

MORE AND MORE CALL SPOOFING

The Dewitt Police Department informed me they received complaints of folks in Dewitt receiving telemarketing calls that show up on Caller ID as originating from a Dewitt city hall number. This is yet another example of call-spoofing, or the practice by crooked telemarketers, or just plain crooks, to deliberately falsify Caller ID information, to disguise their identity. While the technology which allows this deception is not new, advances in technology now allow more widespread use of this technique.

In recent months, I received reports of spoofed calls appearing to originate from the Clinton Red Cross and Genesis Medical Center in Dewitt. Those are the kind of calls which most people will answer when they see that name display on the caller ID screen. Which is exactly why crooks want to spoof those numbers. I'm also getting several reports each week of "neighbor spoofing", or calls which appear to come from a private residence number in the local area. Again, the goal of this deception is to mislead us to believe an incoming call comes from someone in our locality, and there is no harm in answering.

Is anyone trying to shut down these operations? The Federal Communications Commission (FCC) is the agency charged with regulating telecommunications. I checked their website and saw the agency issued a statement on August 3, 2017, notifying us of a proposed fine of \$82 million against a health insurance telemarketer, Best Insurance Contracts of Wilmington, North Carolina. An FCC investigation starting in December 2016 showed this telemarketer made 21 million robo-calls trying to sell health insurance to elderly, infirm, or low-income families, using phony Caller ID information.

The same FCC statement reported two other FCC actions:

- Proposed a \$120 million fine against someone for making almost 100 million spoofed robo-calls selling timeshares
- Fined a New Mexico company \$2.8 million for providing the technology allowing fake Caller IDs

But we all know it is easier on everyone if we can prevent these calls in the first place, rather than going after the violators after the fact. The telecommunications industry seems to be making some effort at this. They developed a "Do-Not-Originate" list, which allows phone service providers to block spoofed calls from certain numbers, such as those that do not make outgoing calls, or from non-existent numbers. If you are a phone service subscriber with lines which do not make outgoing calls, you can contact your provider to get that number on this list.

These kinds of solutions to the call-spoofing problem are heading us in the right direction, but we are a long way from our destination. In the meantime, we just need to realize Caller ID is

imperfect, and to be extremely wary of any telemarketing call, however it shows on the Caller ID.

ONLINE APARTMENT FOR LEASE AD FAKED

A young Clinton woman came very close to losing \$500 in a fake apartment lease scam this week. While the occurrence of this kind of scam is rather lower down the scale, it comes up from time to time. If you are a landlord, or someone using online sites to look for housing, this is something to keep in mind.

This woman, I'm going to call her Kelly, wanted to move with her children to another, larger apartment or house. She used a Google search to seek out Clinton listings, and ended up using a search engine for real estate classified ads called Trovit. She saw an ad for an apartment, but when she clicked to open, the ad re-directed her to another property. This was a house for rent, it looked pretty nice and the rent was within Kelly's budget. Kelly corresponded by email with the landlord, who claimed his employer transferred him to New York. He sent a rental application and approved Kelly as a tenant, providing she sent the first month's rent to him by Moneygram, a wire transfer service.

So far, this sounded okay to Kelly. She went to a Moneygram agent, and paid the \$500 to transfer, but Moneygram rejected the transfer. Apparently something in the information provided by Kelly triggered a fraud alarm within the Moneygram system, blocking the transfer. Kelly called the landlord back and explained the problem. He suggested going to Western Union, another wire transfer service. She did, with the same result. Now Kelly started doing some background work, and found a phone number for the real landlord of the house she wanted to rent. When Kelly called him, she learned he did not list this property on Trovit, and he didn't expect rent it for \$500 a month. The landlord recognized this as a scam, and put Kelly in touch with me.

It seems what happened was the crook lifted the material and photos from a real classified ad posted by the landlord on Zillow, a popular real estate website, and created his own listing on other websites, directing potential renters to contact him. He offered pretty cheap rent to entice victims in.

This story shows us again, it is not difficult to fabricate a deception on the internet. The first red flag here was the landlord's request for payment via a wire transfer service. Such requests are ALWAYS a scam.

DRIVEWAY PAVERS STRIKE AGAIN

In both May and July of this year, I warned in this column of driveway sealers. These are the folks who show up and offer to seal your asphalt driveway. They almost always come from out-of-state, and are considered peddlers or door to door salesmen, under Iowa law. They commonly aggressively badger their potential customers to accept the service, use a low-grade product, do sloppy work, and demand outlandish compensation. And they never comply with the local ordinances and state laws which govern their business practices.

True to form, that's how a sealing contractor based out of Texas scammed a Clinton man in early August. The contractor pulled into the man's driveway, and without mentioning price, offered to seal the asphalt portion of the driveway. When the customer hesitated, the contractor started spraying oil, to demonstrate "how far a gallon will go." And he never stopped. He never bothered to write a contract, discuss price, or offer the customer the chance to stop the work. When he finished, the contractor demanded \$16,000 for spraying a driveway I measured at 294 square yards. The customer balked, so the price got lowered to \$15,000. Feeling intimidated by the whole process, the customer went to his credit union and obtained a cashier's check for the contractor. A few hours later he reconsidered, and tried to stop the check's payment – too late.

If these traveling sealers or pavers show up on your property, don't talk to them except to tell them to leave. They will cheat you any way they can, and once they leave, will be difficult to find again. If you start talking to them, they will unpack their trucks and begin working, and won't stop. My advice is to run them off right away, and if they won't leave immediately, call law enforcement.

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