SECURING KEY ACCOUNTS AND DEVICES

Passwords and Securing Your Accounts

Passwords are like keys to your personal home online. You should do everything you can prevent people from gaining access to your password. You can further secure your accounts by using additional authentication methods.

Passwords

Passwords can be inconvenient, but they're important if you want to keep your information safe.

- Protecting your personal information starts with STOP. THINK. CONNECT.™: take security precautions, think about the consequences of your actions online and enjoy the internet with peace of mind. Here are some simple ways to secure your accounts through better password practices.
- **Make your password a sentence**: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- **Unique account, unique password**: Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.
- **Write it down and keep it safe**: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

Other Ways to Secure an Account

Typing a username and password to access a website isn't the only way to identify yourself on the web services you use.

- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media. https://www.lockdownyourlogin.org/

Over time, more websites will be adopting **strong authentication.** Strong authentication – sometimes called 2-step verification, multi- or two-factor authentication, or login approval – provides an extra layer of security beyond your username and password to protect against account hijacking. In some cases, the services may be available but are not required.

Many email services offer strong authentication on an opt-in basis. Ask your financial institution, email provider and other online services if they offer strong authentication or additional ways to verify your identity.

Find more information at https://www.staysafeonline.org