Watch out for these impersonation scams

No, it isn't Microsoft, your grandchild, E-ZPass, or the electric company contacting you. It's a scammer!

Published: August 12, 2014 12:00 PM

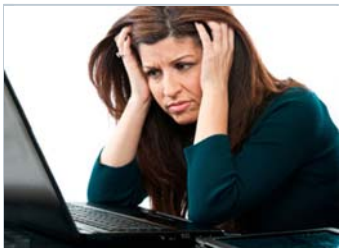
Judging from warnings we've seen online, impersonation fraud is rampant. Scammers are trying to get your money, your personal information or both by pretending to be a government worker, a utility-company rep, or even a family member.

We recently wrote about imposters posing as IRS agents attempting to recover back taxes and hotel employees seeking guests' credit card information. Sadly, plenty more scammers are out there. Consider these cases from across the country. Even if a scam is limited to specific states now, it's likely to spread or show up in other forms, as evil-doers look for new and creative ways to trick you.

Scam 1: You're a deadbeat

The Illinois state attorney general has warned about scammers pretending to be from her office, e-mailing final notices about overdue loans. Don't pay, and you'll face prosecution, the e-mails say. "Do not respond to anyone claiming to represent my office with demands for money or threatening prosecution," Attorney General Lisa Madigan said in a statement. Attorney General Patrick Morrisey of West Virginia recently sent out a similar alert about fake debt collection companies' calling about unpaid credit card debt.

Scam 2: Your computer's in critical condition



A couple of Consumer Reports employees recently were targeted with what's known as the tech support scam. Someone calls claiming to be from the likes of Microsoft, Windows, or "computer tech support," saying your computer is experiencing serious errors or has a virus. To prove it, the caller may ask the would-be victim to check his or her Windows event log viewer, which is likely to contain thousands of records about various errors, most or all of which actually are nothing to worry to about. That was the case with a woman who called one of our employees, claiming to be from Windows PC services and warning that the staff member's computer was in critical condition based on the reports it supposedly had sent to the "Windows main Web server." Following her instructions, the employee reported that there were about 20,000 application-related events recorded.

"20,000?" she said. "Oh God!"

"That's no good?" the employee asked.

"No, that's not good," she said, with someone coaching her in the background, "Sir, these are the errors and warnings I was talking about."

The employee played along until the caller asked him to log onto a Web service that would let her take control of his computer. Ironically, the independent website has a warning about the tech support scam and the danger of allowing people you don't know access your computer. In tech support scams, the FTC says, the scammer's goal may be to change your computer's settings, install malware that can steal your personal information, or trick you into enrolling in phony computer maintenance or warranty programs.

Scam 3: You're a toll dodger

In a scam that's making its way around the country, e-mails tell would-be victims that they owe the E-ZPass system for unpaid highway tolls (PDF). The e-mail instructs recipients to download an invoice that supposedly has been sent many times before. It appears to be an attempt to persuade people to download malware to their machines. Representatives of the real E-ZPass toll agency say they send violation notices by the U.S. Postal Service, not electronically. They advice against opening or responding to these e-mails.

Scam 4: You're a scofflaw

People in Maine have been receiving phone calls from imposters claiming to be from the state department of motor vehicles. The scam? Pay overdue fines immediately over the phone or end up in the pokey. In a similar scam reported months earlier, imposters claimed to be from the state's judicial system.

Scam 5: You're eligible for education grants

In yet another scam reported in Maine, the state's bureau of consumer credit protection says that people have been receiving calls from the likes of the "Federal Grant Program" and "Federal Treasury Department" promising thousands of dollars in government grants. Just pay a program or administrative fee, using Western Union, MoneyGram, or Green Dot MoneyPak, the callers say. Some also ask for bank account information so the grant money can be deposited automatically. Provide it, and you'll risk having your money withdrawn. One of the calls displayed a "202" area code on caller ID but was traced to India, the state said.

Scam 6: You're late on your electric bill

Want to keep your lights on? Then pay your overdue electric bill, say the bogus calls to residents of South Dakota. The Ohio attorney general reported a similar utility worker imposter scam in that state last year. Two victims lost about $800 each.

Scam 7: You're a wonderful grandma and grandpa

So-called grandparent scams have been showing up a lot this summer, says yet another alert from the West Virginia attorney general. There are many variants, but in all of them someone calls claiming to be a grandchild, niece, nephew, or other relative who has gotten into trouble, typically while traveling. Maybe they've been arrested, or they're having a medical emergency. Whatever it is, they need cash, which they ask the grandparents to wire. Callers may identify themselves as "your favorite grandchild" or they may get an actual name by checking Facebook or other websites where personal information is ripe for the grabbing. During the calls, the impersonators may pass the phone on to someone identifying his or herself as a medical professional or police officer. Or that second person may call back. The Michigan attorney general reports on one such case that cost the grandparents $33,000.

Don't be a recycling identity theft victim. And avoid being scammed by unscrupulous locksmiths, home improvement contractors, and burglar alarm companies.

What to do

Given the number of impersonation scams and the new versions that are popping up all the time, the best way to protect yourself is to be vigilant, especially when someone contacts you, whether by phone, e-mail, text, regular mail, or even in person, perhaps by going door-to-door. It doesn't matter how savvy you think you are. Ask yourself, "Could this be a scam?"

In some cases, you'll have clues that something is worth investigating further—the caller may have a foreign accent or your caller ID may display "not unavailable" or "private name, private number." Maybe that e-mail is from a company you know you've never done business with. Or perhaps you're asked to pay immediately by wiring money, obtaining a prepaid debit card, or handling out your credit card number or checking account and routing information.

In other cases, it will be hard to tell. The caller ID may have a "202" area code, exactly what you'd expect from an agency based in Washington, D.C.. Or you actually may owe money to the company or an agency that's supposedly contacting you, or you may have some type business relationship with it. Maybe the caller is using the name of someone you know or has personal details about you that you wouldn't expect anyone but a legitimate person, company, or agency to possess.

If you're asked to make a payment or share personal information, always verify. It doesn't matter that that e-mail is using a government or company seal or that a caller is being aggressive and threatening you with arrest or lawsuit. If you think the communication may be legitimate, recontact the individual, company, or agency to make sure. Don't click on links or use numbers provided in e-mails or texts. They could be bogus, taking you to the scammer's call center or a "phished" Web page that mimics the real one. Instead, obtain phone numbers, Web addresses, and other contact information separately, or check a previous bill or use a bookmark you've saved on your computer.

Illustration: David Senior

Also be careful about the personal information you make public, whether on Facebook or another type of social media, a Web site, or even to someone in person, perhaps someone asking you enter a contest in a mall or online. Also shred or carefully rip up sensitive documents before discarding or recycling them.

Beware of charity solicitations as well. Charity impersonation is widespread, especially following earthquakes, hurricanes, or other disasters. Before donating, check out the group with one or more charity watchdogs, the BBB Wise Giving Alliance, Charity Navigator, CharityWatch. Or, if it's a disaster-related donation, give to an established group that's equipped to help in the emergency, such as the Red Cross.

Also, be cautious when using a Web search. If you're not observant, you can end up at a bogus website instead of at the legitimate one.

Finally, carefully examine your monthly checking and credit card statements. Don't simply assume that small charges or withdrawals are legitimate. Scammers sometimes attempt to rip off victims in small amounts, hoping they won't notice or bother questioning.

—Anthony Giorgianni