CITIZENS

FRAUD MADNESS

UPDATE

Sharp Shooter Tips About Online Selling Scams

Low prices for high quality items. If it's too good to be true, it most likely is. If someone is selling next to new items for very low prices, beware! Often, an impersonator has hijacked someone's profile and used it to upload items for sale. It is often disguised as an estate sale for a family member or a moving sale and they need items gone ASAP. Impersonators often have the same posts on many different groups. You may see the same items being sold across different groups.

Commenting has been turned off. If the seller turns off comments and asks you to message them directly, it's likely because they don't want anyone commenting or alerting others that the post is a scam. By communicating through direct messaging (DM), they can try and scam many people on the same items all at once. Steer clear!

Down payment. If a seller asks you to pay up front or even put a little money down to secure your sale, do not do it! Chances are, the item may not even exist. Make sure you have seen the item, and it meets your expectations before exchanging any money.

Safe meet-up suggestions. Make sure you are safe when meeting someone for an online pick-up. Meet in a public area with lots of people when possible. Bring another person with you if you can. Always tell someone where you are going. If something seems off about the pick-up, report it.

Citizens BANK MINNESOTA

Member FDIC

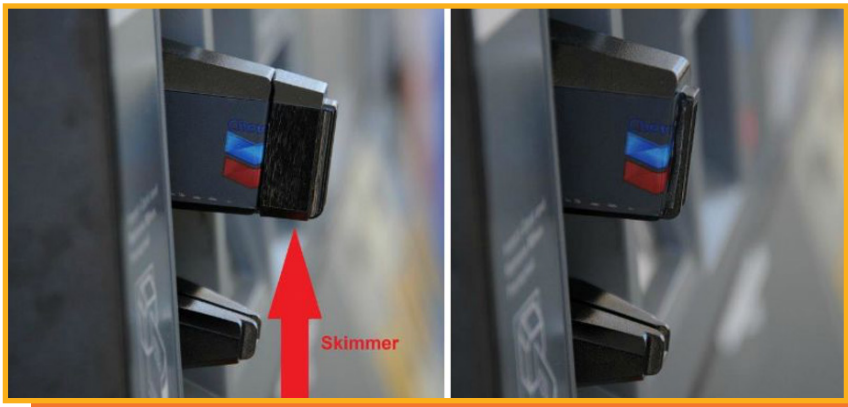
WooHoo! Banking®

WooHoo! IT'S WHAT WE DO!

SPOT THE WARNINGS
CARD SKIMMERS

- Look at security seals and note if they have been broken or tampered with. If tampering has occurred, you may see the words "void" appear on the sticker where the sticker has been peeled.

Check to see if anything looks suspicious. If so, compare it to other card readers in that place of business. For example, look at other pump terminals at a gas station or glance at another checkout lane in a store.

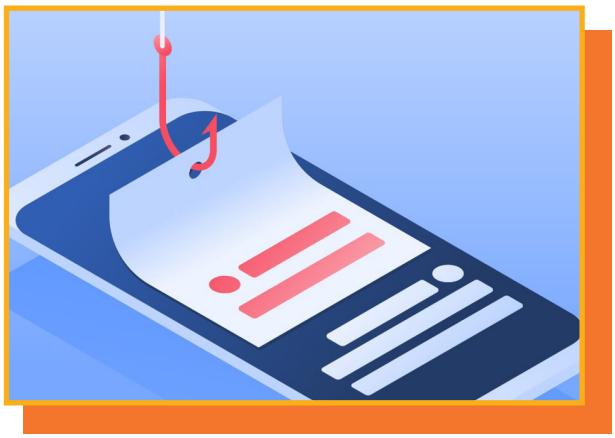


- Give the terminal a little jiggle. If something seems loose or wiggly, inform an attendant or employee about your concerns.

PLAY TOUGH DEFENSE AGAINST PHISHING SCAMS:

PHISHING: Targets consumers by sending them an e-mail that appears to be from a well-known source.

DO Inspect the email, make sure everything looks correct. Hover over any links before clicking on them to see where they would take you and if it looks legitimate. When in doubt, reach out to the sender to see if they did indeed send that email. If you're at work, report it to your IT department and have them take a closer look.



SMISHING: Social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals.

DO Do not respond to the text or click any of their links. Call the merchant or business directly using verified contact information that you can find directly on their website or in a phone book. If something seems odd, do not respond and block the number.

VISHING: A fraudulent phone call that tricks victims into providing personal information by pretending to be someone they are not.

DO When in doubt, always hang up and call the business directly with a verified phone number. Do not respond to someone who is creating urgency for an action. Do not trust caller ID, caller identities can be faked or spoofed.