. But if you also used the same password that you used for the hacked email account, those accounts are now compromised as well. Even if you didn't use the same password, you could still be in trouble. Think about this. If you forget a website password, what do you do? Right—you click to get a password reset link sent to your email address. A smart hacker who has control of the email account will quickly seek your other accounts, social media, perhaps, or worse,

shopping and banking accounts," explains Neil J. Rubenking in an article at PCMag. Twitter: @neiljrubenking

101. Find out precisely why the breach or hack occurred.

If your account has been hacked, your data lost, or device stolen, consider it a learning opportunity. Find out exactly what went wrong and how you could have protected your data by taking better precautions. "While you are fixing things, it's a good time to take a step back, and ask yourself a more basic question: What was the reason for the breach? If it was your bank account, the answer may be obvious. In other cases, such as e-mail, it can be for a host of reasons — from using it to send spam, to requesting money from your contacts, to getting password resets on other services. An attacker may even be trying to gain access to your business. Knowing why you were targeted can also sometimes help you understand how you were breached," says Mat Honan at Wired. Twitter: @WIRED

Original Article Link:

https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe