

CREDIT CARD FRAUD AND CARD SKIMMERS

There's been some local publicity recently on credit card skimmers hidden in gas pumps, and their potential to compromise credit or debit cards. According to one caller I spoke to, she knew of 35 people who believed their cards were compromised at gas pumps. As with a great deal of credit card fraud, this is something quite difficult for folks at the consumer level to thwart. When we use a credit or debit card, we must rely on the security of the whole system to safeguard our information. That system is only as strong as the weakest link. Card information stored with retailers is subject to computer hacking. And we know skimmers at the point of sale also represent a vulnerability which can be well near impossible for the consumer to detect. Gas pump skimmers found in this area in recent months were found hidden inside the wiring of the pumps, invisible from the outside. They silently recorded the information from card transactions at these pumps, until the criminal returned to retrieve the information remotely through wireless technology, or by removing the skimming device itself.

Are we completely helpless in this deal? Not quite. Recognizing that the system is only as strong as the weakest link, we need to make sure that the weakest link is not ourselves. A woman reported to me this week, her mother received a phone call from someone claiming to work for DISH, threatening a disconnect unless she "upgraded" her service. The "upgrade" required a credit card payment, so she gave her card number to the caller. Since the caller was a scammer, that card is now compromised. Never give out personal information, to include credit card numbers, to a stranger who called you on the phone.

And there is something else to consider, tightening up the security of our cards. Particularly with debit cards, the bank or credit union issuing the card can set up parameters for their use. You can personalize these parameters. For instance, many debit cards allow only \$200 per day paid with the card. You can lower this limit to reflect your own habits. You can also impose geographic limitations on their use. These limitations might only allow use in your state or nearby states. Many card issuers already impose their own geographic limitations, preventing the use of cards in some transactions in certain states, due to the high incidence of fraud in these states. You should know this ahead of time if you plan on traveling.

Some financial institutions and card providers offer an app for smart phones which enables immediate text or email alerts when a card is used. You should contact your bank, credit union, or card provider if you want to research these options further.

FOLLOW UP FILE

In my last column, I wrote about timeshares. I did some further reading on topic, finding *Consumer Reports* explored timeshares in a March 2016 article. I learned the timeshare

industry likes to be called, “vacation ownership”, or “interval travel”. One other thing I picked up which I wanted to pass on concerns how to get out of one of these arrangements. But first, realize timeshares are no more of an investment than buying a new car is. Both depreciate – fast. *Consumer Reports* writes that only 25% of the cost of a new timeshare bought from a developer actually pays for the building. The rest pays for the developer’s overhead and profit. You’re buying a good time, a vacation experience, not an investment.

Consumer Reports named one company which specializes in marketing “used” timeshares, Timeshare Exit Team. The firm claims a 99% success rate, but its average fee is \$3900. I looked them up and found they earned an A+ rating from the Better Business Bureau. But from reading between the lines on their website, I believe they will charge at least some of the fee upfront.

In early November 2016, I wrote about the steep decline in complaints I received on the IRS phone scam. That trend continues. For most of last year, I received two or three dozen complaints, or more, each month on that scam. In December 2016, I received one. The Federal Trade Commission released a statement last week, noting a 95% drop on this type of complaint. Included in that release was a link to a *New York Times* story written about some Indians who worked this scam. They described working in a seven-story building outside Mumbai, India, with 700 others, all making these kind of calls all day long. Those working there made about \$230 a month, well above the average for call center workers.

Indian police raided the place, shutting it down, but the young men interviewed by the reporter predicted it will return. It was so profitable. The scammers also commented the scam was extremely effective with recent immigrants to the US.

FACEBOOK ADS

A 72-year old Clinton woman, let’s call her Jill, visited with me this week to tell me how she lost \$51 in a scam and was forced to cancel her credit card. It all started with Facebook. She saw a post on her Facebook feed promoting a weight-loss supplement. The ad told her she could get a free sample, paying only for shipping and handling, for which she needed to supply a card number. Jill did this, and received the samples. And then she received full bottles of this supplement, which she did not order. It seems buried in the fine print on page two of the terms and conditions of the agreement, was provision allowing the marketer to charge her card \$93 a month indefinitely, and send her monthly shipments. Jill complained to the marketer, who agreed to halve the price. Jill needed to cancel her card to get this stopped.

Jill wants to warn readers to be very suspicious of these Facebook ads. It’s always risky to give out your card number unless you absolutely trust the online seller. And always read and understand the fine print.

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