Scams & Cyber Threats II

Everybody Is Somebody to an Online Scammer. You may think you're a nobody, too small a target to be worth criminals' time. Not so. Technology has made scams so nearly effortless that everyone is an attractive mark. But while anyone can be a victim, it's important to remember that everyone can take steps to better protect themselves online. To online scammers, you're not a nobody—you're an opportunity. Let's talk about how to minimize, monitor, and manage your way to better safety for your data, identity, and money.

Scammers are difficult to stop because they're continually perfecting their scams, taking advantage of tech innovations and honing their methods to better manipulate their targets. "We keep coming up with different tools to combat scams and fraud, but it's just like playing whack-a-mole," says Better Business Bureau spokesman Josh Planos. Scammers have become much more adept at impersonating legitimate institutions, including creating websites and messages that are "carbon copies" of legitimate health care providers, businesses and banks, with fewer grammatical mistakes and other red flags for scams, according to Planos. And criminals are not only taking advantage of technological innovations such as artificial intelligence (AI), they're also growing ever more adept at psychological manipulations.

Charity Scams

Americans contributed $319 billion to charity in 2022. This generosity supports many amazing organizations that put those billions to work for health care, education, environmental protection, the arts and many other causes. Unfortunately, it also opens a door for scammers, who capitalize on donors' goodwill to line their pockets. Charity scammers are especially active during the holidays, the biggest giving season of the year.

Some sham charities succeed by mimicking the real thing. Like genuine nonprofits, they reach you via phone, direct mail, email and even door-to-door. They might make appeals on social media and create well-designed websites with deceptive names. 4 Ways to Avoid a Charity Scam Video (1:00): https://www.aarp.org/money/scams-fraud/info-2019/charity.html

Many operate fully outside the law; others are in fact registered nonprofits but devote little of the money they raise to the programs they promote. Some create massive fundraising networks, often in the form of political action committees (PACs) - entities that can solicit money on behalf of charities or political candidates/causes - that they use as cover while requesting donations purportedly for various causes. Then they keep the bulk of the cash themselves. Two men who created PACs (including one called Americans for the Cure of Breast Cancer), were recently arrested and indicted on charges of colluding in a multiyear scam in which they stole millions of dollars from misled donors. With a little research and a few precautions, you can ensure your donations go to organizations that are genuinely serving others, not funding scammers.

Warning signs:

- Pressure to give immediately. A legitimate charity will welcome your donation whenever you choose to make it.
- A thank-you for a donation you don't recall making. Making you think you've already given to the cause is a common tactic unscrupulous fundraisers use.
- A request for payment by cash, gift card or wire transfer. These are scammers' favored payment methods because the money is easy to access and difficult to trace.

Protect yourself:

- Check how watchdogs such as Charity Navigator, CharityWatch and the Better Business Bureau's Wise Giving Alliance rate an organization before you make a donation, and contact your state's charity regulator to verify that the organization is registered to raise money there.
- Do your own research online. The Federal Trade Commission (FTC) recommends searching for a charity's name or a cause you want to support (for example, "animal welfare" or "homeless kids") with terms such as "highly rated charity," "complaints" and "scam."
- Pay attention to the charity's name and web address. Scammers often mimic the names of familiar, trusted organizations to deceive donors.
- Keep a record of your donations and regularly review your credit card account to make sure you weren't charged more than you agreed to give or unknowingly signed up for a recurring donation.
- Don't give personal and financial information such as your Social Security number, date of birth or bank account number to anyone soliciting a donation. Scammers use that data to steal money and identities.
- Don't click on links in unsolicited email, texts or fundraising messages on social media platforms; they can unleash malware or a virus.

More Resources:

- The Internal Revenue Service maintains an online database where you can check whether an organization is a registered charity and if your donation will be tax-deductible.
- You can report suspected charity fraud to the FTC and the government agency in your state that regulates charities.
- The BBB Wise Giving Alliance, Charity Navigator, CharityWatch and GuideStar provide a bevy of resources on charitable organizations, including ratings, reviews and tax and financial data.
- AARP Podcast #176. Couple and a homeless veteran stole $450,000 in a GoFundMe scam to benefit homeless veteran Johnny Bobbitt. When things don't seem to add up, investigators learn this story was all based on a lie.

Scams & Tips

- Bank Scams - Creating a fake version of a bank website is almost effortless for a scammer. They attempt to dupe enough people into giving away their accounts and passwords on the fake site. With stolen credentials in hand, they drain bank accounts, steal personal information, or just sell those credentials to other scammers.
- Texts from strangers - When you get a phone text from someone you don't know, a natural, polite instinct is to respond with a "sorry, you have the wrong person." But that can open the door to fraud. Delete the text and mark it as junk to block further contact. Even if it was an honest mistake, it's safer for you not to answer.
- Fake business eMails - If you receive a business eMail claiming there was a suspicious purchase on your account, do not respond or call the number listed. Go directly to the company's website and log in to your account. (The other option: Go to the organization's website, find its customer service number and call.) Crooks replicate big-brand emails in links that take you to a fraudulent site where they seek personal information or some kind of payment.
- Social media friend requests - Anytime you get a new friend request on social media, especially on Facebook, ask yourself: "Do I really know this person?" or "What does this person want from me?" Generally, it's best to turn down requests from strangers; they might be seeking personal information or intending a fraud attempt.
- Pop-up ads - These suddenly appearing ads have been around for years. Scammers insert code into the pop-up that, if clicked on or tapped, downloads malware to your device. Never click on one unless you are positive it's associated with a legitimate website.
- Computer virus alerts - Most people have seen those pop-ups claiming your device has been infected with a virus; sadly, this crime continues to work for scammers. Never call a number listed or click on the link provided. If you are having problems that suggest a computer virus, get in touch with a reputable computer tech support service.
- Phone calls from numbers like yours - Free software exists that lets a caller falsify the caller ID number that appears on a target's phone. So criminals might use a number that looks similar to yours, or your bank's number, or that of a government agency such as the IRS, Medicare or police department, to get you to answer. Let all suspicious or unexpected calls go to voicemail. Note that federal agencies will never call and ask for your Medicare or Social Security number or other identifiers.
- QR code directing you to a crypto ATM - Crooks can quickly and easily get you to send them money via a cryptocurrency ATM—then it is likely gone forever. They text you a QR code and instruct you to scan it at a machine at a store or gas station. Once you scan the QR code and make your payment, your money is in their hands.
- Gift cards - Consumers lost $228 million in gift card scams in 2022, says the Federal Trade Commission. Scammers prefer them because they have fewer protections for buyers compared with payment options such as credit cards. And the transaction is largely irreversible. If you are asked to pay for something by sending the codes off a gift card, it is very likely a scam.

- Scam or Real test about bank accounts: https://www.banksneveraskthat.com/
- Show Spam in eMail examples.

Additional Links and Information

Carondelet Tech Help Resources: https://carondeletvillage.org/tech-help-resources/
Questions or comments can be sent to: TCKreuzer@gmail.com