DATA PROTECTION TIPS

DIGITAL GUARDIAN®

How to Keep Your Passwords, Financial & Personal Information Safe

Here are 101 Data Protection Tips to help you protect your passwords, financial information, and identity online.

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. Here is 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 Connected Devices

1. 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

2. 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

3. 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

4. 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

5. 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

Data Protection Tips For Mobile Devices

6. 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

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

While it's not all-inclusive, MyPermissions.com 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

8. 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

9. 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 DeviceCheck.ca, formerly known as ProtectYourData.ca. Twitter: @CWTAwireless

10. 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."

Protecting Your Identity

11. 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

12. 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.

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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.

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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

25. 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

Protecting Your Data Online

26. 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."

27. 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

28. 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

29. 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

30. 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

Data Protection Following A Data Breach

31. 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

32. 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

33. 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.

34. 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

35. 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

ABOUT DIGITAL GUARDIAN

Digital Guardian's data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats. By harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.

DIGITAL GUARDIAN®

SHARE

Copyright © 2018 Digital Guardian, Inc. All rights reserved. Digital Guardian and Security's Change Agent are trademarks of Digital Guardian, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.