7 common security mistakes you're probably making

by Matt Elliott, CNET CONTRIBUTOR

Here are seven common mistakes you might be making online. Better to correct these mistakes now then wait until after you get hacked or otherwise compromised.

1. Using weak passwords

Sure, a simple password is quick to enter and easy to remember. It's also easy to crack. Avoid using a short word for your password. And don't use the same password for multiple accounts because if one of your logins gets hacked, then hackers can access your other accounts. For tips in creating strong, hard-to-crack passwords, check out our guide to password security.

2. Not using a password manager

Using a password manager is a win-win. It makes your online life more secure and easier. A password manager stores the passwords for your various online accounts and profiles, across all your devices, and saves you from having to remember and enter each one each time you visit a password-protected site. Instead, your passwords are encrypted and held by your password manager, which you then protect with a master password.

Since you are saved from having to remember all of your passwords, you will be less tempted by the dangerously poor idea of using the same password for all of your accounts. With a password manager, you can create strong passwords for all of your accounts and keep all of them saved behind a stronger master password, leaving you to remember just one.

My colleague Rick Broida says you're crazy if you're not using a password manager and is happy to show you how to get started with LastPass.

3. Not using two-factor authentication

If you are using strong passwords and a password manager, then take the extra step of setting up two-factor authentication to add an extra layer of security to your online accounts. The most common form of two-factor authentication when logging into an account is the process of entering your password and then receiving a code via text on your phone that you then need to enter. The second layer in two-factor authentication means a hacker would need to steal your phone along with your password in order to access your account. This one I have written about -- learn how and why to use two-factor authentication.

4. Making online purchases with your credit card

Most credit cards offer fraud protection, but a mobile payment system is safer and will save you the hassle of filing a claim if your credit card does, in fact, offer fraud protection. A mobile payment system like Android Pay or Apple Pay features something called tokenization, which creates a one-time-use credit card number for each purchase instead using of your real credit card number so it can be kept hidden and secure. PayPal also offers tokenization. And Apple Pay can be used on Macs.

5. Clicking links, opening attachments from sketchy emails

If you receive an email from your bank, the IRS, PayPal, Facebook or another reputable institution that says there's a problem with your account and immediate action is needed, do not click the link included in the email. Instead, go to the site directly and log into your account to see what's up. Odds are your account is fine and that the email you received was part of a phishing scam trying to trick you into revealing sensitive information like your username and password or bank account or credit card number. Learn how to spot a phishing email.

6. Treating public Wi-Fi like it's private

Hopping on Wi-Fi at Starbucks or the airport is generally safe, but not if you're logging into your bank account to check your balance or pay a few bills. You should treat all public Wi-Fi spots as insecure and easier than your home network for someone to see what you're doing online. Also, hackers and other nefarious individuals set up Wi-Fi networks that look like a coffee-shop network or another public Wi-Fi hotspot to steal your information. Make sure you're connecting to the right network and not a spoof set up to grab your information -- steer clear of any random open networks you don't recognize. And when connected, avoid banking or logging into other sensitive accounts.

7. Not updating your OS

Apple, Google and Microsoft update their operating systems regularly with security patches. These patches fix known vulnerabilities that hackers like to exploit, the most recent example being the WannaCry ransomware attack that hit outdated Windows machines. Don't ignore those updates-are-available notifications; keep your laptop and phone up to date and make yourself a tougher target for hackers.

Source: www.cnet.com

CHICAGO TITLE®