

FREE MONEY AND GOOGLE PLAY CARDS

One of the more common free money offers is back in circulation, targeting folks who want to believe it's time for them to get a lucky break. Instead this "reward" will only turn out to enrich some scammer. Becky Nestrusz of Camanche tells the story better than I can, and is willing to share it, in hopes of preventing someone else from getting clipped as she did.

Becky told me, she received a call from professional sounding man, who spoke with a European accent. He told her he worked for Capital One, the banking and credit card company. Capital One, he told Becky, knew she was a good person, and deserved a break, so wanted to give her a \$5000 grant, no strings attached. Becky got not have been happier. "I wanted it to be true so bad" she said, she believed everything the caller told her. He said he wanted to wire the money to her, but the state of Iowa required a "refundable bond" get posted. How much? Just \$200. The caller gave Becky instructions to go to a retail outlet and buy a Google Play card, and load \$200 on it, then reveal the card's PIN code to him. Becky did it.

And did she get her \$5000 grant then? No. What followed was a series of demands for more purchases of Google Play cards, to satisfy more and more "bonds", "fees", or insurance. In the next two days, Becky bought loaded \$1500 on seven Google Play cards she bought at grocery stores and convenience stores. She revealed the codes on all of them, relying on the caller's promise Capital One planned to refund the money to her as part of the award. After \$1500, and even more demands for more money, Becky had enough. She realized what happened and stopped taking the calls from "Capital One."

What happened to Becky did not surprise me. For the last three weeks, quite a number of people called me and told me they received similar calls. The callers said they represented some vaguely described "government" or a bank, and wanted to award a grant of \$5000, or \$9000, to "good citizens who pay their taxes and credit card bills on time." But the grant always comes with a catch. The lucky recipient needs to buy a Google Play card and load money on it.

Just remember one thing from this story. If you find yourself talking to anyone who wants you to buy a Google Play card, for any reason, it is a scam. ALWAYS.

Those cards are offered as a means for internet gamers to fund their hobby. That's all. They don't pay for merchandise, insurance, or anything else.

FACEBOOK HACKING

I get a fair number of calls from people who tell me someone hacked their Facebook account, took it over, and used it to try and scam their Facebook friends. What they mean by "hacking's is, someone accessed their account and changed the password, locking the real user out, and allowing the crook to re-configure the account, and send out phony messages. Those messages usually ask for money, or direct the "friends" to some website or phone number promoting a scam.

In the latest incident reported to me, a Fulton woman used Facebook to correspond with a party who offered a rare breed of dog for sale. The Fulton woman ended up sending \$500 away to someone through Walmart 2 Walmart, a money wire system, and...got nothing. Except after losing this money, the culprit locked her out of her own Facebook account, and used it to promote more sales of non-existent dogs.

How can you keep from getting hacked? Your first line of defense is a strong password. But perhaps just as important is taking advantage of a Facebook security control called two-factor authentication. If you use two-factor authentication, Facebook will alert you by text or another messaging system, if someone tries to access your account from a device Facebook does not recognize. Facebook knows what computer or smartphone you normally use to conduct your Facebook business. When it sees an access attempt from something different, it won't allow the access unless you approve by responding to their message.

To enable two-factor authentication, go to the Facebook setting for security, or just click the help icon on your home page. You are not only protecting yourself with two-factor authentication, but all your Facebook friends as well. Their risk of getting messages from your hacked account will be minimal.

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.

End of column/rmeier