knowledgeable thoughtful ethical experienced interac

summaries

SIGMA INVESTMENT COUNSELORS

the official newsletter of sigma investment counselors September 2025

PHONY LINKS AND OTHER SCAMS

Almost asleep, when my phone buzzed at 10pm, I checked my notifications and found a Fraud Detection alert text from our bank. I've received these texts before when making purchases that USAA's algorithm deems to be outside of our normal spending pattern, but this charge, for $972.14 at the Mircosoft Center in Atlanta, Georgia was not made by me or my husband. Ugh – what a nuisance. Grateful that the algorithm caught and denied the transaction, but annoyed I would need to cancel the card and all automatic payments set up using the card, I hesitated before confirming that, "NO," I did not authorize this activity. I'm used to deleting texts about my "unpaid tolls," and those offering me a job making $300/day for an hour of work, but this was a text from my bank, in a similar format to what they've sent before. I opened my banking app to see if there were any alerts on the app, and finding none, asked the chatbot if it had noticed fraud on my account. With no alerts, and no confirmation from the USAA chatbot, I looked again at the text. The "Mircosoft Center." There it was – a giveaway typo.

Scammers have always been trying to part us from our money, but with the rise of Artificial Intelligence, the prevalence of texting and transacting online, and editing software, these attacks are becoming harder to detect. Below are a number of common cons, and how you can protect yourself.

Phishing Texts (Smishing): These are fraudulent text messages, urging you to act to remedy a problem (a package delivery, or suspended account), typically by clicking on a link. This link may install malware, or prompt you to enter sensitive information which will be delivered right to the criminals. If you receive these texts, avoid clicking on any links. If it appears to be a legitimate text – verify by logging into your account with the company using your phone app, or by searching for the company's phone number and calling customer support.

Pig Butchering: Another type of texting scam; this often preys on the lonely. The texts start out innocuously and look like wrong number texts – asking to meet for coffee, or confirming you'll be at the park tomorrow. If you respond to let the person know they have the wrong number, they'll tell you how kind you seem and attempt to create a relationship. Once a relationship is established, they request money – either convincing you to invest in a product so you both can be rich and travel the world together, or for a personal "emergency," - a surgery, or a repair. For as tempting as it can be to make a new virtual friend, it is better to not respond to these texts.

Phone Call Scams: These calls are designed to create a sense of urgency – a phone call comes in to Grandpa, telling him it's Grandson, and he's in trouble. Please don't tell mom or dad, but money is needed urgently, either by wire, or gift cards. These callers are preying on your desire to help your family. Often, if you question their story, or ask for verification that it is indeed the person they are claiming to be, they'll hang up. Have a passphrase established or a question that you can ask your children/grandchildren to verify their identity.

Personal Email Compromise: When your password is compromised, and criminals are able to access your email, the havoc they can wreak is unlimited. Combing through your emails, they can determine where you bank, update passwords on other sites, and impersonate you to request funds, or email address or bank account changes. It is tempting to reuse passwords

across websites, but the password for your email should be different from any other password you use.

Phishing Emails: Similar to phishing texts, phishing emails look like they are being sent from legitimate companies, and ask you to verify or confirm information by clicking on a link. Once you click on the link, they may ask you to share identifying information, or they may install malware on your computer. You should never click on an unexpected link (we will always email you separately to let you know if you will be receiving correspondence from us that requires you to take action), and if you have any concerns, call the company which has sent the email using the phone number for customer support found on the company website for verification.

Checkwashing: Handing a check to someone you know likely doesn't pose much risk (as long as they dispose of it appropriately after cashing it). However, sending a check through the postal service can expose you to checkwashing – where criminals steal a legitimate check, and "wash" it – changing the payee, amount, and/or check number. Because the signature on the check is legitimate and matches the signature the bank has on file, banks often cash these checks. Try to use checks only with people you know and trust, and avoid putting a check in the mail if you can. If you do need to mail a check, make sure you monitor your checking account, and view the image of the check once it has been posted.

Unfortunately, this list represents just a fraction of the fraudulent methods criminal's use. Although technology makes our lives easier in many ways, it also opens up new and myriad ways for us to fall victim to scammers. Be wary – trust, but verify – when it comes to your money. We all know better than to believe that there is a prince who is just looking for someone to share his millions with; we also need to be wary now of our "bank" trying to "protect" us.

Amanda E. Lehnert, CFP®