Strategic Wealth Partners
Deerfield, IL • 224.632.1600
Milwaukee, WI • 414.359.1000

Protecting Yourself from Cybercrime

Cybercriminals are becoming more sophisticated every day, but they rely on people not being vigilant about potential threats, so you are still the best defense against cybercrimes! Thankfully, there are cybersecurity best practices that can help keep you from becoming a victim. We've compiled a list of some of these practices below:

Stop Phishers from Catching You

Phishing attacks are where someone poses as a legitimate entity to gain access to your personal information, often through email.

- If you have any doubts about the legitimacy of an email, phone call, or text, call the institution's main phone number to confirm it actually came from them. Make sure you call the institution's main number listed on their website or your account statement. Never use a phone number listed in the email.
- Never use a link found in your email to log in to financial accounts. Instead, bookmark the institution's website in your browser and always start from that login page. This ensures that you are entering your credentials in the correct location.
- Never provide your personally identifiable information or passwords over unsecured email. **Most institutions, including Strategic Wealth Partners, will never ask you to provide passwords or personal identifying information over email.**
- If you are not expecting an email requesting information; consider it suspicious. Never click on any links or attachments from suspicious emails.

Watch for Malware

Malware is intended to damage or lock down a device or gain unauthorized access to a device.

- Even if a link in an email looks legitimate, it can easily be disguised and contain malware. When in doubt, hover your mouse over the link. A pop up will appear showing the link address. Make sure the pop up shows the URL for the intended destination before clicking.
- To help prevent malware from infecting your computer, make sure you have an antivirus program installed and that it is up to date. Norton, Webroot, and F-Secure are among the plethora of options available.
- Make sure to use secure websites that begin with "HTTPS" (as opposed to "HTTP") and have a lock icon in the address bar. Websites that do not have this could contain malware.

Make a Hacker's Job Hard

- Create strong, unique passwords for each site and do not reuse passwords. Never use your name, birthday, or other easily identifiable information in your password. Passwords should be a minimum of fourteen characters and contain at least one upper and lowercase letter, number, and special character. Consider using a passphrase or another language.
- Use a password encrypted vault such as Keeper Security or SafePass to store your passwords.
- Use two-factor authentication for your email account(s) and financial institution(s). This creates an additional level of security beyond your password. For example, each time you log in to your bank, you will need to also provide a code from an app, such as Symantec VIP Access or Google Authenticator. A hacker would need both your password and your phone to access your account(s).
- If you are hacked and receive an email demanding ransom, do not engage with the hacker. Reach out to an IT professional for help (Geek Squad at Best Buy provides 24/7 support). Hackers will often deposit a new virus on your machine after receiving a ransom payment.

Date Published: 09/23/2019