

CLASSIFIED AD SCAM SNARES WOMAN

In my last column, I wrote about several examples of scams which don't work through some of the methods we worry about the most, like computers or phones. I reported on good old-fashioned scams that rely on the printed word and the US Mail.

To build on that theme, I want to report to you today, on a scam which relied on a very low-tech feature, the newspaper classified ad. A woman from the Welton area, let's call her Lettie, told me about losing \$3000 in a scam.

Here's the story. Lettie for a long time wanted a used Toyota Tacoma pickup truck. From personal experience, I know they can be hard to find, and so did Lettie. So when she saw one advertised in the classifieds in the Quad City Times, this looked like something she needed to check out. She called the number listed in the ad, and received a text message reply to contact the seller through email. She did, and received a long message from "Brandon Shinkle", which described the truck in glowing terms, offered for \$3000, including shipping from Utah to Iowa. Shinkle claimed the truck belonged to the estate of his recently deceased father, and Shinkle further described himself as serving in the US Air Force, stationed in Utah. At first, Shinkle agreed to take a check, but then changed his mind, and wrote to Lettie, about using Google Wallet.

Shinkle described Google Wallet as an escrow service maintained by Google. Shinkle reported if Lettie sent Google Wallet \$3000, they would hold the money until she received and inspected the truck. If she liked it, she notified Google Wallet, who planned to release the money to Shinkle. Lettie agreed, and received emails from Google Wallet which told her to purchase \$3000 in reloadable prepaid One Vanilla debit cards, and provide Wallet with the serial numbers of the cards. Lettie called the number the Google Wallet emails provided, and talked to a foreign-sounding woman, to whom she recited the serial numbers. After this, Shinkle assured Lettie the Toyota pickup truck was on the way...Well, it never arrived.

After several days, Lettie did some research and found a phone number for the real Google Wallet, who told her this was all a scam. Google Wallet, which is a legitimate financial option for paying some bills, does not run an escrow service. In fact, if you type "Google Wallet scam" in an internet search engine, you will learn in seconds how crooks use this service to defraud victims.

Lettie is the first to admit she missed some red flags on this transaction, which should have warned her away, here are a few:

- Seller refuses to communicate by voice, but insists on using text messages or email. Fake email accounts are ridiculously easy to set up. Phone numbers sending text messages can be easily disguised.
- Seller seeks to inject some emotional or sympathy-generating tone in the sale. In this case, the truck belonged to the seller's just dead father, and the seller was active duty military. Both are pretty common features of scam stories.
- Seller offers a desirable items or commodity for a low price. In this case, the seller offered a 2003 Toyota Tacoma truck in excellent condition for \$3000. Actual value according to Kelley Blue Book was \$8000. This is easily checked online
- Seller wants to use a payment service unfamiliar to the buyer. In this case, the seller fabricated the Google Wallet escrow service, and easily faked emails appearing to show them as involved in assuring the integrity of the transaction. It's pretty risky to get involved with a payment scheme you've never heard of before.
- Seller wants payment using reloadable debit cards. This is a huge red flag. The potential for fraud is huge, and there is no way for a consumer to dispute or get the card issuer to charge-back on these transactions, as you can with regular credit cards.

This is not the first time I've looked into scams from classified ads. From previous cases, I learned many of these ads come to newspapers through online marketing, so it is not a case of someone walking into the newspaper office wanting to place an ad. I was unable to get a comment from the Quad City Times on their screening process, but the folks at the Clinton Herald tell me they do review submitted ads, and reject quite a few they recognize as fake. But at the end of the day, we need to do our own homework on any deal that calls for us to hand over money to a stranger.

ANOTHER FACEBOOK HACKING

How do you know if someone hacked your Facebook page? It's likely you won't know about it until your Facebook friends contact you and ask why you are sending out info on collecting grants, or asking for money. Or wondering why you are sending out "friend requests" to people on your friend list for a long time. These are indicators someone hacked into your Facebook account.

I wrote in my last column about this fraud, and I keep hearing more about them. Most recently, a Clinton woman, Joan, reported one such hacking this week. Joan received a message from her cousin through Facebook. Her cousin told her, the United Nations, in an effort to eradicate global poverty, made grants of \$150,000 to worthy people. And the cousin got such a grant. And saw a list of other grant recipients with Joan's name appearing on it. Joan was urged to contact someone and get her \$150,000. Joan did, and got messages telling her to go to Walmart and send \$150 through Moneygram to someone in Loxley, Alabama, to claim the

money. Joan went to Walmart, and, fortunately for her, found the Moneygram form a little difficult to understand. So she called her cousin for instructions, and learned this was all a scam, committed through a Facebook hacking.

NEW TELEMARKETING RULES

As of June 13, 2016, telemarketers must follow new rules on taking payments. The federal government now prohibits telemarketers from accepting payment using these methods:

- Wire transfers, such as Western Union or Moneygram. I've written many times about avoiding these services, so this is not new to me.
- Reloadable prepaid cards – these are debit cards which consumers can purchase and load money on to at many retail outlets. They can be used like credit cards, but they lack the same protections as credit cards. It is a lot like using cash with these cards. Examples are One Vanilla, iTunes, Amazon.
- Remotely created check – This is pretty much an authorized withdrawal from your checking account, to another bank account.
- Remotely created payment order – you can also call this an electronic check, or eCheck, much like the remotely created checks

So legal telemarketers can no longer accept payment by these methods. The thing to remember is, if a telemarketer presses for a consumer to pay by one of these methods, it is a scam. ALWAYS.

CONTACT SENIORS VS. CRIME

Let me know about scams, fraud, or other crookedness you run across. Most of what I learn, I learn from you. Contact me at Seniors vs. Crime, Clinton County Sheriff's Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us.