Personal Cyber Security Guide

Presented to the Faculty and Staff of Hancock College

About this Guide

I created this guide as a companion to my presentation Personal Cyber Security presented to the Classified Staff of Hancock College in December of 2024. My goal was to distill the complex advice on cyber security to the most basic set of actions that you can employ to combat against the threats you are most likely to face today. By following these straightforward steps, you can significantly enhance your online safety and protect your personal information from cyber threats.

I intend for this to be a living document and to update and make changes when new circumstances arise. If you find any corrections or dead links, please email me and I will correct.

Christopher McMains - December 2024

cmcmains@hancockcollege.edu

Passwords

The Evolution of Passwords

The first defense to secure your accounts is your password. Over the years the advice on what a password "should be" has evolved. Today (December 2024) the prevailing wisdom is that length is by far the most important aspect of password security.

This is a change from the previous decade where complexity (adding in special characters and numbers) was thought to improve security the most. Passwords like "Tr0b4dor&3" were encouraged in the past because adding all the characters available on the keyboard would make passwords harder to guess.

With modern computers, hackers can brute force (or randomly guess by trying every possible combination of passwords like "aaaaa", "aaaab", "aaaac") in a decreasingly short amount of time. Using this technique, hackers are also mostly unphased by passwords using special characters. This is because, while it does take longer to guess, that increase is generally only 4 times longer than it takes to crack a password without special characters.

Every two characters added to a password makes the time required to crack a password increase by about 60 to 70 times. Using password lengths of greater than 14 requires more time than most human lifespans to crack by brute force. View this chart of estimated time it takes to crack passwords based on their length and complexity.

So how should you make long passwords? Use a technique known as pass phrases. Pass phrases are essentially random words strung together. "correct horse battery staple" is four simple English words that, when combined with spaces, total 28 characters. This is a password that is incredibly unlikely to ever be cracked by brute force methods. Pass phrases might still be susceptible to guessing attacks if you use a phrase that uses personal information.

A great tool for generating these long pass phrases is Random Passphrase Generator. I find that 4 words normally make a long secure pass phrase. Many logins still ask that you add special characters or numbers or disallow spaces in passwords. Random Passphrase Generator easily allows you to add in those required characters.

There should be two types of passwords that you use, those you remember and those you can't possibly remember. Passwords that you need to remember should be long (14+ characters) pass phrases. These should be used for logging into your computer and as we'll discuss shortly, your password manager. These pass phrases can be stored securely on paper in a safe or possibly at a relative's home.

The other type of password – those that no person could reasonably remember should be long (12+ characters) and complex. Most importantly these passwords should be stored in a software tool known as a password manager.

Password Managers

A password manager is a software application designed to store and manage your online credentials securely. It helps you generate, retrieve, and autofill complex passwords, ensuring that each of your accounts has a unique and strong password. There are a lot of good password managers out there. Below are the products that I can recommend:

- **1Password** - No free tier, but a 14-day free trial is available.
- **Bitwarden** - Free option available.
- **Dashlane** - Free option available.
- **LastPass** - Free option available.
- **Google Password Manager** – Free
- **Apple iCloud Keychain** – Free, Apple products only

Unique Passwords

Using unique passwords for each of your online accounts is crucial for maintaining strong cybersecurity. Unique passwords ensure that if one of your accounts is compromised, the breach is contained to that single account. This practice significantly reduces the risk of a domino effect, where hackers gain access to multiple accounts because they share the same password. Unique passwords also make it more challenging for cybercriminals to use automated tools to crack your credentials, thereby enhancing your overall security.

Imagine you have an account on a not so reputable website like FreeStuff4U.com, and you use the same password for your Gmail account. If FreeStuff4U.com experiences a data breach and hackers obtain your login credentials, they can easily try the same email and password combination on other popular services, including Gmail. If your Gmail account uses the same password, the hackers now have access to your email, which can lead to further security issues such as identity theft, unauthorized access to other linked accounts, and loss of sensitive information

Passwords summary

- Pick unique long passwords
- Don’t reuse passwords on multiple sites

- Remember two passwords – your computer login password and your password manager password – both of these should be long (14+ characters)
- Use a password manager
- Let your password manager remember your passwords for every other website

Multi-Factor Authentication

Multifactor Authentication (MFA) is a security measure that requires users to provide two or more verification factors to gain access to an account. This additional layer of security ensures that even if your password is compromised, unauthorized access to your account is still prevented. MFA typically combines something you know (like a password) with something you have (like a smartphone or security token) or something you are (like a fingerprint or facial recognition). This multi-layered approach significantly enhances the security of your accounts by making it much harder for cybercriminals to gain access.

It's particularly crucial to enable MFA on your most important accounts, where the potential impact of a security breach is highest. Examples of such accounts include:

- **Email accounts**: Your email is often the gateway to other accounts, as it can be used to reset passwords and receive sensitive information.
- **Cell phone providers:** Like email, cell phones are often used to reset account passwords.
- **Banking and financial accounts**: These accounts contain sensitive financial information and access to your funds.
- **Social media accounts**: Unauthorized access can lead to identity theft and misuse of your personal information.
- **Sites with private data**: Health data and information about family members can be used by criminals to impersonate you.

MFA Methods

Email and SMS are no longer considered robust options for multifactor authentication due to several security vulnerabilities. Both methods are susceptible to interception and phishing attacks. SMS messages, for instance, are transmitted in clear text, making them easy targets for interception by cybercriminals using various tools.

Additionally, SIM swapping attacks, where an attacker convinces a mobile carrier to transfer a victim's phone number to a new SIM card, can allow unauthorized access to SMS-based authentication codes.

Email-based MFA is also vulnerable to phishing attacks, where attackers trick users into revealing their authentication codes. These weaknesses make email and SMS less reliable compared to more secure MFA methods like authenticator apps or hardware security keys

Better MFA methods today do not require the sending of a code to you. Instead, these methods provide the code themselves. There are three methods that are now simple to set up and use – Authenticator Apps for mobile phones, hardware keys and a new standard known as Passkeys.

Mobile authenticator apps like Google Authenticator (Android | iOS), Microsoft Authenticator (Android | iOS), and Twilio Authy (Android | iOS) are popular choices for implementing MFA. The app is installed on a smart phone and generates time-based one-time passwords. This means that every 30 seconds a new code is created based on the time. Most apps show a count down to how long the code is valid.

Hardware security keys, such as the YubiKey, provide an even higher level of security. These physical devices use cryptographic protocols to authenticate users, making them resistant to phishing attacks and other common threats. The YubiKey 5 series, can be used by many services as an authentication method and can be plugged into a computer or used wirelessly with any current mobile phone.

Passkeys represent the future of both MFA and may even replace passwords entirely. Passkeys come in a few forms, including hardware USB keys, but they are most intriguing for personal use when they are implemented in the operating system of computers and phones. Windows, Android, iOS and macOS all have implementations of passkeys built into their operating systems. Some of the password managers listed in the earlier sections also have their own implementations. Many larger websites have started to accept passkeys as an MFA method and some even allow you to substitute passkeys for your password.

Setting Up a Passkey: When you first set up a passkey for an app or website, you'll typically be prompted to create one during the login or registration process. For instance, if you're setting up a passkey for a banking app, you'll enter your username and password as usual. Then, the app will ask if you want to create a passkey for future logins.

Creating the Passkey: You'll be prompted to use a biometric scan (usually a facial scan or fingerprint), or your device passcode to create the passkey. This step ensures that only you can create and use the passkey. Once authenticated, the passkey is securely stored on your device.

Using the Passkey: The next time you log in to the app or website, instead of entering your username and password, you'll simply use the biometric scan, or your device passcode. The app or website will recognize your passkey and log you in securely.

On this date (December 2024) the only reason to not start using passkeys is the issue of portability. Passkeys are still new and the entities that have created the standard have not

yet agreed on a way to transfer passkeys across devices, like from an iPhone to an Android phone. This will eventually get worked out but is one consideration if you think you might be switching your passkey platform in the near future.

Device Security

In today's interconnected world, securing your devices is crucial to protect your personal information and maintain your privacy. This section covers essential tips for safeguarding various types of devices, including computers, phones, network gear, and IoT devices. By following these guidelines, you can significantly reduce the risk of cyber threats and ensure a safer digital environment.

One key tip that is true for all devices is **to turn on automatic updates**. This ensures that your devices receive the latest security patches as soon as they are released. Automating eliminates the temptation to delay the process with thoughts like "I'll do it later."

Computers

AntiVirus: While mobile phones have taken up a great amount of our personal computing attention, computers are still found in most homes. In the past, additional antivirus software was always recommended. Today, Windows Defender, which comes pre-installed on Windows systems, is a robust and effective option. It provides real-time protection, frequent updates, and integrates seamlessly with the operating system. In contrast, some third-party antivirus programs can be resource-intensive, cause system slowdowns, or come with unnecessary bloatware. The surest way to prevent viruses and malware is to use reputable websites and software.

Admin Accounts: Most users should avoid running their computers with administrative privileges because it significantly increases the risk of accidental or malicious changes to the system. Running as an admin means that any action taken, whether intentional or not, has the potential to affect the entire system, including installing malware or making critical system changes. Instead, users should operate with an unprivileged account for everyday activities like browsing the web, checking email, and using applications. This limits the potential damage that can be done if the account is compromised. When administrative tasks are necessary, such as installing software or changing system settings, users can temporarily elevate their privileges by entering an admin password. This approach, known as the principle of least privilege, helps maintain system security and stability by minimizing the risk of unintended or harmful actions.

- How to check if a User Account is an Admin in Windows
- How to check if a User Account is an Admin in macOS

Phones

The smartphone has truly revolutionized the world of technology, becoming an indispensable part of our daily lives. From communication and entertainment to productivity and navigation, smartphones have integrated seamlessly into almost every aspect of modern living. One of the key benefits for their adoption is their enhanced security features, which were designed with the lessons learned from the vulnerabilities and issues that plagued the PC world.

Smartphones were built with security in mind from the ground up. They incorporate features such as sandboxing, which isolates apps from each other and the operating system, reducing the risk of malware spreading. Additionally, app stores like Google Play and Apple's App Store enforce strict security policies and vetting processes to minimize the distribution of malicious software. Regular updates and patches are also more streamlined and frequent, ensuring that security vulnerabilities are addressed promptly.

Despite these built-in security measures, there are still steps users should take to improve their security.

Downloading apps only from verified stores, such as Google Play and Apple's App Store, is very important. These stores not only vet the apps but also can pull back apps that have been reported as malicious by other users.

The NSA recommends shutting down your phone weekly. This is because most malicious activity that can be run on phones only live in the transient memory of the device. This memory is cleared each restart and is a simple way to reset your device after an infection.

Wi-Fi Pineapple attacks, which exploit vulnerabilities in wireless networks to intercept data and execute attacker-in-the-middle attacks, are increasingly being used by cybercriminals. It can be mitigated by turning off Wi-Fi autoconnect. Most phones are set up by default to remember a Wi-Fi network and try to reconnect when they see a network they recognize. But what happens when the attacker has a device that pretends to be the Wi-Fi from Starbucks? In many cases, your phone might automatically connect to this network even if you're nowhere near a Starbucks and even if you're not using your phone. This can give attackers access to your data and potentially allow them to intercept sensitive information. To protect yourself, disable the Wi-Fi autoconnect feature (Android | iOS) and manually connect to trusted networks only.

Network Gear

We connect to the internet through network gear. For most of us we have a cable or fiber line coming into our house from an internet service provider. Often, they provide a modem

and router to allow you to split that connection between many devices. I encourage you to buy your own router, as it offers more options to configure and enhance the security settings on your device. What should you look for? A reputable brand is most important – Eero, Netgear, and Asus are all good. Try to stay away from the cheapest stuff on Amazon with names that are a mix of 4 consonants and 1 vowel. Make sure to change the router default password and again remember to turn on automatic updates.

Most new routers today have a guest network available which is great for family or friends visiting who might not have followed the secure protocols that you have when you finished this guide.

Internet of Things

The Internet of Things or IoT refers to a new group of devices, often called "smart objects," and include things like thermostats, light bulbs, appliances and security cameras. Again, reputation matters. Brands such as Philips, Honeywell, Google and Ring are the safest choice.

Putting a smart thermostat on your guest Wi-Fi network is a smart security measure. It isolates the thermostat from your main network, where your personal devices are connected, reducing the risk of a compromised smart device affecting your critical devices. Guest networks typically have restricted access, meaning even if someone gains access to your guest Wi-Fi, they won't easily reach your main network devices or sensitive data.

Browsing the web

From shopping to banking to entertainment, the web has revolutionized how we interact with the world. As we continue to integrate the web into our daily lives, it's essential to stay mindful of online security and privacy to fully enjoy the benefits of this digital age.

The first question to ask is which browser to use. The answer to this question changes every year. At this date, Chrome, Firefox and Edge are all essentially equal in my eyes. All are performant but all the companies that make them do have agendas that might not square best with consumers. I have a slight preference for Safari on Apple devices, but that is only available on those Apple devices. One newer browser that might be worth looking at is Brave which by default ads some ad blocking technology to what is essentially a copy of Chrome.

Speaking of ad blocking, I strongly recommend installing one on your browsers. Three I can recommend are uBlock Origin, Ghostery and AdBlockPlus. Ad blockers speed up your page load times, protect your privacy and can prevent you from seeing scam ads. The past year has seen a number of scams where an attacker purchases an ad on a search engine like Google or Bing and pretend to be the support site for an entity like PayPal or Southwest Airlines. Unaware users will click on the ads believing them to be legitimate search results and possibly give away passwords or credit card information. Users with ad blockers installed will not even see these ads.

Email Security

Email remains the top vector for bad actors, as it is frequently used to deliver phishing attacks, malware, and other malicious content designed to compromise sensitive information and systems. The advice for personal email security is similar to the advice you are given at work.

- Don’t open messages from people you don’t expect email from.
- Don’t click on links inside emails, even if its from someone you know.
- Don’t open attachments at all, unless it is absolutely expected and necessary.

With the rise of social media and alternative channels of communication, email should become less and less a part of your personal computing life. It will be with us for a long time but try to find alternate ways of communicating. Many financial institutions have their own secure messaging system on the platform that you can use. Social media offers a better way to share photos and quick messages.

Securing your Identity

Credit Freeze

Freezing your credit is one of the simplest and most effective ways to protect yourself from identity theft and financial fraud. When your credit is frozen, lenders cannot open new accounts in your name without your permission, even if a criminal has your personal information. Data breaches and scams are increasingly common, and most people won't know their identity has been misused until real damage is done. A credit freeze is free, does not affect your credit score, and can be temporarily lifted whenever you need to apply for credit, making it a smart, low-effort step to safeguard your financial identity.

What a Credit Freeze Does (and Does Not Do)

- A credit freeze **blocks lenders from viewing your credit report**, which prevents new loans or credit cards from being opened without your permission.
- It **does not affect your credit score** and does not cancel or change existing accounts.
- Credit freezes are **free by U.S. federal law** and stay in place until you remove them.

What You'll Need Before You Start

Have these ready (you'll be asked for them):

- Full legal name
- Social Security number
- Date of birth
- Current address (and sometimes past addresses)
- Email address and phone number

This information is required to confirm your identity.

Step-by-Step: Freeze Your Credit at All 3 Bureaus

You **must do this separately** for each company. Freezing one does **not** freeze the others.

Equifax

1. Go to: **Equifax Credit Freeze Page**
   https://www.equifax.com/personal/credit-report-services/
2. Create a free account or sign in.

3. Choose **“Place a Credit Freeze.”**
4. Follow the on-screen steps and submit.

By phone: Call **1-888-298-0045** [experian.com]

Experian

1. Go to: **Experian Credit Freeze Page** https://www.experian.com/help/credit-freeze/
2. Create a free account or sign in.
3. Click **“Freeze Your Credit.”**
4. Confirm your identity and submit.

By phone: Call **1-888-397-3742** [experian.com]

TransUnion

1. Go to: **TransUnion Credit Freeze Page** https://www.transunion.com/credit-freeze
2. Create a free account or sign in.
3. Select **“Add Freeze.”**
4. Submit your request.

By phone: Call **1-888-909-8872** [experian.com]

After You’re Done

- Your credit is usually frozen **immediately or within one business day** when done online or by phone.
- Keep your **login information** safe. You’ll need it if you apply for credit later.
- You can **temporarily unfreeze** your credit anytime (for example, when applying for a loan), then turn the freeze back on.
- Consider freezing credit for young and elderly relatives.

Common Mistakes to Avoid

- Freezing with only one bureau (you must do all three)
- Paying for a “credit lock” (freezes are free by law)
- Forgetting login credentials

California DROP

DROP stands for Delete Request and Opt-Out Platform. It is a free, state-run privacy tool created by the California Privacy Protection Agency (CPPA) that allows California residents to request deletion of their personal information from data brokers in one place.

Instead of contacting dozens or hundreds of data brokers individually, a consumer can submit one verified request through DROP, which is then sent to over 500 registered data brokers operating in or affecting California residents.

Data brokers collect and sell personal information about people they do not have a direct relationship with, such as

- Names, addresses, phone numbers, and email addresses
- Purchase history and interests
- Location data
- Sensitive data like health or family information

DROP makes it dramatically easier for Californians to:

- Delete personal information held by data brokers
- Opt out of the sale or sharing of that information
- Reduce spam, scams, profiling, and identity-related risks

To use DROP, you must:

- Be a California resident
- Be requesting deletion for yourself, or

- Be an authorized person (for example, a parent for a child or a caregiver for an elderly relative)

Once submitted, data brokers are legally required to process the request within defined timelines.

You must verify that you are a California resident using the California Identity Gateway, which is the state's secure verification system. You will be asked to provide some personal information so data brokers can find your records. This typically includes:

- Full name
- Date of birth
- ZIP code
- Email address(es)
- Phone number(s)

Providing more information increases the chance that data brokers can correctly locate and delete your data, but you control how much you share.

Your request is sent to all registered data brokers at once. The request acts as both a deletion request, and an opt-out of sale or sharing of your personal data. Data brokers must retrieve DROP requests at least every 45 days. Starting August 1, 2026, brokers must delete applicable data within 90 days. Brokers must also suppress future collection or sale of your data where required by law.

DROP applies only to data brokers, not banks, employers, or companies you directly do business with.It does not remove data from:

- Credit bureaus
- Social media platforms
- Government records

You can access the platform here:

https://consumer.drop.privacy.ca.gov/

Revisions

2024-12-19 – Just one week after publishing the first version of this guide, news broke that the US Government is considering a ban of TP-Link routers due to security concerns over the company's close ties with the Chinese government.

2026-02-06 – Added section "Securing Your Identity" with instructions on requesting a credit freeze and California DROP