Daily Union – Saturday, April 4, 2015
Vol. 3 Issue 14: Consumer Scams

As consumers, we would like to believe that we are fairly smart when it comes to protecting our own interests. The problem is, people who set up scams or commit fraud are smart, too. They know human behavior and use that knowledge in attempt to stay one step ahead of their victims. They seem to adjust and tweak their approaches just enough to make sure we sometimes lose our balance and fall into their schemes.

Being aware of some of the trending scams and fraudulent efforts of these criminals can help us maintain our balance and avoid their traps.

Merriam Webster defines fraud as "the crime of using dishonest methods to take something valuable from another person." Related to fraud, scam is defined by the same source as "a dishonest way to make money by deceiving people." Fraud is illegal, while a scam may or may not be.

There are many areas targeted by frauds and scams. Here are a few general avenues used:

1) E-Mail Scams – These scams flood our inboxes and crowd our communication channels with junk. The distributors of these massive scams collect, steal, or illegally purchase email address data bases. Sometimes they create email addresses and documents that look like a legitimate company or source so we often click "open" before we realize our error. In general, if it sounds too good to be true – it is! Look for misspelled words or poor grammar to help you determine as a "red flag." Sometimes the extension on the "from" address will help you identify scams, as well.

2) Fake Check Scams – One common example of this scam is with the ploy of winning a lottery. Often communicated through an e-mail, the sender will say you've won an overseas lottery. They ask you to claim your winnings my giving them enough information that they can mail you the winnings check, but you'll need to pay for the taxes and handling fees in that country. By the time you get the fake check in hand, you have wired money to them to pay for the taxes and handling fees. When your bank catches that you have cashed a fraudulent check, the wired money is long gone and you can't retrieve it. If you have to send money to get money, it is likely a scam. Put the initial email in your junk mail folder and mark the sender's address as junk, too. This will help filter out any future communication from the same address.

3) Mail Fraud – A classic mail fraud that continues to make its rounds is that of the fake Publisher's Clearing House (PCH) award letter. It will claim that you have won some

outlandish amount of money through this long standing award program. It is such a common act of fraud that PCH themselves have added a consumer awareness video and link to their blog. Their message is straight forward: "You never have to pay to claim a legitimate publishers clearing house prize!" There are other forms of mail fraud, as well. They, like the one mentioned above, work by enticing you to send money to claim your winnings. Don't do it! It's not a legitimate claim.

4) Phishing – This is another scam associated with our use of email. Phishing (pronounced just like *fishing*) is what it sounds like. The sender of an e-mail message is trying to get you to get "hooked" on their claim so that they can "net" your personal information. Your information is then going to be used for illegal purposes and financial gain for the sender who collected it. If possible, don't open emails from people you don't know. If you feel you need to open unfamiliar email, certainly do not open any attachments or answer any personal questions. In this age of online banking, electronic financial management, and making online application for services, determining which emails are "bad" is a challenge. You don't have to respond to them.
4) Smishing and Vishing – Smishing is a combination of SMS texting and phishing. The sender is using your mobile phone and phishing techniques to obtain your personal information. Vishing is a combination of voice and phishing where a person actually calls you (on your mobile phone OR your land line) for the same purpose – to get information from you. Criminals will set up an automated dialing system to text or call unsuspecting consumers. They often claim that there is a problem with your "account." If you are not familiar with the person or company who contacted you, don't answer their questions. If you want to check on their claim, contact your credit card company the caller claimed to represent. When YOU initiate the communication, you can feel more confident that the information you are getting is accurate.

6) Telephone Scams – Con artists use the phone to get money from people the same as charities or other solicitors raise money. If you are unsure if the call is legitimate, don't send any money. You can contact that charity directly to support their efforts to raise funds.

According to a Truecaller/Harris survey report, Americans lose $8.6 billion annually through telephone scams (at an average of $488.80 per victim.)

Protect yourself from scams and frauds. If it's too good to be true, it most likely isn't true in the first place. Take some time to do some researching on your own at: http://www.usa.gov/topics/consumer/scams-fraud/types
and http://www.ic3.gov/crimeschemes.aspx (Internet Crime Complaint Center)

You can also call me at the Geary County K-State Research and Extension office to find out more about other consumer concerns: 785-238-4161. Until next time, keep living resourcefully!