The Daily Union

Saturday, April 8

Title: Be Smart About Phone Scams

One of our friends who owns his own business, recently received a phone call from Microsoft. The customer service representative explained that Microsoft was correcting a problem in their software that could lock up the hard drive on computers that came preloaded with software. They went on to ask for the business owner's login and password so that they could fix the problem remotely. He was eager to make a change that would prevent his hard drive from "crashing" and save his valuable customer and billing information data that he had accumulated over years. Thus, he shared the information. After a few moments and with a few additional technical comments of how they were making the repair, the customer service representative hung up.

Within minutes of hanging up the phone, our friend shared that he was unable to access anything on his computer and just got a blue screen on his monitor. Perhaps you smelled a rat from the beginning of this article, but in case you didn't I recommend you read on.

Today's article is about the many different ways consumers can be deceived and become victims of fraud. In the story above, what was the first clue that the phone call was a scam? First, Microsoft will NEVER reach out to you with unsolicited PC or technical support. Any communication made with Microsoft must be initiated by the consumer. In fact, their website addresses this very issue head-on and explains that cybercriminals are very clever in how they try to convince their victims that they are legitimate. When they are able to make believers out of their victims and get the information they need to gain access to your computer, they are able to do any of the following:

- ✓ Trick you into installing malicious software that tracks how you use your computer, preview what websites you commonly go to, and acquire login information to your online banking system. They can retrieve data off your hard drive – such as the customer records kept in our friend's computer.
- ✓ Convince you to visit legitimate websites to download software. Once you have downloaded the software they can take control of your computer remotely and adjust the settings to leave your computer vulnerable. This is exactly what happened to our friend.
- ✓ Request credit card information so they can bill you for phony services.
- ✓ Direct you to a specific website and ask that you enter your credit card and other personal/financial information there. In this case, you're entering onto a

fraudulent website with the sole purpose of collecting data from unknowing victims. This date is then used to steal money and information from the consumer.

How do you avoid becoming a victim of phone scams? Here are a few suggestions offered by the U.S. Federal Trade Commission (FTC):

- Ask yourself "who's calling and why?" The law says telemarketers must tell you it's a sales call, the name of the seller and what they're selling before they make their pitch. If you don't hear this information, say "no thanks," and get off the phone.
- Why are they in such a hurry? Fast talkers who use high pressure tactics could be hiding something. Take your time. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.
- Does it make sense that you have to pay for a supposedly free service? Question fees you need to pay to redeem a prize or gift. Free is free. If you have to pay, it's a purchase — not a prize or a gift.
- Why am I "confirming" my account information — or giving it out? Some callers have your billing information before they call you. They're trying to get you to say "okay" so they can claim you approved a charge.
- What time is it? The law allows telemarketers to call only between 8 am and 9 pm. A seller calling earlier or later is ignoring the law.
- Do I want more calls like this one? If you don't want a business to call you again, say so and register your phone number on the National Do Not Call Registry (https://donotcall.gov/). If they call back, they're breaking the law.

Don't be embarrassed if you have been caught up in a phone scam. Cybercriminals work hard to make themselves believable and use a wide variety of ploys to hook their victims with. When you find yourself the victim of any type of consumer scam, the FTC wants to know about it so that they can take action the criminals from taking advantage of other consumers. To file a report with the Federal Trade Commission call 1-877-FTC-HELP or visit ftc.gov/complaint.

For more information on consumer protection, you can contact me at the Geary County Extension office at 785-238-4161. Until next time, keep living resourcefully!