A VISUAL GUIDE TO FRAUD

Look for signs that you are being stalked by crooks

BY AMY NOFZIGER AND MARK FETTERHOFF

Sometimes the items shown here are perfectly legitimate; increasingly, though, scammers are finding ways to use these tools and technologies to defraud older Americans. Here's what some of the widely used fraud attempts floating around right now look like—and how they can be used to steal money.

1. 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.

2. A TEXT ABOUT YOUR NETFLIX ACCOUNT BEING SUSPENDED Did you get an email or text about your Netflix or other streaming service being suspended? As freaked out as you might be about not being able to catch up on your latest drama, take a breath and go into your Netflix account via the legitimate website. Do not call the number or click on any links in the email or text. This is a way for criminals to steal from you. If you provide any personal information through this link, they will try to commit identity theft in your name.

3. CAR WARRANTY OFFERS Criminals prey on our anxiety about facing large vehicle repair bills by pitching worthless car warranties. Often these scams come via a phone call, but they also come in the mail. Federal regulators have recently shut down groups that have stolen hundreds of millions of dollars through deceptive auto warranties. But others are out there.

4. FAKE BUSINESS EMAILS If you receive an email—ostensibly from Amazon, Netflix, Walmart or another retailer or service provider—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.

5. 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.

6. 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.

7. 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.

8. COMPUTER VIRUS ALERTS Most people have seen those computer 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.

9. 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.

10. 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.

ILLUSTRATION BY NICOLAS RAPP