DON'T BE A VICTIM: STAY VIGILANT FOR EVOLVING FRAUD SCHEMES

Fraudsters have become increasingly creative in finding ways to exploit vulnerabilities and unlawfully access personal and/or business information and assets. These cons have evolved over the years with dramatic spikes during times of economic and political global duress. Fraudsters have exploited the pandemic by offering COVID-19 services in exchange for personal details, including Medicare information. We've also seen a rise in tax-related schemes during year-end tax filing season. It's critical to stay aware of these evolving trends to protect both yourself and your company. Below are some examples to stay wary of.

IT Security
Scammers impersonate online tech support and feign security issues in order to request direct access and compromise your machine. These attacks are often initiated through calls, texts, emails or pop-up windows.
IRS
Impersonators seek payment for non-existent tax bills and even threaten arrest, deportation or federal tax liens. A rise in IRS impersonations has been implemented through phone calls and text messages.
Unemployment
A surge of fraudulent unemployment claims has been filed using stolen identities

in order to collect benefits. The IRS reminds all individuals to watch for unemployment claims or other benefits reported on their 1099-G, to which they never applied.

Popular Companies

Scammers leverage famous company names and fake email accounts alerting you to problems within your account to acquire personal information.

Mortgage Closing

Criminals take advantage of the vast number of transactions taking place during mortgage closings. They may impersonate a mortgage professional with false instructions on where to deposit funds.

Online Dating

Romance scammers seek to build online relationships with individuals through social media and online dating sites to later exploit the unknowing victims through fake investment opportunities, emergency requests for money, phony charity requests and even requesting compromising pictures which can later be used as extortion tactics.

Social Media

Fraudsters like to use social media profiles to "scrape" information from your profile, such as birthdate, email address, contact information, family and friends in an attempt to figure out your passwords, answers to security questions, or gather other insight to tailor their scams to you.

A host of other well-known cyber-attacks such as ransomware and malware are designed to encrypt data or deny access to the organization until a ransom is paid. These attacks are often initiated through successful phishing or spear-phishing attacks by clicking invalid email links.

Key Tips & Reminders

- **Consider** – Take the extra second before clicking on links or opening attachments in unsolicited, suspicious or unexpected emails or text messages.
- **Secure** - Adjust your privacy settings and be selective with what you share online. Don't connect with people you don't know.

- **Verify** - Do not give out any financial information via the phone unless you have appropriately validated that you know you who are speaking with.
- **Report** - Tech support companies will not contact you via pop-up messages or problems with your machine. If you suspect an issue with your machine, contact your trusted IT department directly and immediately.
- **Know** - The IRS generally makes first contact through regular mail (not by phone or text message) and will never request personal or financial information through e-mail or text messaging.

Identity theft, phone scams and tax frauds are just a few ways that individuals can be compromised. In response, the IRS issues an annual list of the top twelve tax-related schemes, known as the "Dirty Dozen," that taxpayers may encounter, many of which peak during filing season. Always stay vigilant so that you don't fall victim to these scams!