How to Create Stronger Passwords and Protect Your Online Accounts

From email accounts to bank accounts, online shopping to online stock trading, you have many passwords to create and remember. Life would be easier if they were all the same. Or if they all came to mind quickly—like your child's name or birthday. But just as those are simple for you to remember, they're fairly simple for a scammer to figure out and use to drain your savings or steal your identity. So, how can you create the strongest passwords that aren't a pain to access when you need them? Let's explore some tactics for password protection and other ways to safeguard your digital accounts.

Build a Bulletproof Password

While there are many steps you can take to keep your funds secure from cyberfraud, a strong password is one of the first lines of defense. When creating a new password, keep these tips in mind for the best protection.

- **Length is strength.** An 8-character password was once standard, but current recommendations say to aim for at least 12 characters, ideally more. The longer your password, the tougher it is to crack. Think about how much easier it would be to guess a four-letter word than a twelve-letter phrase.
- **Mix it up.** Using letters alone won't do the trick. Combine uppercase and lowercase letters, numbers, and symbols to create a more powerful password that's trickier for hackers to decode.
- **Make it unique.** Using the same password across various accounts is like giving a thief a master key to every door in your home. Setting up unique passwords ensures that even if one account is compromised, your other accounts are safe.
- **Avoid the obvious.** Your birthday, kids' names, pet's name, anniversary, and other personal information can be simple for hackers to get from social media profiles or public records. Stay away from personal information that can be easily obtained. Avoiding sequences, like "12345" or "qwerty," is also recommended.
- **Passphrases are better than passwords.** Instead of a single, complex word, create a memorable passphrase. This could be a random string of unrelated words, like "YellowUmbrellaSkippingRocks," or a nonsensical sentence, like "PizzaAlwaysGoesWithFridays." These work best because they're long and unpredictable.
- **Use a password manager.** Remembering a unique, complicated password for every account is a challenge, so password managers can be very helpful. These are secure applications that store and encrypt all your passwords, eliminating the need to remember them all.

McCarthy & Cox
Retirement & Estate Specialists LLC

McCarthy & Cox Retirement & Estate Specialists
127 West 5th Street | Marysville, OH 43040
937.644.0351 | 937.644.0356 fax | www.mccarthyandcox.com

Add More Protection: Multifactor Authentication

Multifactor authentication (MFA) adds another verification step beyond just your password. When you enable this service on one of your accounts, you'll get a temporary code (via text, email, or an authentication app) that you need to enter to log in along with your password. This extra layer of protection will make it much harder for a hacker to break in to your account, even with a stolen password.

How can you enable MFA? Go to account settings for your bank account, investment platforms, and online payment services, find the MFA option, and follow the instructions to set it up. Many nonfinancial accounts also offer this—you can use it for email, social media, and any other service that contains sensitive information.

Don't Take the Phishing Bait

When scammers send emails or make phone calls that appear to be from legitimate sources, like your bank or credit card company, so they can solicit your login credentials, it's called phishing. Phishing messages often have a sense of urgency or pressure you to act quickly, perhaps by claiming your account is compromised—or even that a family member is in trouble and needs your financial help.

To stay safe from phishing attempts, always check the sender's address. An email that doesn't match the institution's official domain name should raise suspicion. Even if the address looks legitimate, it's safest for you to initiate contact with anyone requesting personal information via the phone number on their official website rather than hitting reply or clicking a link in an email. You can do the same with a suspicious phone call—tell the caller you'll call the bank or other institution back using their publicly listed contact information. In general, it's a safe policy not to answer calls or respond to text messages from unknown numbers, especially those claiming to be from your bank or financial institution.

More Digital Safety Steps

Update regularly.

App and device updates often include security patches that protect against threats and vulnerabilities that hackers can exploit. Enable automatic updates whenever possible so your device remains protected.

Avoid public Wi-Fi for sensitive transactions.

Public Wi-Fi networks, like those in coffee shops or airports, are convenient but can be insecure. Stick to your home password-protected Wi-Fi when accessing financial accounts or entering sensitive information.

Stay vigilant.

Regularly review your financial statements and credit reports. Early detection of suspicious activity can prevent significant losses. Set up alerts to notify you of any significant changes or activities.

Enable screen locks.

Set a strong screen lock on your phone, be it a PIN, fingerprint scan, or facial recognition. This adds a key layer of security that prevents anyone from accessing your device and the financial apps on it.

“S” is for secure.

Look for the https:// prefix at the beginning of a website’s address, especially when entering sensitive information like login credentials or financial details. The “s” indicates that the website encrypts the data you send and receive, making it more difficult for hackers to intercept.

In today’s world, your financial health is closely linked to your digital security. Cybercriminals are constantly evolving their tactics, targeting not just bank accounts but also investment portfolios, retirement savings, and even real estate transactions. Strong online security practices are no longer optional—they’re essential.

By creating safe passwords and following these digital security best practices, you’ll not only protect your data, but your financial future and your peace of mind, too.