YOUR MONEY *Matters*

Anne Blain, CEO
Chiropractic Federal
Credit Union

Best practices for computer security

Computer hacking has become a profession for some people. These individual are able to use cookies, not the sweet snack, but the sequences of letters and numbers your computer stores. As an example, "**Remember me**" box on a login page? By checking that box, you are asking your computer to keep track of cookies.

When I read this I thought to myself, I know how busy our members are and how nice it is to take a convenient path to accessing secured websites. But that is what the hackers love and through reverse engineering, they can re-create cookies to trick websites and email accounts into automatically logging them in. If that happens there becomes a risk of identity fraud and any personal details available in their accounts are at the mercy of someone with malicious intent.

Beyond consumers' personal information, forged cookies could lead hackers to something equally vulnerable – payment card information. Some websites remember credit and debit card information for repeat customers. While this offers time-savings convenience at checkout, it also presents an increased risk of card fraud should an account become compromised.

Incidents of forged cookies have already occurred on a large scale. I am sure everyone is aware of Yahoo's big email breach. It affected more than 32 million people. This breach demonstrates just how valuable robust security measures are and we are all vulnerable if security **best practices** are not followed.

Mitigating our vulnerability to forged cookies is importing and following these practices below may be in your best interests.

1. Frequently change passwords.
2. Never share PIN's or passwords.
3. Ignore the "Remember me" box.
4. Regularly review financial account information and activity.
5. Browse responsibly. Always open a new web browser when using financial and other sensitive sites. General web surfing activities should be kept separate.

We know that knowledge is power when it comes to preventing fraud and identity theft. Below is a list of common scams to be on the lookout for:

Keylogger: A program that logs sequential strokes on a computer keyboard and sends them to hackers so they can figure out a person's log-in credentials.

Malvertising: Malicious online advertising that contains malware — software intended to damage or disable computers.

Man-in-the-Middle Attack: When a fraudster secretly intercepts and possibly alters messages between two parties who believe they are securely communicating with each other.

Ransomware: A malicious program that restricts or disables a person's computer, hijacks and encrypts files, and then demands a fee to restore the computer's functionality.

Scareware: A program that displays on-screen warnings of nonexistent infections on a person's computer or Smartphone to trick a person into installing malware or buying fake antivirus protection.

Skimming: The capture of information from the magnetic stripe on credit and debit cards by "skimmer" devices that are secretly installed on card-reading systems at gas pumps, ATMs and store checkout counters.

Smishing: Phishing attempts that go to a person's mobile devices via text message, telling them to call a toll-free number. This is named for SMS (short message service) technology.

Spoofing: This involves any situation in which a scammer masquerades as a specific person, business or agency. This typically means the manipulation of a person's telephone's caller ID to display a false name or number.

Vishing: Short for "voice phishing," the use of recorded phone messages intended to trick a person into revealing sensitive information for identity theft.

I think with good internet habits, it will enhance your overall peace of mind of knowing you have done everything within your power to stay "computer" safe.

Anne Blain, CEO of Chiropractic Federal Credit Union
If you have a financial question, please forward to:
ablain@chirofcu.org or contact us at 248.478.4020
Subject: "Your Money Matters"