SAFE Tip Sheet
All About Passwords

Nov 2019

Passwords can be annoying, hard to remember, and inconvenient when you're in a hurry – and with the growing number of internet services available, very difficult to keep on top of all those passwords you need and use every day. But passwords and password management are important if you want to protect your privacy and keep your sensitive information safe from hackers and cybercriminals!

To help you with our ever growing number of passwords, we've provided some simple ways of creating and securely managing them all.

Creating and Securing Your Passwords

According to the National Institute for Standards and Technology (NIST), you should use the longest password or passphrase permissible. And substituting look-alike characters for letters or numbers may no longer be sufficient (for example, "Password" and "P@ssw0rd"). A password should look like a series of random characters.

- Make your passwords long & strong. Use complex passwords with a combination of numbers, symbols, and letters.
- A strong password could be a sentence, or passphrase, that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember. On many sites, you can even use spaces!
- Avoid using common words found in a dictionary.
- Passwords should have no connection to the user, so don't use pets' or people's names for your password. And avoid things like your zip code or key dates like a birthday or an anniversary, or your phone number.
- Don't use simple patterns like password1, password2, password3 for different sites—those are too easy to guess.
- Keep your passwords private—and NEVER share a password with anyone else.
- Change your passwords for sensitive websites often, like online banking, every 60-90 days.
- On the web, if you think your password may have been compromised, change it at once and then check your website accounts for misuse.

Some websites ask you to answer a security question if you forget your password. Make your answers to security questions just as hard to guess as your password. This answer should not be used anywhere else.

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. At work you should follow your company's policies on creating and storing passwords. At home, keep a list that's stored in a safe, secure place away from your computer. Alternatively, you can use a service like a password manager to generate and remember complex passwords for each of your accounts.

GET TWO STEPS AHEAD

Finally, turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security and helps verify a user has authorized access to an online account.