CYBERSECURITY AWARENESS MONTH

Passwords

Passwords are the keys to your digital castle. Just like your housekeys, you want to do everything you can to keep your passwords safe.

Passwords can be made ironclad with additional authentication methods, such as multifactor authentication (MFA).

Creating, storing and remembering passwords can be a pain for all of us online, but the truth is that passwords are your first line of defense against cybercriminals and data breaches. Also, it has never been easier to maintain your passwords with free, simple-to-use password managers. With a few moments of forethought today, you can stay safe online for years to come.

Long, Unique, Complex

No matter what accounts they protect, all passwords should be created with these three guiding principles in mind:

Long

Every one of your passwords should be at least 12 characters long.

Unique

Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts remain secured. We're talking really unique, not just changing one character or adding a "2" at the end – to really trick up hackers, none of your passwords should look alike.

Complex

Each unique password should be a combination of upper case letters, lower case letters, numbers and special characters (like >,!?). Again, remember each password should be at least 12 characters long. Some websites and apps will even let you include spaces.

CYBERSECURITY AWARENESS MONTH

Passwords

How often do I change my password?

If your password is long, unique and complex, our recommendation is that you don't need to ever change it unless you become aware that an unauthorized person is accessing that account, or the password was compromised in a data breach.

This recommendation is backed up by the latest guidance from the National Institute of Standards and Technology. For many years, cybersecurity experts told us to change our passwords every few months. However, this constant change isn't helpful if your passwords are each long, unique and complex. In fact, if you change your passwords often, you risk reusing old passwords or falling into bad habits of creating similar or weak passwords

But remembering all my passwords is so hard!

You probably have a lot of online accounts. And because all your passwords should be unique, that means you have a lot of passwords. But the fact remains that using long, unique and complex passwords remains the best way to keep all of your digital accounts safe. There are many free and easy-to-use tools out today that makes managing your library of unique passwords a snap.

Today, the truth is that you don't have to remember your passwords. If you use the latest tools, you don't need to rack your brain at every login screen. You just need to remember the one password that unlocks your password manager vault.

Don't take a pass on password managers

As our lives expand while we do more online, we've gone from having just a couple of passwords to today, where we might manage upwards of 100 or more. If you're like most people, you're probably using the same password for most of your accounts—and that's not safe. If your one password gets stolen because of a breach, it can be used it to gain access to all your accounts and your sensitive information. But no need to fret, password managers are easy to use and make a big difference.

CYBERSECURITY AWARENESS MONTH

Password Managers

We've all probably used one password to secure multiple, maybe even all, of our digital accounts. But that's not safe, and it becomes even more unsafe as time goes on. If your one password gets stolen because of a breach, it becomes a skeleton key for your whole cyber life. This compromised password can be used it to gain access to all your accounts and your sensitive information.

Here's where password managers really shine. **Password managers are pieces of software that often take the form of apps, browser plugins or they might be included automatically in your browser or computer operating system. With a few clicks, you can generate new, secure passwords that are long, unique and complex. These passwords managers automatically store your passwords and can autofill them when you arrive at the site.**

You can fill in all your passwords at once, or just add a few passwords for your key accounts (email, banking and social media, for example) and add more over time.

Many times, when you log into a site, your password manager will ask if you want to store the password – click yes, and, boom, another account is secured. And to keep your password manager extra safe, secure it with multi-factor authentication (MFA).

It's safe to ditch the notebook

A password manager is like a combined security guard and butler who tags along as you surf the web, safely carrying your passwords like a ring of keys.

A password manager is best the way to create and maintain strong passwords for the every-increasing number of online accounts we log into. These programs store your usernames and passwords in a secure, encrypted database. When you need a new password, you can get a hyperstrong suggestion that is automatically stored in the password manager.

CYBERSECURITY AWARENESS MONTH

Password Managers

A password manager frees you from keeping a confusing notebook of passwords in a drawer, or a messy sticky note with all of your most important passwords stuck on your computer. Now you only need to remember the single password that unlocks your password manager vault.

Password manager advantages

Password managers not only let you manage hundreds of unique passwords for your online accounts, but some of the services also offer other advantages:

- Saves time
- Works across all your devices and operating systems
- Protects your identity
- Notify you of potential phishing websites
- Alerts you when a password has potentially become compromised

Understanding password managers

Even though password managers are the best way to keep your information safe, many people are afraid that storing all their passwords in one place means they are at risk if a hacker breaches your vault.

Password managers today are safer than ever before, and they are much safer than using a physical notebook, storing passwords in a Notes app or reusing passwords that are easy to remember.

Compare your options and look for a quality password management system – you have a lot of choices! Here is why a password manager is the best for keeping your passwords safe:

CYBERSECURITY AWARENESS MONTH

Password Managers

1. Encryption

Quality password managers encrypt all of the passwords stored on them, no matter whether the passwords are stored on your device or on the company's servers. This means that your passwords would be basically impossible to decode if a hacker tried to breach your password manager. The only access to your passwords on a password manager is with a password only you know.

2. Multi-Factor Authentication

Because your password vault on a password manager is so valuable, the best password managers require multi-factor authentication for you to log in. This means that anyone trying to view your passwords from unfamiliar device will need to log in multiple ways. This can include a facial ID, fingerprint scan, inputting a code you get in an SMS text message or approving the log-in attempt on a separate app. This builds another wall around your passwords, so you know they are kept extra-secure.

3. Zero Knowledge

As the name suggests, zero knowledge means a password manager does not know what your password is – the company does not store the keys needed to decrypt the main password that unlocks your vault. This means that your main password is never kept on the system's servers. You are the only one who knows it, so you should make it strong and protect it with MFA.

Choosing a password manager

We recommend that you compare the different password managers and find the one that works best for you with these trustworthy guides:

- Consumer Reports
- PC Mag
- CNET
- Tom's Guide
- Global Cyber Alliance