April 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people

Getting Personal With Security

- **Top Tips for Personal Security**
- **5 Security Tools Everyone Should Use**
- **Common Scams to Watch Out For**

Top Tips for Personal Security

Let's shift our focus from how you can help our organization remain secure to how we can help you stay secure. Here are a few tips to avoid data theft, financial loss, or malware infections:

Stay alert for phishing attacks

Phishing is one of the most common attacks you'll encounter both at work and at home. Stay on the lookout for common warning signs like bad grammar, misspellings, threatening language, and a sense of urgency. Don't click on any links or download attachments that came to you randomly.

Think like a scammer

Before sending someone money or revealing personal information, think through the situation from a scammer's perspective. Does it seem like a good way to defraud someone? Does anything seem out of the ordinary? Trust your instincts and avoid assuming someone is who they claim to be.

Stay safe on social media

Unless you're trying to build a personal brand, it's best to set your social media accounts to private and always vet anyone who wants to connect with you. Cyber criminals search public profiles for any information that might be useful to carry out scams.

Protect your mobile devices

From messaging to banking to social media, our smartphones open a lot of digital doors. If available, enable remote services that allow you to locate a missing device or erase all data when the phone can't be recovered. Only download applications from trusted sources, and keep an eye on the permissions any software asks for.

Replace your passwords with passphrases

We need our passwords to be easy to remember, yet hard to crack. Passphrases accomplish this by forming a sentence (at least 16 characters long) that is meaningful to you and only you. Obscure song lyrics or book quotes, for example, make for great passphrases.

Common Scams to Watch Out For

Cyber criminals are opportunistic. They'll gladly target individuals just like they do large organizations. Let's explore a few common scams that anyone might encounter.

The fake rental property

Imagine paying a deposit on a new rental home, only to find out later that someone already lives there. Rental scams usually involve a fraudulent listing of a real property. The scammers sometimes figure out how to copy keys (or break into the home to unlock it) so the victim gets an opportunity to view the home in person.

The caller who demands payment by gift cards

The caller might claim to be from a power utility company or a financial collection agency and threaten you with fees or account closures. Instead of a traditional payment, they ask you to purchase gift cards and provide the relevant information on the cards.

The extortionist

Fear is the most powerful ingredient in extortion scams. They typically involve an email with a threatening subject line like "I saw what you did." The messenger claims they used remote desktop software to record your screen and your webcam. They then threaten to send the video to all of your contacts unless you immediately pay the scammer.

The one where your account has been suspended

This common phishing scam comes via an email that features logos and contact information from a real business. The message states that your account has been suspended due to fraudulent activity and that you must update your login credentials, or the account will be closed permanently.

In all cases, you can easily avoid becoming a victim by:

- *Using situational awareness and common sense*
- *Verifying someone's legitimacy before sending payment*
- *Slowing down if a situation is emotionally triggering or unrealistic*
- *Thinking before clicking or downloading anything*