**Lock Down Your Login**

****

October is National Cyber Security Awareness Month, which is the perfect time of year for individuals, businesses, and other organizations to reflect on the universe of cyber threats and to do their part to protect their networks, their devices, and their data from those threats.

We invite you to participate and become actively involved in National Cyber Security Awareness Month. Everyone can do something – **it’s Our Shared Responsibility**.

**Follow these six simple steps to gain peace of mind and more control over your online security.**

Compromised accounts cause reputational harm and embarrassment and put others at risk through the spread of malware and viruses. You have enough to worry about, so what can you do about it?

## ****Protect Accounts with Strong Authentication****

**What is strong authentication?**

Strong authentication – sometimes called 2-step verification, multi- or [two-factor authentication](https://twofactorauth.org/), or login approval – provides an extra layer of security beyond your username and password to protect against account hijacking. Many online services, including email, banks, and social networks, offer this free extra security protection to help ensure it’s actually you trying to access your account – not just someone who stole or guessed your password.

**How does it work?**

Strong authentication requires you to have more than just your password to sign into your account. Strong authentication tools are widely available on major email and social networking sites. Here are the most common methods you can choose from:

* **Security keys:** A small device that plugs into your USB port or is used in conjunction with a phone, which you use when logging in.
* **Biometrics:** A fingerprint, facial recognition or other unique personal identifier, used during the login process.
* **One-time codes:** A unique code sent after entering your username and password, usually by text to a mobile device that is then entered on the site to verify it’s you.

Learn how to turn on strong authentication for major online companies by visiting: <https://www.lockdownyourlogin.org/strong-authentication/>

## ****Keep software updated****

**Why is updated software important?**

Running out-of-date software can put you at risk of security vulnerabilities that hackers seek out and exploit. Security experts agree that keeping your software — including Internet browsers, operating systems, plugins, and document editors — up to date on internet-connected devices is a fundamental cybersecurity practice and helps prevent malware infections that could compromise your devices and accounts.

**Why is preventing malware important?**

Malware can take many forms, including capturing keystrokes and passwords when they are entered, ransomware, which can encrypt files and demand payment to release them, and using devices to send out spam or participate in a distributed denial of service (DDoS) attack. If your device is infected, sharing files may also infect others.

**How do you keep software up to date?**

When you receive notification that a software update is available, install it as soon as possible. Knowing your programs and operating system is important. Some programs, like reputable antivirus/security software and some web browsers, including Chrome, automatically update. Mobile operating systems, apps, and other critical software may require your action to update.

Learn how to update your software by visiting: <https://www.lockdownyourlogin.org/update-software/>

## ****Avoid Phishing Attempts****

**What is phishing?**

Attempts by cybercriminals, nation states, or hacktivists to lure you into giving away personal information to gain access to accounts or to infect your machine with malware and viruses are called "phishing." Phishing attempts can happen through a variety of channels, including email, social media, or text messages, and can compromise security and lead to theft of personal and financial data. Highly targeted attacks on groups or individuals are known as "spear phishing".

**What tactics are used in phishing attempts?**

Phishing messages can come from hijacked accounts of people you know, making them hard to distinguish from real messages. Additionally, cybercriminals commonly use infected documents or PDF attachments as vectors for their phishing attempts. Another common trick attackers use it trying to get victims to sign in on a fake login page where their usernames and passwords can be stolen.

**How do you avoid phishing attempts?**

Phishing attempts can often get through spam filters and security software that you may already have in place, so stay vigilant and trust your instincts. Keep an eye out for things like unexpected urgency or a wrong salutation. Think twice about clicking a link or opening a document that seems suspicious. Double-check that every URL where you enter your password looks legitimate. And if anything raises doubt, delete or report the communication.

**What to do if you receive a phishing attempt?** [More Information](https://www.rsccd.edu/Departments/Information-Technology-Services/Documents/Spam%20Reporting.pdf#search=phishing)

Learn how online services help fight phishing by visiting: <https://www.lockdownyourlogin.org/avoid-phishing/>

**Use unique passwords**

**Why are unique passwords important?**

Password reuse for multiple accounts is one of the most commons ways accounts are hijacked. When passwords are reused, having your credentials stolen for one account means hackers can gain access to other accounts that use the same login details.

**What makes for a strong password?**

In addition to being unique, security experts agree that a strong password is at least 12 characters long, containing a mix of letters, numbers and symbols. Maintaining strong and unique passwords will decrease the risk of password guessing based on commonly used passwords, information about you that might be publicly available, or password cracking tools that hackers use.

**How do you manage better and unique passwords?**

It is really hard to remember a lot of strong and unique passwords. Thankfully, there are a lot of tools out there to help. Using a password manager only requires you to remember one master password to access your other passwords. If needed, you can write passwords down on a piece of paper and store them in a secure location away from your computer, but be careful not to store passwords right on your computer.

Learn how to use unique password by visiting: <https://www.lockdownyourlogin.org/unique-passwords/>

## ****Protect Your Mobile Devices****

**Why should you secure your mobile devices?**

Mobile phones and tablets contain a wealth of personal data, including emails, contacts, schedules, your locations, and direct access to apps. When your mobile device is lost or stolen, your data goes with it, making any information contained on the device vulnerable.

**How do you secure your mobile devices?**

The first layer of mobile security is locking your device with a passcode, touch ID features, or other biometric. In case your phone is ever lost or stolen, make sure you’re aware of the different offerings that exist to help you remotely locate or lock your device, or wipe data from it. Some of these features may be built in by the operating system, carrier, or available via an app. Your systems administrator might also have specific rules to follow if you lose a work device.

Here's how to protect your mobile device: <https://www.lockdownyourlogin.org/mobile-devices/>

**Use trusted security tools**

**Why use security tools?**

Many online service providers offer useful settings and tools to help you manage your online presence, keep your data secure, and get the most out of the services you use. For example, strong authentication is rarely turned on by default, but offered by many online services for users that want an extra layer of protection on their account.

**How do security checkups work?**

Guided security checkups help you understand the security settings available, and give you confidence you are using the strongest options available. And managing your notification settings, including alerts when your location is being used or when new information about you or a new photo is posted online, can help you manage your online presence.

Learn how use trusted security tools by visiting: <https://www.lockdownyourlogin.org/trusted-security-tools/>