Modern Technology Fuels Old Scams

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity and respect

Scams and scam artists have been around for hundreds of years. For instance, in the early 1820s, Gregor MacGregor, a Scottish soldier, arrived in England claiming that he was the Prince of Poyais. MacGregor issued bonds and sold land in Poyais, a phony country. Eventually, two ships of settlers departed for Poyais, a land described as extravagant and civilized. The ships, however, arrived in a desolate South American jungle containing snakes and deadly disease. The survivors returned to England to expose MacGregor's fraud.

Today, old scams have been given new life by modern technology that makes it cheaper and easier for perpetrators to target large numbers of victims. The following are some examples of the latest scams being fueled by new technology:

Fake Check Scams

People are being targeted by an array of fake check scams. The scammers send the person a real-looking check, which is actually a fake. Technology allows the scammer to cheaply print thousands of counterfeit checks that look authentic. The person is told to deposit the "check" and wire some amount of money to the scammer. After the check is deposited, it bounces; by then, however, the person has already wired money to the scammer and can't get it back.

The scam has many flavors. In some cases, the scammer targets someone who posts an item for sale online. The scammer may offer to buy the product and then send a fake check in too high of an amount, asking the seller to wire back the overpayment. In another twist, the scammer may send a counterfeit check as a phony prize winning, then ask the person to wire back money for taxes.

No matter the flavor, if you receive a check from someone you don't know—and that person asks you to wire back some portion of the amount of the check—exercise extreme caution. You're probably being hit up by a fake check scam.

Caller ID Spoofing

In years past, Caller ID could reliably tell people who was calling. Today, using inexpensive technology, scammers often "spoof" the Caller ID so that the number appearing on the consumer's Caller ID display is a fake number or fake business. Scammers may "spoof" their calling number to commit a wide variety of scams. Remember: just because a number or business appears on your Caller ID display does not make it the real thing. Exercise caution when you receive a call from an unknown caller who asks you to reveal private information, such as your bank account or Social Security number.

Bogus Cell Phone Text Messages

Nowadays, scammers sometimes send bogus text messages to cell phones of innocent consumers. The message may offer a junk product for a monthly fee, often $9.99. If the consumer doesn't "opt out" and decline the product (or sometimes even if she does), she may find unauthorized charges on her cell phone bill. For example, "Claudia" received the following text message: *IQQuizApp:Fun Facts billed at $9.99/mo.msg&data rates may apply. Reply HELP for help, Reply STOP to cancel.* Claudia had never heard of the company and ignored the message. A few weeks later, she received her cell phone bill and discovered she had been charged $9.99 for "IQQuizApp," a "service" she never ordered.

Most people do not know that their landline or cell phone bill can be used like a credit card, posting charges for unwanted products or services. This practice is called "cramming." Carefully review your phone bill each month to detect and stop unauthorized charges.

Phishing

Phishing, a widespread Internet and email scam, happens when a scammer lures consumers into divulging private account information. The scammer will pose as a consumer's bank and ask the consumer to "confirm" their account information. If they do, the scammers use the information to make unauthorized charges or commit the crime of identity theft. Phishers can send thousands of emails for pennies on the dollar; if even one person bites, the scammers make money. Remember: legitimate financial institutions do not send unsolicited emails asking their customers to reveal their account information.

Tips for Avoiding These Scams

- Never give out your personal information, including name, address, telephone number, and financial account information, unless you can verify the security and reputability of the company that is contacting you.
- Do not trust a website or Internet pop-up ad just because it looks professional.
- If somebody you don't know sends you a check and then asks you to immediately wire money back to them, the check is probably counterfeit.
- Carefully review your bank, credit card, and telephone bills each month for unauthorized charges. If you find one, promptly write to or call your bank or credit card company.