

Password Strategies

These days, online accounts are a way of life. Keep yours safe by using 'strong' passwords that are unique to each of your important online accounts. Most of us have accumulated tons of passwords – how do you manage them to keep you safe online? Consider the tips below.

Why do they need to be strong?

The latest password cracking software can try billions of password combinations each second (yes, that's billions with a 'b'). In addition, hackers have also expanded beyond using dictionary words found in any language to content that resides on the Internet: so things like song lyrics, Bible verses, movie quotes and other common phrases are now quickly scanned and recognized.

Why use unique passwords?

Using unique passwords protects your online accounts – if the password for one account is hacked, the others remain safe.

How do I apply these practices with so many online accounts?

Step 1: Identify your important accounts. Think email, financial and social media accounts – and include online shopping accounts that store your credit card numbers. Focus on these first.

Step 2: Develop strong passwords for these accounts. The more random and complex, the better. Here are three techniques to consider:

A reusable, nine-character technique

- First two characters are letters associated with your account
- Next three characters are a numeric combination, significant and private to you
- Last four characters are mixed-case letters, also significant and private to you
- Switch out one of the last seven characters for a symbol
- The first two characters make the password somewhat unique to each account, while the last seven characters provide a foundation that's easy to remember

Fictitious examples for Main Street Bank and Emporium Clothiers

Private, three character number: 173

Private, four character mixed case letters: AbYz

Symbol substitution: switch '7' to '@'

Passwords: MS1@3AbYz & EC1@3AbYz

Password Strategies

A phrase only you know and can remember

- Start with something like “At work I do my part to Protect the Network”
- Use the first letter of each word, or replace with a number or symbol, and use mixed case
- In this example, that phrase could become @WiD-Omp2PtN!W

At work I do my part to Protect the Network
 @ W i D-O m p 2 P t N!W

Combine random words

Combine short words using mixed case, numbers and symbols that are significant to you but random to anyone else. The more characters, the better. Example: c@tPillow9asia\$

You can test the strength of your passwords at:

<https://www.microsoft.com/security/pc-security/password-checker.aspx>

How do I remember my passwords?

It's okay to write them down – just make sure you take steps to secure that list. If someone can access it, they can access ALL of your accounts. If you write your passwords down on paper, lock it in a drawer or safe; if you keep them in a document on your computer, give it an anonymous name (not 'passwords.doc') and encrypt it, if possible. If you use an app to manage passwords (LastPass, SplashID, KeePass, 1Password, etc.), use a very strong, unique password to protect it!

What about those security questions that sites are using when I reset my password or access from a different computer?

Most sites use one or more question-and-answer combinations to reset your password if you forget it or lock out your account. Be cautious when selecting the answers for these questions. Don't use anything that is publicly known or that you've posted on social media sites. The secrecy of this information is just as important as your password. You may need it to get back into your account someday, but you want to ensure you are the only one who can do so.

A couple final tips ...

- If a company or service you use has suffered a breach, change your password for that account immediately.
- Be wary of public computers at locations such as libraries, hotels and kiosks; don't use them to access important accounts – software may be installed that can capture everything typed on that system, including your passwords and account numbers.
- Don't let your web browser save or store passwords. Otherwise, anyone with access to your computer can log into your important accounts.