ACCESSbank®

Digital Banking Safety: Tips for Senior Bankers

Phishing scams and spam frequently target seniors with Medicare actions, spoofed bank notices, urgent needs, family scares or official looking IRS documents.

Understanding characteristics that may increse vulnerability:

- **Limited computer skills** such as installing security software and setting up firewalls.
- **Minimal internet skills** and interacting with websites, understanding the reach or the internet, tricks used by cyber criminals, and how to recognize fake websites.
- **More trusting** even though they may be able to size up the character of someone in person, online is a different story.
- **Social networking** targets seniors with irresistible quizzes and surveys that often are asking for information about health, wealth and personal lives used by many companies to generate spam.
- **Cyberbullying** with emotional abuse, threats, accusations and financial abuse aimed at finding out personal and account information.

Major Scams Affecting Seniors:

Personal emergency scam: Scammers email or post social media messages that appear to be from someone you know saying they are in distress, such as having their wallet stolen or having been arrested. If you get such a message, find another way to verify if it's true, such as reaching out directly to the person. If you get such a message from a friend, there is a good chance that their account was hacked and that it's a criminal who is out to steal your money.

You owe money scam: Be wary of emails that claim you owe money. If you hear from a bill collector or a government agency about money "owed" by you or a family member, don't respond unless you are certain it's legitimate. It's common for scammers to send "bills" to people who don't owe them money.

Online dating scam: Many people have found love via dating websites, but others have been scammed out of money by online con artists. These fraudsters create fake profiles on dating sites and social media. They can be quite good at playing the long game. Never share any personal information such as financial circumstances, account numbers, or your social security number with anyone.

Infected computer scam: You might get a call from "Microsoft," saying your computer is infected or vulnerable to hacking, with an offer to fix it for you. Hang up. Microsoft and other reputable companies never make these calls. These are criminals trying to steal your money and plant viruses on your machine. Also be suspicious of any messages in email or that pop-up on your computer, in your Web browser or on a mobile app warning you of a virus or a security risk. If you have reason to suspect that your device is at risk, consult a trusted expert but never download software or apps that you aren't certain come from legitimate sources.

ACCESSbank®

Digital Banking Safety: Tips for Senior Bankers

Follow these tips to avoid scams

1. Never click a link sent to you by someone you don't know. Clicking a link may take you to a website that looks like your bank or credit card company. Look closely at the website address and make sure it is real. And verify the URL address from a separate source such as a bill.

2. Do not trust an email that's "phishing" for personal or account information. These can be very convincing, so look for things like spelling errors and be warned that a quality scam can look very real. Just remember, no bank or reputable company is going to send you an email asking you to correct or validate personal information or re-enter your password.

3. Watch for unsolicited emails with an urgency for response or deal that is too good to be true. Scammers want you to react without taking time to think things through, so their emails frequently sound urgent.

4. Protect your information. It is better to be rude than to be ripped off, so demand validation, verification, and authentication before giving your information to anyone.

5. To avoid being the victim of a scam, don't click on or respond to suspicious links, attachments, calls, and pop-up messages.

6. Ignore and do not answer unsolicited phone calls, calls with "unknown" displaying on caller ID and "robocalls." Be careful – a scammer can also display a known company on caller ID. This is called spoofing.

7. Don't respond to or click on pop-up windows on your phone or computer.

8. Don't open any attachments unless you know the sender and were expecting them to send it.

9. Be wary of strange or unexpected messages, even if they're from people you know.