6 Best Practices to Protect Your Confidential Information

Presented by CJ Ferrari and Mark Miller

Although there is a vast amount of technology available that is designed to safeguard your devices and personal information, that information is still vulnerable to cyber criminals and identity thieves. In fact, security breaches are not always due to a weakness in technology control. Sometimes, they are the result of the *action or inaction* of the user—you! Therefore, you are one of the best lines of defense against cyber crime.

As October is National Cyber Security Awareness Month, it's the perfect time to implement the following information security best practices to do your part in keeping your personal information safe and secure.

1) Build strong passwords

It's important to create strong passwords for *all* of your online accounts. But what exactly does this mean? A strong password:

- Contains both uppercase and lowercase characters, as well as digits and punctuation
- Is at least eight characters long
- Is not a word in any language, slang, dialect, or jargon
- Is not based on personal information, names of family members, and so on

A good rule of thumb is that **passwords should be hard to guess but easy to remember**.

2) Use multifactor authentication

A user ID and strong password alone are not sufficient protections for securing web accounts. Multifactor authentication—one of the simplest and most effective ways to secure your data—adds an extra layer of protection. With multifactor authentication, users must provide two forms of identification in order to log in to a site.

Here's how it works: After a user enters a user ID and password, the website will send a passcode to the user's mobile device. He or she must then enter this code on the site, ensuring that *only* that individual can sign into the account.

3) Be suspicious of unsolicited e-mail

Be wary of any e-mails that convey a sense of doom and gloom (e.g., threatening to close an account) or that claim immediate action is required. Grammar mistakes, spelling errors, and generic salutations are also red flags. Perhaps most important, scrutinize those e-mails that contain links and attachments from sources you don't know (and, unfortunately, even from sources you do know). It's quite easy for cyber criminals to craft a legitimate-looking e-mail in the hopes that you'll be fooled into thinking it came from a company you do business with or from a friend. To protect yourself from this scenario, don't hesitate to verify: Call the source directly to authenticate from whom it was sent it; if it came from a company you know, go to the company website directly to log in.

4) Protect your mobile devices

Outdated software can leave your mobile devices open to security vulnerabilities. By keeping your apps and mobile operating system software up to date, you can mitigate the risk of a cyber criminal exploiting a hole in your system. Most devices simplify this process for you by offering automatic update options for apps, as well as notification systems that let you know as soon as an operating system update is available. It's your job to take care of these updates immediately!

Another mobile device necessity is to do your homework, making sure the apps you're downloading are from a reputable company (e.g., by checking their ratings and comments). Be sure you know what the app does and what information it's going to access on your mobile device.

5) Engage in safe web browsing

Keeping your browser up to date is critical in preventing malware. Just like apps and your operating system, an out-of-date browser can open up security gaps that cyber criminals will take advantage of. Be alert to pop-ups and advertisements: Both could be spyware used to plant tracking cookies on your machine, which can steal your information, direct you to bogus phishing sites, and pummel you with pop-ups.

When transmitting personally identifiable or payment information, you can ensure that you are on a secure site by checking for the "https://" before the "www.whateversite.com." When on public Wi-Fi networks, consider connecting through a personal virtual private network (VPN) and disable auto-connect; this way, your device won't automatically connect to found public networks.

6) Stay vigilant

Although advanced technology today is certainly a safeguard and buffer to keep cyber criminals at bay, it's critical to remember that *you* are in the first line of defense to keeping your data safe and secure.

For more tips and tricks to stay safe online, visit the National Cyber Security Alliance at ***www.staysafeonline.org***.

###

CJ Ferrari and Mark Miller are financial advisors located at Miller Ferrari Wealth Management, 400 SW Bluff Dr., Suite 107, Bend, OR 97702. They offer securities and advisory services as Investment Adviser Representatives of Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. They can be reached at 541-639-8055 or at cj@millerferrari.com or mark@millerferrari.com.