BE $CAM $MART

It is imperative, now more than ever, that you protect yourself, identity and lifesavings.

Have you received an urgent message by phone or e-mail such as:

- "Your password has been stolen."
- "There's a problem with your Social Security."
- "Your account (bank, social media, e-mail…) has been hacked."
- "You face legal action if…"
- "Your computer is infected…"
- "You won a lottery or inheritance and need to send money."

The occurrences of SCAMS and PHISHING are ever-increasing. Follow these simple steps to protect yourself.

1. **DO NOT click the link in e-mail, text, Messenger or provide information over the phone.** Call your bank, credit card company, Social Security Administration, utility company, etc. through a verified phone number on a statement or your card.
2. **NEVER give anyone you don't know remote access to your computer or pay them to fix it.**
3. **NEVER give personal information** (Social Security number, credit card, birthday or other sensitive information) over the phone unless you initiate the call.
4. **STOP ALL contact** with someone you meet online as soon as you suspect they're an imposter.
5. **DO NOT send gift cards or money** to someone that you do not know or someone you have met online.
6. **DO NOT answer calls from phone numbers you do not recognize.**
7. **BE WEARY and do not rely on caller ID.** Scammers are using "spooling" tools to make it appear the phone number is from a legitimate business, utility or government. Let it go to voicemail and then independently look up the entity's phone number and call it to verify you were legitimately contacted.
8. **Misspellings and grammatical errors are RED FLAGS.**

Once you fall prey, you are added to a list that is shared throughout the dark web as a potential target and will continue to receive scams. Report the incident to the Federal Trade Commission and local authorities.