Scams-a-Lot: A New Series

by

Mike Pancione

With all the benefits the Internet has brought us there are also increased risks due to cybercrime. In the past, the Computer Club Executive Committee has attempted to highlight these risks in different ways: through cybersecurity sessions, training classes and Club meetings.

This series is devoted to identifying the large and growing list of scams that threaten the financial security of WV residents. I call this cyberthreat topic "Scams a Lot" to highlight various ways cybercriminals seek to steal money from naive people whether on the internet, via phone or even shopping. Of course, this is not a joking matter, as you may know already or will see as this series unfolds.

It's important to understand that all scams are fundamentally about taking your money. That's it. No matter what form scams take – phone scams, internet scams, scams in retail stores, ATMs, gas stations – in the end, scammers are trying to steal your money, no matter where it is kept. All they need is your help; and your ignorance can't hurt either.

Seniors are the most vulnerable to scams mainly because they are less educated about cybercrime and because they generally tend to have more money than other age groups.
That's why the AARP is devoting so much time to informing its members about scams. This is from a recent posting on its website:

> "The most common scams … now include several sophisticated schemes that criminals are using to steal money and personal information. Impostor scams are the most frequently reported, where criminals pretend to be government officials, police, businesses like Amazon or PayPal, relatives in trouble, celebrities, banks, or tech support professionals to steal money or personal data.
>
> Other prevalent scams include fake delivery-related text messages appearing to be from Amazon, FedEx or the U.S. Postal Service about package issues, phony job offers that steal personal information or money, bogus bank fraud warnings via text, fake unpaid toll notices, and romance scams. Employment scams have become particularly common, with fraudsters posting fake job ads or sending recruitment pitches to steal information or trick people into becoming unwitting money mules. Investment scams, especially those involving cryptocurrency, while fourth-most-reported, caused the highest financial losses at $5.7 billion in 2024."

It's debatable what your first line of defense against scams should be, but perhaps the easiest thing to do is to be a skeptic when dealing with unknown people or activities. If you become familiar scam-based terms, scenarios and the guidance of experts, you will be able to build a healthy wall of skepticism.

But, until you get that far, here is a brief look at what you can do, how you can do it, and what you will likely miss when you become fully skeptical.

How to Become a Skeptic – *In Brief*

1. **Become educated. There are numerous ways to stay informed**
   a. Identify a few trusted sources for information and be in the habit of checking them frequently
   b. Identifying and understanding scams will help you avoid being scammed.
   c. Avoiding being a scam victim takes some work, but far less than dealing with the fallout if you are scammed
   d. Check the two real examples of how scams occur, but remember: there are dozens of scams.

2. **Stop a Scam Before it Starts:** an ounce of prevention is worth a pound of cure
   a. **Share less in public.** The more personal info you post publicly, the more material a scammer has to work with when crafting a personalized attack.
   b. **Be suspicious of "emergencies."** Scammers often make urgent requests and pressure victims to act fast. Don't!
   c. **Have a no-share policy.** Never give anyone who contacts you—whether by email, text, phone, or in-app message—sensitive personal data.
   d. **Get an outside perspective.** Suspicious about something? Talking it over with friends, family or a neutral observer may help you see what's really going on.

3. **Deeper dives: two scams and what can be learned from them**
   a. **The Bank Scam: Your account has been compromised.** A 70-year-old widow, received a call that appeared to be from her bank's fraud department. The caller gained her trust by sharing the last four digits of her Social Security number and claimed her account had suspicious charges. Believing she was helping prevent fraud, the woman spent 90 minutes providing banking details, including her password. During the call, the scammer changed her account phone number and authorized a **$25,000 wire transfer** pretending to be her. Because the scammer kept her distracted, she missed the bank's alert email. When she later contacted the bank, the money was already gone. The bank denied reimbursement, saying she had voluntarily shared her information. The incident left the victim with only about $2,000 in savings and ongoing distress about how she was deceived.
      i. **How to protect yourself:** Scammers use technology that make it appear that a call or text is coming from your bank. Be a skeptic. Hang up contact your bank yourself, never via the caller (or texter). Remember much information about you is already on the internet.
      ii. **Confirm that the communication is real.** If a bank or government agency contacts you, don't assume caller ID is showing you correct information. Hang up and find a verified phone number, independently to call the bank or agency back. It's also a good idea to have all unknown calls sent directly to voicemail. This will dilute the sense of urgency scammers try to build.
      iii. **Never give your financial info to anyone.** Legitimate bank employees should never ask for your username, PINs, one-time access codes, or passwords. Banks understand this information is meant to be private and secure.
      iv. **Don't act fast.** To put you off guard, scammers will often say that a matter needs to be handled immediately or your money could be at risk. Don't react; hang up and confirm whether there is really an issue by calling and checking with the bank or government agency independently.

b. **The Shopping Scam: I'll take it!** A woman with a professional education listed a dining table for $250 on Facebook Marketplace. A buyer quickly agreed to purchase it and claimed to be Swedish, even sending a photo to appear legitimate. The buyer asked the woman to send $200 through Zelle to prove she was a real seller, promising to return it with the table's payment. Trusting the request, the woman sent the money. The buyer then asked for another payment for "insurance." Suspicious, she nearly backed out but tried to send it; however, her bank flagged the transaction as suspicious. When a bank employee questioned her, the woman realized she had been targeted by a scam. Meta says it is working to improve technology to detect and remove such scams on Facebook Marketplace. The woman only lost $200 but she could have lost more if her suspicions, and her bank's suspicions hadn't been raised. Protect yourself: selling or buying products online from another person is risky.
    i. **Know who you're dealing with.** When selling or buying on a site like Facebook Marketplace, check the buyer's or seller's Facebook profile and see whether they have friends and realistic activity, like recently posted vacation photos. Separately, check their past Facebook Marketplace transactions and reviews by other buyers and sellers.
    ii. **Be wary of anyone offering you full price.** If the buyer is willing to pay full price and/or isn't interested in the items condition, be skeptical that they are legitimate.
    iii. **Do not give a buyer your address or other personal information.** Agree to meet at a public place (such as a police station) and accept payment only in cash. Avoid Zelle, Venmo, and other instant payment methods which lack certain consumer protections.
    iv. **Use marketplaces with built-in protections.** Etsy and eBay, for instance, offer warranties for both buyers and sellers if transactions go awry.