Don't be caught off guard......

Protect Your Money

Be Cautious Using Public Wi-Fi........

Free public Wi-Fi is great, but always be aware of what you do online over free Wi-Fi. Catching up on the news or checking sports scores is fine, but it's a good idea to avoid accessing any personal information — including online banking. That's because hackers have developed new and nefarious ways to steal your information over free Wi-Fi, including using a device known as a "Wi-Fi pineapple."

A Wi-Fi pineapple is a small, battery-powered device that a hacker can conceal in a backpack or bag. With it, the hacker can essentially insert him or herself between you and the real public Wi-Fi, fooling your computer or smartphone into thinking it's connecting to free Wi-Fi when, in fact, it's really connecting to the Wi-Fi pineapple.

Then, when you enter your login information, the hacker receives it all before it's relayed on to the real website. From that point on, your account is compromised, without you suspecting a thing.

Hover Before You Click.........

If you have an email address, odds are at some point you've received an email from some well-known business — or rather what appears to be some well-known business —asking you to confirm your identity or personal information.

Often these fraudulent emails, referred to as phishing attempts, come from companies you may never have done business with, thereby making the fraud attempt easy to spot. But every once in a while, the fraudsters may get lucky and trick you into clicking on the wrong link before you catch on.

The easiest way to avoid falling victim to one of these phishing scams is to hover before you click. In other words, before clicking on any link in an email you're not quite sure about, hold your cursor over the link for a moment. When you hover over the link, a pop-up will appear that will show you the true destination of the link.

So if, for example, you receive an email purportedly from PayPal asking you to update your information, and you just happen to have a PayPal account, before you click on anything, hover over the link and see whether it's actually directing you to PayPal. If it's not, or if anything else about the email seems unusual, it's best just to delete it without clicking on anything.

If you suspect the request may have been legitimate, simply contact the company directly via its website or over the phone. That way you can be sure you're dealing with the real company.

swan VALLEY
CREDIT UNION

"Building a better future with you"