18 streetdesign
web + print + graphics

A Guide to Online Security & Privacy

I have created this guide to help you protect your personal and business information on the internet and on digital devices.

Phishing

Phishing is a technique that hackers (and other bad actors) use to try and trick people in providing information that they can use to access accounts. For example, you've probably received spam emails that pretend to be companies like FedEx telling you to click on a link or a file to get your tracking information. Those emails typically will have misspelled words or other indications that it isn't legitimate.

However, some phishing techniques can be harder to notice right away. Hackers can easily make a from address appear to be from a legitimate email (usually from a manager or director in a company). This is called email spoofing.

Here are a few tips to detect and watch out for phishing:

- Many email programs (such as Google Gmail) allow you to view the details of the email which will also show two important records: SPF and DKIM. Both SPF and DKIM are signing techniques that help to prevent counterfeiting emails. Viewing the status of either or both of those can help determine if the email is legitimate or not. In Gmail, clicking

the three dots menu for the email and choosing “show original” will display the raw information for the email as well as the SPF and DKIM status.

- Look for bad grammar and misspelled words. Many hackers are outside the United States and try to word the emails in English, but it usually doesn’t go too well.
- Before clicking any links in an email, hover your mouse over the link and view where the link will take you. In many cases, hackers will create pages on hacked sites with a single purpose: to capture login information or financial information.
- Social engineering techniques are used by hackers to try and fool employees of businesses or organizations that an email is coming from a manager or director. These emails usual request financial or other information that could be used to access business services or credentials. If in doubt, reach out to the original person and never reply directly to that email.

Check out the article on Sophos that has excellent information on phishing and how to protect yourself.

Think you can spot a phishing attempt? Take Google’s Phishing Quiz to see how well you can spot phishing on the internet and how to protect yourself.

Extortion Tactics

Hackers will use brazen attempts to extort users with made-up threats that can be distressing to many.

As more and more online services suffer security breaches, hackers will take all the login information of hacked accounts and store that data on the “dark web” where it is either provided for free or sold to other hackers. Sadly, some of the services hacked used weak or no encryption for things like passwords and other

personal information, so hackers will even have account passwords for thousands, if not millions of people.

Hackers will use that stolen information to try and extort users to pay ransoms. For example, a common technique is called “sextortion” where a hacker will send out mass emails to people telling them that they’ve hacked their computers and found their viewing history to salacious websites or that they have hijacked their computer’s camera and recorded you. The hacker will threaten to tell your friends and family (since they also claim to have hijacked your social media and address book.) They may even provide your password as “proof” of their exploit. They then demand a payment using bitcoin. Since they tell you the password you use or are using your email as the “from” address, you may think they have genuinely hacked your computer.

These types of extortion emails will only continue to grow as more and more services are hacked. For this reason, it is essential that you use a unique password for every service you use. Using the same password for everything is asking for trouble. Chances are one or more of your passwords is already floating around the dark web.

More information on these types of extortion techniques and how you can be prepared can be found on the Sophos web site.

"Juice Jacking"

See all those convenient USB charging stations at coffee shops and even hospitals? Be careful where you charge your phone using a USB charging station. Nefarious actors can use the USB connection to plant malware on your phone or download data. You're better off using a standard power supply to charge your phone instead of a USB power station. You can read more about juice jacking and how it works on the Malware Bytes blog.

Keep it Secret, Keep It Safe

One of the most common way hackers gain access to secure account is through weak passwords. Your password is the key and the lock. Storing your passwords correctly and using the right kind of password is essential to good security.

Use unique passwords.

Chances are if you are reading this you probably use the same password for all of your accounts. If you do, stop right now and change your passwords. Why? If a hacker gains access to one of your accounts, they will move down the list (now having knowledge of your other accounts) trying to gain access to other accounts you use with that same (or a subtle variation) of your password. Using a unique password for every account you use helps to prevent a domino effect if a hack occurs.

Use a strong password.

Avoid using simple words or phrases for your password. Sadly, ‘password’ continues to be one of the most used password. A good password should be something that will be very hard to guess. It’s something that doesn’t contain information that could be tied to you such as birthday or spouse’s name. (Information that can easily be obtained from social media!) The longer and more obscure your password the better.

Use two-factor authentication when possible.

Let's say you've followed all of these steps and created a unique and strong password. However, someone somehow manages to get access to your password. Panic sets in… unless you have set up two-factor authentication (2FA) on your account. Most of the major services such as Facebook, Google, Twitter, and Microsoft offer 2FA. If you have not activated that feature you need to do so. 2FA creates a second layer of security by requiring a unique code sent to your phone. So, even if someone does steal your password they would also have to have your phone to log into your account. There are even other 2FA options including USB keys that provide physical security for accounts.

Use a password manager to stay sane.

You're probably thinking, "I have dozens of accounts and you are wanting me to use unique, strong passwords for all of them? Impossible!" The solution is a password manager. A password manager works by storing all of your passwords for you in a secure encrypted vault. You need only remember one master password and the password manager manages and stores all of the other passwords for you. A solid password manager not only provides security for all of your passwords but also allows you to have strong and unique passwords for each account you use. It takes the headache out of trying to remember dozens of complex passwords. We recommend 1Password as a top-notch password manager with a solid reputation.

Keep Updated Software

We live most of our digital lives through our web browsers. Both your desktop and mobile devices utilize some kind of web browser to access most everything - including email. Be sure to keep your web browser updated to the latest versions.

Fixes for exploits and vulnerabilities are included in patches for browsers like Safari, Google Chrome and Firefox. Make sure you are always using the latest version of your browser and operating system to help protect your accounts and your computer from potential problems. Be sure also that you have the most recent versions of antivirus and anti-malware software. Malware is also a method hackers can use to cause all kinds of problems. Never download or double-click an attachment in an email that you are not sure of. Hackers can embed scripts and other nefarious code in attachments.

Browser Extensions to Protect You

The most widely used browser by far is Google Chrome. Developed by the folks at Google, it's a fairly secure browser, but as with any of the other browsers such as Firefox and Safari, it can be smart to add some additional extensions to further protect your online browsing. In addition, alternatives to Chrome like Firefox and Brave offer much better privacy and help to disconnect you from Google's tracking. One of our favorite browsers is Firefox.

One recommendation is an ad blocker. While the ethics of using an ad blocker are sometimes debated, unfortunately ads are sometimes a way that malware can be a problem and sites full of ads will slow down your browsing experience. A popular ad blocker is called UBlock Origin and works well to block ads as well as other problematic online code such as trackers.

Another recommendation is to use an extension that forces all your connections to use SSL. This ensures that your data (usernames, passwords, etc.) are encrypted completely and cannot be viewed by hackers who may be "listening in" on the local network. One such extension is called HTTPS Everywhere.

Both these and other extensions can be installed using your browser's extension feature. (Sometimes also called plugins.) The folks over at Pixel Privact have created a great article describing tips and resources on encrypting your internet traffic that you may find helpful.

Also - review the extensions you currently have installed and remove any that you are not using or that may have been installed by a malware site. (Some problems people experience browsing the web are due to a rogue or malicious browser extension.)

Have You Been Pwned?

As we've outlined in this article, it's mostly likely that one or more of your passwords has been breached and distributed on the dark web for hackers to utilize. This is why it is absolutely essential that you use unique, strong passwords for all accounts. *Pwned* is a term used by video gamers to indicate complete defeat. In the hacker world, it can mean that you've been defeated by a hacker.

Troy Hunt, a well-known security specialist, has put together an excellent resource that allows you to check if one or more of your emails has been part of a security breach and if that information has been spread to places like the dark web where hackers will get to it. This is helpful in many ways - including alerting you to breaches that your account info has been involved in so that you can change or delete your account on that service.

To check if your email has been breached and to be alerted of future breaches of your information, visit https://haveibeenpwned.com. If you use Firefox, they have partnered with Hunt's service to offer a free service called Firefox Monitor that offers the same monitoring.

Public Wi-Fi Can Be a Hacker's Playground

Try to avoid using public wifi. Free wifi at coffee shops, hospitals and restaurants are a playground for hackers. Software and devices can easily be used to "snoop" on the traffic from your computer to the wireless network. This traffic (if not encrypted) can be seen in plain text by hackers listening in on the public network. While more and more websites are using encryption (https), there are still connections that may not be encrypted.

Instead, use your mobile phone's wifi hotspot if available. This way your internet traffic is not going over a public network. If, however, you must use a public wifi be sure to use a VPN (virtual private network). A VPN encrypts all of your data as it is sent over the internet. There are many VPN services available, and your place of business may even offer VPN services to securely connect to your office network. Using a VPN is a safe and smart solution in the event you need to use public/free wifi to protect your connection and data. Just be sure you use a reputable VPN service as some may actually serve up ads and tracking.

Email is *Never* Secure

Email is one of the most open technologies on the internet. It's important to remember that email is one of the least secure methods of transmitting data on the internet. Email is almost always sent and stored in clear text on multiple servers as it goes from one server to another. Email also is often easily accessed and read by other server administrators. As an example, Google's G-Suite offers a vault option that records a copy of every email received and sent by all users for an indefinite period of time allowing administrators to easily read all contents of email. For this reason, it is never a good idea to email sensitive information such as passwords, social security numbers, tax information or other sensitive documents and content. In addition, if you email account is ever hacked, all of your saved, sent and archived email will be available to the hacker. This could put you and your clients at risk.

There are ways to encrypt email, but they are not always the easiest and require some technical know-how. There are also email services such as ProtonMail that allow you to have encrypted email, but those services may not be as user-friendly. Best rule of thumb is to assume that everything you send and receive in email is never secure.

Using Safe File Transfers

If you need to send sensitive files to another person, you should use an encrypted service to do so. (Mozilla used to have a great service called Firefox Send, but it's been discontinued.) A newer alternative is from the folks at Tresorit that allow you to send files securely from one person to another. The encryption ensures that no one but the recipient (or whoever else is given the link) can access the file due to client-side encryption. Check out Tresorit

Send to see if it is a good option for you when you need to send a sensitive file to someone.

Most cloud services such as Dropbox, iCloud, Google Drive and OneDrive are not inherently secure when it comes to the privacy of files stored there. Even though they may say the data is encrypted, it is encrypted with a key they hold, not you. This is called server-side encryption. The only truly safe method of transmitting sensitive documents is client-side encryption where *only you* have the encryption key. Services like Firefox Send use this type of encryption model. For things like everyday files that you wouldn't care if it gets out in the wild, Dropbox and Google Drive may be fine, but if you need to send information that has personal information or sensitive information it is vital that you encrypt it before sending it, or use a service that is fully compliant with client-side encryption.

Use Disk Encryption

This isn't necessarily an internet issue, but have you thought about what would happen if your laptop or computer got lost or stolen? We store our entire lives on our computers - everything from financial reports to our beloved collection of family photos. For businesses, the risk is even greater as corporate data and trade secrets could easily be let loose if data storage hardware isn't protected.

Thankfully, most all major operating systems offer disk encryption. For example, Apple has a setting called FileVault that encrypts the entire hard drive. Likewise, Microsoft also offers full device and disk encryption. When encryption is turned on, even if the device is lost or stolen the data cannot be read unless the hacker or thief has the account password. Even if they remove the hard drive and attempt to gain access that way, the data is

still encrypted. You can (and should) also typically encrypt your backup drives as well.

Be sure that the main password that you use on your computer is a strong password. If you use a weak password and still have disk encryption, it kinda defeats the purpose! Most security and privacy professionals highly recommend turning on disk encryption for your operating system. Reach out to your operating system manufacturer or your IT department for assistance in making sure your data is secure.

In Conclusion

Staying secure and safe online doesn't have to be a technical challenge. Hopefully, the tips and recommendations in this article will help you make a few steps to protect your data from the bad guys. It's also a good idea to stay updated on the latest issues that may impact you as an internet user. We routinely follow the folks over at Sophos on their blog where they post current information on all kinds of security and privacy issues on the internet.

Now go surf the web in a safer way!