8 password safety tips.



Let’s face it, we spend a lot of time on computers and mobile devices these days. We read the news, connect with friends on social media, shop, and even do our banking online. And when it comes to password safety, you probably know the basics. Don’t use the same password for all accounts. Don’t share passwords with friends or colleagues. And never use “password” as your password. Creating passwords that are as strong as possible (and that you will remember) for multiple online accounts can be difficult. But these eight tips will help keep your information secure.

1. **Make passwords a minimum of 10 characters.** When it comes to passwords, longer equals stronger. In fact, many security experts recommend crafting a complex “passphrase” instead of a “password.” An example of a passphrase is IceFishingIsColdInMarch. The Cybersecurity & Infrastructure Security Agency encourages people to think of a sentence and use the first letter from each word. Then, replace some of those letters with symbols and numbers. Using the above example, you could easily modify the passphrase as follows: I3eF!$h!ng_I$Col4*In03.

2. **Don’t use real words.** Passwords that are easy to remember can also be easy to hack. With that, we suggest avoiding words that could be found in any dictionary, in any language. Instead, use long strands of seemingly random numbers, symbols, and uppercase and lowercase letters, similar to the modified passphrase example above. Bonus points if you can avoid using any in sequential order (no ABCs or 123s).

3. **Don’t use obvious information.** Names and numbers like addresses, phone numbers, birthdays, anniversaries, etc. are publicly available and are easily accessible. Do not use them in your passwords.

4. **Use a different password for every account.** Otherwise, if one password is cracked, every account could be compromised.

5. **Consider a password manager.** Internet browsers like Safari and Chrome have free built-in password managers. However, there are also third-party services like LastPass and RoboForm that can randomly generate and store strong passwords for all of your accounts. These programs will keep your passwords locked in one convenient location and accessible with one master password.

6. **Use two-factor authentication (2FA).** Sure, it's an extra step. But it's also an extra layer of security. To further safeguard your accounts, 2FA requires you to enter a unique multi-digit code that's texted to your smartphone upon any login attempt. Start using it on your Apple device or Google device now.

7. **Don't enter passwords on public Wi-Fi.** When you're connected to an unsecured network, like the free Wi-Fi offered in cafés and restaurants, your unencrypted data could be intercepted.

8. **See if your passwords have been compromised.** Have I Been Pwned? is a website that allows internet users to see if their account information was leaked by a data breach. Note: If it has, you should change your password immediately.

To learn more about password safety, read our blog post: 7 tips to keep your personal information protected.

Did you know? Frankenmuth Insurance offers home and personal auto policyholders complimentary access to fraud specialists if they become victims of identity fraud. To learn more, talk to one of our local, independent agents today.