JUNE EDITION Chief of Police Dennis J. Mc Enerney 2017—Volume 4, Issue 6

S.C.R.A.M. GAZETTE

Beware of 'Deceptive Door-knocker' scams

Experts say with the warmer weather comes a rise in scams across the Chicago area – and offenders are emboldened to knock directly on their victims' doors.

The Better Business Bureau and ComEd warned consumers on Tuesday about "deceptive door-knockers" who claim to be utility workers or contractors, but are really looking to steal your money or personal information.

According to the BBB, these kinds of con artists will knock on their victims' doors and try to convince them to purchase a variety of shoddy home services, or attempt to take payment with false claims on their alarm, cable or electric services.

ComEd said the company has seen an alarming increase in a variety of

energy-related scams, from fake utility workers to callers threatening to cut off power to a home unless an immediate payment is made.

"They'll use any trick to get into your home," said BBB Chicago president and CEO Steve Bernas. "Every week, we hear from consumers who have basically been duped in some way by allowing somebody into their house, whether it be, 'I gotta check your water, your pipes in the basement. I want to take you out to the yard.'"

"We had one a few weeks ago that said, 'I hit your garage on accident, can you come out and look at the garage damage?' and basically the person went in the front door and robbed them," Bernas added.

According to experts, there are ways to recognize these scams and protect yourself.

Officials warn against giving out your Social Security number or any personal information to someone who claims to be a utility worker without contacting the company first.

You also should not believe claims demanding payments in 30 minutes, or with cash or a prepaid debit card.

Consumers are also encouraged to report anything suspicious to the Better Business Bureau's "Scam Tracker" on the agency's website.

ComEd and the Better Business Bureau Warn of Potential Scams

A warning for homeowners: Beware of who's knocking at your door or calling claiming to be with ComEd. The weather is warm, and that means utility scam and home repair scam seasons are just beginning.

ComEd and the Better Business Bureau have teamed up to warn consumers to watch out for people posing as utility workers to cheat people out of their money.

Most victims of utility scams tend to be elderly people, but ComEd says an increasing number of victims are in the Hispanic community.

ComEd and the Better Business Bureau said it's a combination of spoof calls and in-person scams.

"They look very credible. People are typically very charming. They have a good story to tell, and this lack of awareness and people just wanting to believe people are doing something good for them lead them to fall victim," ComEd vice president Fidel Marquez said.

ComEd states that they will never call to threaten a customer with disconnection if you don't pay immediately, or make a payment. They will not go to your home and request to see payment.

Next Presentation
9/13/2017
11 am
Confidence Scams

Niles Police Department
7000 W. Touhy Ave
Niles, IL 60714
847-588-6500
www.nilespd.com

Connect with US!

WWW.NILESPD.COM

Don’t fall for this computer virus scam!

The Federal Trade Commission said Friday that it's bringing 16 new enforcement actions, including complaints, settlements, indictments, and guilty pleas, against tech fraudsters. But Florida Attorney General Pam Bondi -- who is working with the FTC on the issue -- warned there are still more scammers out there, and regulators need the public's help to catch them.

"The only way we're going to stop this is if you report it," Bondi said.

She asked that people immediately notify the FTC if they see pop-up ads that warn people their computers are infected with a virus or malware and solicit them to buy virus protection software. The ads are often designed to resemble legitimate security alerts.

They often prompt the user to call a phone number to get help. Anyone who calls gets a slick-talking telemarketer who works to convince them that they need to spend hundreds of dollars on new protective software, even though their computers may have never been infected in the first place.

After a victim grants computer access to the scammers to install protective software, the scammers can put spyware on the victim's computers, which can expose everything from family photos to financial information, the FTC says.

The commission has received more than 96,000 complaints from people who have been swindled out of a combined total of more than $24.6 million, according to FTC Acting Director Tom Pahl.

Elderly people and tech newbies are particularly vulnerable. At Friday's press conference, Pahl played a recording of a 90-year-old man on the phone with an alleged scammer.

"I'm new to the computer," the elderly man says.

Then, a salesman tells the man "you have a [computer] infection" and pressures him into agreeing to pay for "repairs."

"You're 90 years old, you have intelligence," the salesman says. "This is not hard stuff."

The salesman also identifies himself as a certified Microsoft repairman, a common tactic used by these types of scammers, according to the FTC.

Pahl said the FTC has worked with Apple (AAPL, Tech30) and Microsoft (MSFT, Tech30) to bring charges against these fraudsters. And he advised people who suspect their computer has a virus to contact Apple or Microsoft support centers directly.

"If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, stop. Don't download anything, don't call the number on the pop-up and don't give anyone control of your computer," the FTC said in a blog post Friday.

Malicious ads can be reported to the FTC online at ftc.gov/complaint.

Scams most frequently target those who use Social Media

A recent trend in which victims are being targeted for financial crimes are occurring in which they target victims via social media. Officials say the scam starts with the suspects befriending a potential victim online, before asking for their banking information, ATM card and PIN numbers, with the promise that the victim will receive a portion of the monetary gain.

As part of the scam, the suspect deposits forged payment instruments into the victim's account and then withdraws as much money as possible. The victim is then left responsible for the lost funds when the bank determines that the original instrument was forged.

Officials say the scam typically targets young adults.

Local law enforcement is urging all citizens, in particular young adults and parents of young adults, to protect their banking and financial information.

In light of the scam, Police offer the following tips:

- DO NOT give out your personal information (SSN, bank account number, PIN).
- DO NOT give access to your ATM card.
- Check your credit and bank account transactions often.
- Be cautious when communicating with unknown people on social media.

Upcoming Events
National Night Out
August 1,2017
Oak Park (Main & Ottawa)