

MAIL FRAUD GOES ONLINE

Most of the scams I write about hit us through the phone or online. But it's worth remembering, not all scams depend on electronic communication, and some scams that involve the phone or online use, also need action through the mail to complete the scam.

I've got an example out of Delmar, Iowa to drive this point home. A Delmar couple noticed they did not receive mail for several days – thought it was odd. At the same time, they noticed a \$1 charge on their bank account, paying the US Postal Service. Even more odd. The couple made a trip to the Delmar post office, and learned someone went online to the postal service website and filed a change of address for their mail, forwarding it to Michigan. As it turned out, the forwarded mail went to a vacant house.

What happened here? Well, you can go to the postal service website, www.usps.com, and create an online account. With that account, you can take care of different kinds of post office business, including filing a change of address. But when you do it online, it's not a free service. The postal service requires you to post a credit or debit card number. The postal service system verifies your card number as associated with your address, as a safeguard against malicious or criminal change of addresses. In the case of the Delmar couple however, the crooks who filed the change of address already compromised the couple's card, allowing their change of address to go through unchallenged.

Why did the crooks want to forward the Delmar couple's mail? Most likely, the crooks planned to open fraudulent credit card accounts with the compromised information, and get the new cards and statements sent somewhere where the victims would never see them. It didn't work this time, because the Delmar couple paid attention to their lack of mail and their bank account.

The postal service built another safeguard into the system for these mail forwarding orders. Such an order automatically generates a confirmation letter from the postal service to the original address, asking "did you really want your mail forwarded?" In the Delmar case, the victims did not recall ever receiving this letter.

So, I see a couple of tips here for us. First, pay attention to your credit card statement or bank statement. Look at all the charges. Challenge any that you did not make. Second, look at your mail. Don't overlook mail from the postal service. That confirmation letter might be your only clue something crooked is about to happen to you.

The postal service recently introduced another service which allows users to get a heads-up on what mail to expect. This is Informed Delivery. You need an email address for this to work. If you use this service, you can expect an email notification each day of mail delivery, which will

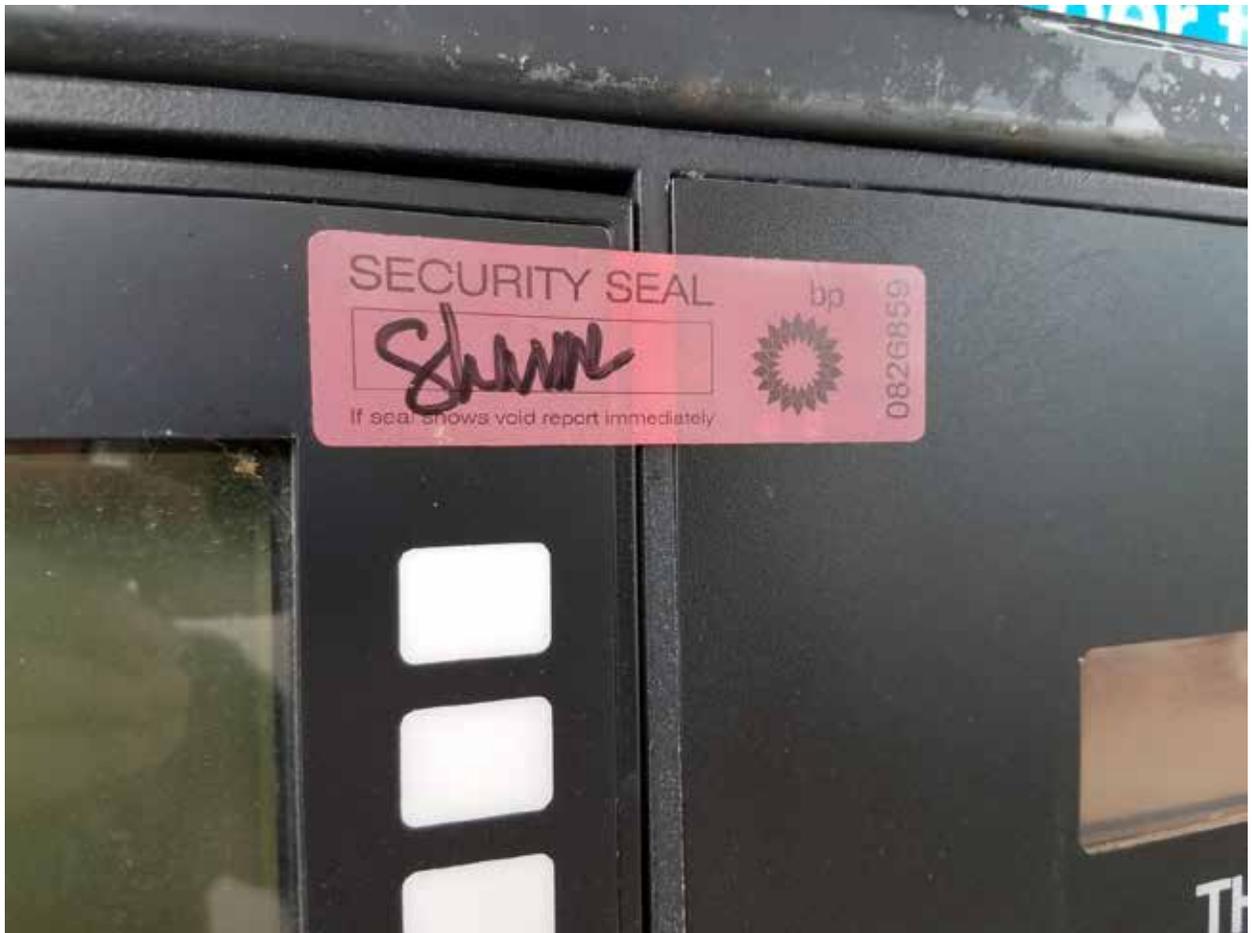
display an image of every letter-sized piece of first-class mail the mail carrier expects to deliver to your address that day. You can sign up for this service at www.usps.com. No charge for this service.

GAS PUMP SKIMMERS – REVISITED

In January 2017, I wrote about the rash of folks complaining of credit card fraud, and how they suspected using their cards at gas pumps compromised their cards. There's no question a lot of credit and debit cards are compromised at gas pumps through the use of skimmers. Skimmers are illegal card readers attached to payment terminals, like gas pumps. These can be difficult to detect, but it is not impossible. The Federal Trade Commission recently published some tips for spotting skimmers:

- Make sure the gas pump panel is closed and shows no sign of tampering. A lot of stations place security seals on the pump panel. If someone tampers with the seal, it will read "void". I would not use that pump, instead notify the attendant. I spot-checked several Clinton gas stations, and found these seals at half of the stations I checked. These photos show you what to look for.





- Look at the card reader. Does it look different than the other readers at other pumps at the station? Does it wiggle? If it moves, tell the attendant.
- If you use a debit card, run it as a credit card instead of entering your PIN. This safeguards your PIN. Not all pumps will allow this.
- Keep a close eye on your credit card and bank accounts for unauthorized charges. If you find one, report it immediately. Don't delay.
- You can always pay inside, by-passing the pumps entirely, and the risk of skimmers.

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