BROKEN ARROW
CHAMBER of COMMERCE

Protect Yourself in a Crazy Online World

By: Josh O'Mealey, Director of Information Security, TTCU Federal Credit Union

With global tensions and cyber-attacks in the news, this is a great time to check your technology practices to ensure you're protected online. Security experts suggest these simple steps to help keep you safe online.

Updates - Keeping your digital devices up to date

Your computer and mobile device* are essential parts of your digital world. Applying Microsoft, Apple, and Android updates when they become available is one of the top ways to protect your digital devices. The same advice applies to your web browsers. It's equally as important to apply updates for Chrome, Safari, Edge and other web browsers as soon as they become available.

Passwords - Please don't re-use them

You don't want to lose access to your accounts – this is priority number one. Most security experts say this is most likely to happen when you re-use passwords. Then, when one password is stolen, hackers can use it to access your other accounts. Coming up with unique, complex passwords to each website can be challenging to manage. Using a password manager can help you create strong passwords for each website and safely store them.

Multi-Factor Authentication - It's worth it

Multi-factor authentication or MFA seems like a pain to some people, but it's one of the best ways to protect your most important online accounts from unauthorized access. Major online services usually provide this functionality for free. In addition to providing a password, MFA uses a second source to verify it's really you logging in. This additional authentication usually comes from an app on your smartphone or by receiving a text message or phone call with a unique code.

Incoming Communication - Scams are always coming

Everyone is at risk for scams you receive via email, voicemails or text messages. Be on guard for any of the following red flags and delete any messages that show one or more of these signs.

- Messages from someone you don't know
- Unexpected or unusual content
- Messages with many misspellings or grammatical errors
- Messages asking you to click on a strange hyperlink
- Someone pressuring you to act quickly or threatening blackmail if you don't pay

If you've received strange emails from someone you know, be suspicious. Their account may have been compromised, and attackers know you're more trusting of a close friend or family member. Use another method to contact them and find out if the suspicious message really came from them.

Public Information - Be careful with your social media posts

If you've set your social media accounts to be viewable by everyone, don't post personal information that attackers could use to impersonate you and gain access to your accounts. An attacker could also use your list of followers on social media to impersonate someone you know to get you to click on a malicious link.

Visit TTCU's website for more information on ID Theft and Fraud.

Josh O'Mealey
Director of Information Security, TTCU Federal Credit Union

Josh O'Mealey is the Director of Information Security at TTCU Federal Credit Union. He has been in the information security industry since 2003 and holds active certifications in the field.