K-State Research and Extension News for July, 2021
Submitted by Kathy Goul, Family & Consumer Science Agent

Liars, Cheats & Crooks are Alive and Well

Despite the best efforts of consumer protection agencies, law enforcement, businesses and government, scammers continue to rake in millions of dollars each year from unsuspecting consumers. In my role as an extension agent, I receive frequent phone calls about potential scams – especially those involving Medicare and Social Security. However, contrary to popular opinion, seniors are not the only potential target for these crooks. Individuals of *ALL* ages fall victim to scammers each day.

While technology has opened up new opportunities for scammers, in reality many of the same old tricks are used. Scams are always evolving, but you can spot, and avoid a scam, if you know what to look for.

Phising is one of the oldest and most widely used methods by scammers to get you to reveal information that can be used to steal your identity and money. Delivered by email, phone, text messages and social media, these scams tempt you by pretending to be from a legitimate business, government agency or trusted entity that could believably have a need for your sensitive personal information to deliver a package, verify a transaction, fulfill and order, issue a refund, keep your account open, etc.

Scams are as varied as their perpetrator's imagination, but they all have certain things in common. An unexpected contact, a request for money or personal information, a sense of urgency, a threat or enticing offer, and pressure to use an unrecoverable payment method are some of the tip-offs of a scam.

To avoid becoming a victim, remember that financial institutions such as your bank, credit card companies and other financial institutions will never ask you to disclose your password. Federal agencies will rarely call you to ask you to confirm personal information by phone. If they do, it is typically only regarding a matter you're already aware of. Hanging up the phone, or deleting the email without responding (or clicking the link provided) is your best way to avoid falling victim.

Do not respond directly to an email, text message or telephone call from a bank, business or agency, or trust the contact information provided in the message or call. Contact customer service using a verified phone number, email address or website to determine that the request for your information is legitimate.

Pay attention to detail. Most phising attempts reveal themselves through spelling and grammatical errors, unusual wording and an unprofessional presentation – things that you would not expect from a business or government agency. Do not trust caller ID. Technology has made

it easy for scammers to block caller ID or to display a name or number that you are likely to recognize and trust. Check the website address. Many times, website addresses provided are altered in a subtle way.

Scammers and crooks can be found around every corner, waiting for their next victim. Be sure to keep your guard up and maintain a healthy level of skepticism. If it sounds too good to be true, it usually is. Do not be rushed into making a decision. Take time to do the research needed prior to responding. If something is legitimate, you will be given the opportunity to check things out.

If you feel that you have been the victim of a scam - report it! Where to report it depends on the type of scam. In all cases, you should notify the Federal Trade Commission (https://www.ftccomplaintassistant.gov). The FTC collects information about current scams and fraud and directs it to law enforcement officials. There are a variety of other agencies you should also contact, depending on the nature of the scam. For more information on scams, how you can protect yourself and where to report fraud, visit www.consumer-action.org.

Source: Consumer Action