RAPID7

Protecting Your Digital Life

January 2021

Technology enriches our lives in amazing ways every day, but it's also important to remember that it can also expose you to risk. Literally anyone who uses internet-connected technologies could fall victim to a cyber-attack—you don't need to be someone high-profile, as most attacks are either automated and untargeted or perpetrated by someone you know. The good news is that a few changes can make a huge difference in helping you protect your digital life. The advice below is designed to be practical, straightforward, inexpensive, and relevant to pretty much everyone. We have broken up the recommendations into two sections: Section 1 contains the six most fundamental steps, which create a baseline every internet user should adopt to protect themselves. Section 2 contains additional steps for those who want to do more or have additional concerns in specific areas.

Section 1: The Fundamentals

1. The password for your primary email account should be unique.

You have to give your email address to pretty much anything you engage with in your digital life, and for most people, there is a primary email account you use that is connected to everything. If an attacker gets access to this email account, they can potentially use it to reset your passwords for any other digital account you have, meaning they basically have control of your entire digital life (and quite possibly some aspects of your physical life, too). In other words, your primary email account is a very valuable asset. We recommend you create a password for this account that is totally separate from any other password you use.

In an ideal world, you will have unique passwords for everything you sign up for, but we understand that is pretty challenging. See our third recommendation below for a suggestion on how to make this more manageable.

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_1

2. Use three random words to create strong passwords.

Every site or app has its own set of requirements for passwords, and security experts frequently offer different advice on how to create strong passwords. Unfortunately, these pieces of advice can be confusing and even unhelpful. Some people will advise that you should avoid real words and fill your passwords with mixed characters. While including numbers and special characters does make your password harder to hack, real words are generally easier to remember, and length of password matters more than complexity. Try putting three real words together. You can add numbers or special characters to make it even harder to hack, but start with the three random words. Avoid using very obvious, easily guessed words or phrases, such as "password", the name of the site or app, the time of year, or the name of a famous person. These are all words hackers will try opportunistically to access accounts. You could use words from a song or book you find memorable, or perhaps choose three unconnected items you can see at the time of setting your password.

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_2

3. Store your passwords somewhere safe and accessible.

It's best to use a unique password for every account you have, but that results in an unmanageable number of passwords to remember. Recognizing this, many browser providers have built capabilities into their browsers to securely save and store your password, and automatically provide it when you need it to access an account. Another way of doing this is to use a password manager (such as LastPass or 1Password) that will also help you generate unique passwords, and, when necessary, securely share passwords with designated individuals (for example, for your Netflix account). For those who prefer a less tech-reliant approach, it is totally fine to write passwords down as long as you do not leave them somewhere that is visible to others, or carry them around with your laptop or other valued device.

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_3

4. Turn on a second layer of protection for your accounts (2FA)

Having unique and hard-to-guess passwords is important, but it's not a magical silver bullet that will make you invulnerable. You may be tricked into giving out your password, or an attacker may be able to guess it. In situations such as these, having a second requirement that proves you are the account owner will stop an attacker from being able to access your account. This is referred to as two-factor authentication (2FA) or multi-factor authentication. The second factor might be a code sent to a trusted device, a physical token (such as scannable key fob), or a biometric token such as your fingerprint or a facial scan. You do not have to set up 2FA on everything (though it definitely doesn't hurt to do so), but we strongly recommend you add it to anything holding sensitive information, such as your online or mobile banking apps, and devices such as your mobile phone.

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_4

5. Let your computer update as soon as it asks, or set it to automatically update

The software that runs our apps and devices is incredibly complex and written by humans at a particular point in time, and as such, it may contain unintended bugs or it may age out as technology advances. To combat this, many technology providers will issue updates or "patches." Not only are these updates likely to make your apps or technology run better, but they will often contain fixes for potential security issues. On some devices or apps, you will need to grant permission for these updates to install. This will often be the case for your computer or mobile device. It is imperative that you accept and install these updates as soon as possible. Yes, it's totally annoying having to wait for them to run, and even more so if it necessitates a restart of your device, but just remember that your device will run better and more safely after you do so, and stop putting it off!

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_5

6. Backup your data

In the age of ransomware, regularly backing up your data is a sensible idea so it cannot be held hostage, and you can restore it, if needed. This is not just good security advice—there are all sorts of research studies offering stats on accidental deletion and loss of data or devices. The cost of storage is now so low that backing up should be a no-brainer. In addition, your technology providers may offer backup options, such as Apple iCloud, Google One, or Microsoft OneDrive. These are great, easy-to-use, and cost-effective options.

Further reading: https://www.ncsc.gov.uk/cyberaware/home#section_6

Section 2: Embracing a More Secure Digital Life

Protecting your identity and sensitive information

Don't overshare!

Information you share online can be used to target you in a variety of ways, from making it easier for attackers to guess your password or the answer to your secure recovery questions, to making you easier to phish or stalk. You may think there is no way you would ever be a target, but these activities are far more common than you may know. Be careful of what information you share and how it may be used against you. Even something as innocuous as your pet's name or the high school you attended can get you in trouble. The other aspect of this is that when you select password recovery questions, it's important to choose things that are not a matter of public record.

Further reading:

- Computerworld - Sarah Palin goes the way of Paris Hilton: https://www.computerworld.com/article/2779812/sarah-palin-goes-the-way-of-paris-hilton.html
- Get Safe Online - Cyberstalking: https://www.getsafeonline.org/protecting-yourself/cyberstalking/
- Tom's Guide - 11 Simple Tips to Avoid Identity Theft: https://www.tomsguide.com/us/avoid-identity-theft-how-to,news-18552.html

Be cautious when sending sensitive information

As we increasingly conduct our personal business online, we send more and more sensitive information in ways that put us at risk. Financial or medical information, as well as documents proving identity, address, or employment information, can all have value to attackers. This is highly sensitive information that can be used for identity theft or to cause other harms if it falls into the wrong hands.

Data is most at risk when it is being sent. If an organization asks you to send this information, ask them for a secure way for them to receive it, such as uploading it directly to a secure web page, or sending through a secure file transfer system. Organizations seem to rarely offer this to individuals (even when they have them), so be sure to proactively ask for it. **You should never send bank details, identity information such as NI or taxpayer numbers, passport scans or details, or other key identity information over standard email.** If you are dealing with a financial or legal organization that does not have a secure means of sharing data, you should find an alternative organization to work with, as they clearly don't value your privacy.

In addition, thanks to various recent privacy regulations, organizations are increasingly eager to provide information on their privacy policies, offering transparency about who will see information or how long it will be kept. You should take the time to familiarize yourself with this privacy information and ask questions if you have any concerns.

Further reading:

- UC Santa Cruz - Protect Information When Using the Internet and Email: https://its.ucsc.edu/security/internet.html

- Computerworld - Top 10 File-Sharing Options: https://www.computerworld.com/article/3262636/top-10-file-sharing-options-dropbox-box-google-drive-onedrive-and-more.html

Configure your privacy settings

Most apps or devices you use should have privacy settings that you can configure. Often, when you are first setting these apps or devices up, you will be presented with options or informed that you can adjust your privacy settings later. In general, it's best to err on the side of caution—for example, limiting apps to only being able to access other functions or data while they are in use. Another good idea is to limit who can see, follow, tag, or connect with you on social media. If you did not do this at setup, take some time to go through your settings now—we challenge you to reconfigure at least three options to increase your privacy!

Further reading:

- Techlicious - The Complete Guide to Facebook Privacy Settings: https://www.techlicious.com/tip/complete-guide-to-facebook-privacy-settings/
- National Cybersecurity Alliance - Update Your Privacy Settings: https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/

Don't give out your information free with your old tech

Eventually our tech starts to feel outdated or stops working. You may decide to throw it out, sell it, or donate it, but be cautious, as even if you use the device settings to "wipe" the data or restore factory settings, your information may still be recoverable. Unfortunately, there's no simple one-size-fits-all solution to this problem unless you want to use a sledgehammer. It's best to research the specific device online and look for recommendations for how to ensure the data has definitely been cleared before disposing of the item.

Further reading:

- Rapid7 blog - Buy One Device, Get Data Free: Private Information Remains on Donated Tech: https://blog.rapid7.com/2019/12/23/dont-spread-this-holiday-cheer-how-to-secure-your-leftover-technology/
- Federal Trade Commission - How to Protect Your Data Before You Get Rid of Your Computer: https://www.consumer.ftc.gov/articles/how-protect-your-data-you-get-rid-your-computer

- National Cyber Security Centre - Buying and Selling Second-Hand Devices: https://www.ncsc.gov.uk/guidance/buying-selling-second-hand-devices

Phishing: Avoid taking the bait

Phishing is currently the No. 1 most successful form of cyber-attack in the world. Phishing attacks are designed to trick individuals into taking an action or divulging sensitive information. Phishing attacks can be untargeted "mass" attacks or highly targeted attacks that leverage publicly available information about you to make them seem more credible (this is called "spear phishing"). Bear in mind that you might be the target of a phishing attack either as an individual or as an avenue to another individual or organization. Phishing typically happens over email or messenger, but there are also telephone- or mail-based versions. To avoid falling victim to a phishing scam, it's best to operate under a philosophy of "trust but verify." Rather than clicking on a link directly, try googling for it. If a contact asks for help or information that is sensitive or concerning, speak to them directly or check with someone else who can verify the request is real before following through.

Further reading:

- NCSC - Dealing With Suspicious Emails, Phone Calls, and Text Messages: https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- Federal Trade Commission - How to Recognize and Avoid Phishing Scams: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
- Rapid7 blog - Foiling Phishing: https://blog.rapid7.com/2013/10/02/national-cyber-security-awareness-month-foiling-phishing/

Protecting your devices and yourself

Protect your home network

Even before the advent of home working brought on by the COVID-19 pandemic, home networks had become increasingly critical to the running of the household. Thanks to the wide adoption of smart devices, the explosion of on-demand entertainment, and the increasing reliance on communications networks, a reliable and secure home network is an absolute necessity. Bear in mind that a successful attack against your home network would likely allow an adversary to access all sorts of devices and information about you, so it's important to take some steps to protect this vital asset.

Further reading:

- Federal Trade Commission - Securing Your Wireless Network: https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network

- Rapid7 blog - Working from Home? Wi-Fi Security and Tips and Tricks: https://blog.rapid7.com/2020/03/30/working-from-home-wi-fi-security-and-tips-and-tricks/
- PC Magazine - How to Secure Your Internet of Things: https://www.pcmag.com/news/how-to-secure-your-internet-of-things

Beware of cameras and smart devices

Smart devices or “internet of things” devices offer a lot of fantastic benefits, including productivity and convenience gains, and even physical security advantages. It’s important to remember that these devices rely on sensors that effectively spy on you—either in the form of cameras, microphones, or the collection of usage data. This in itself does not have to be an issue, but these devices also connect to networks, which may make them accessible to malicious actors who can use the information to gather information about you, such as when your house will be empty. It’s important to set up passwords or change the default password if the device has one. It is also highly recommended to research the devices for known security issues in advance, and to ask the retailer or manufacturer about their approach to security.

Further reading:

- BBC News - Smart Camera and Baby Monitor Warning Given by UK's Cyber-Defender: https://www.bbc.co.uk/news/technology-51706631
- National Cyber Security Centre - 'Smart' Security Cameras: Using Them Safely in Your Home: https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home
- National Cyber Security Centre -Smart Devices: Using Them Safely in Your Home: https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

Practice safe surfing

Exercise judgment when visiting sites or downloading content

Not all websites should be trusted equally. Some websites may be serving up malicious content that can have negative consequences for your device and data. It’s hard to know which sites can be trusted and which should not, so internet companies have tried to help surfers out by providing an indication of their trustworthiness. When you visit a website, check whether there is a padlock to the left of the address bar at the top of your page. If there is not, there should be something telling you the site is not secure. It’s best to avoid sites that have that message.

In some extreme cases, your browser (assuming you are running an up-to-date browser) will provide a warning telling you not to visit this site. In these instances, it’s best to heed the advice of your browser. Only continue if you know for certain that the site is reputable and safe—otherwise, seek an alternative.

As an aside, be wary of content-serving sites, such as streaming sites. Some malicious actors will post "free" content as a means of delivering their malware—for example, in bootleg movies and free copies of books. Of course, not all content-serving sites are bad, and if you listen to the advice of your browser and check for the padlock, you should be reasonably safe. But, where possible, avoid downloading things from the internet unless you have a good reason to trust the source.

Further reading:

- Tech News Gadget - How to Know If a Website Is Secure: https://technewsgadget.net/2020/02/how-to-know-if-a-website-is-secure/
- Northeastern University - How Can I Tell If a Website Is Secure: https://www.northeastern.edu/securenu/how-can-i-tell-if-a-website-is-secure/

Teach your kids to be vigilant

All of the guidance contained in this document applies to any technology or internet users, regardless of age. Malicious actors can target anyone, and automated attacks generally target everyone. Just as in the physical world, though, young people represent a highly vulnerable demographic, and it is important you protect them online every bit as much as you would in the physical world. This does not mean restricting access to technology; however, it is important to educate them on the risks, share the guidance above with them, and teach them to be cautious in their interactions. Remember: Trust but verify. On the internet, it can be hard to verify that people are really who they claim to be, so teach your children to be wary and not to share too much information about themselves, or trust people they meet too readily.

Further reading:

- Federal Trade Commission - Protecting Kids Online: https://www.consumer.ftc.gov/topics/protecting-kids-online
- Get Safe Online - Safeguarding Children: https://www.getsafeonline.org/safeguarding-children/
- NSPCC - Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/