Social Engineering

In a social engineering attack, an attacker tries to manipulate a person into performing an action or disclosing information.

People have a natural tendency to trust. Social engineering attacks exploit this tendency in order to steal your data.

Once the attacker gets your information, they can use it to commit fraud or steal your identity.

Criminals use a variety of social engineering attacks to steal information, including website spoofing and phishing.

This brochure explains the meaning of these common attacks and provides tips you can use to avoid becoming a victim.

Learn More

To learn more about avoiding social engineering attacks, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- CISA.gov

CYBERSECURITY AWARENESS

Avoiding Social Engineering Attacks

TXN BANK

Website Spoofing

Website spoofing is the act of creating a fake website to mislead people into sharing sensitive information. Spoofed websites are typically created to look exactly like a legitimate website published by a trusted organization.

PREVENTION TIPS

Pay attention to the web address (URL). A website may look legitimate, but the URL may be misspelled or different.

Do not click links on social media sites, pop-up windows, or non-trusted websites. Typing an address into your browser is a safer alternative.

Avoid using websites if your browser displays certificate errors or warnings.

Only type sensitive information (e.g., credit card numbers, social security numbers, etc.) into websites you have verified are legitimate. Make sure the URL begins with https:// instead of just http://. (The “s” means your data will be encrypted when you submit it.)

If you are suspicious of a website, close it and contact the company directly.

Phishing

Phishing happens when an attacker attempts to acquire information by masquerading as a trustworthy entity via email, text message (smishing), or phone call (vishing).

PREVENTION TIPS

Delete email, text, and social media messages which ask you to share sensitive information. Legitimate companies will not ask you for information this way.

Do not click links or open attachments in unexpected messages or from unknown senders.

If someone contacts you, but it seems suspicious, try to verify if it is legitimate in another way.

For example:

- Navigate to the website yourself.
- Call the sender to verify.
- Perform a web search.

When in doubt, do not click.

Contact Us

Contact us if you suspect you have fallen victim to a social engineering attack and have disclosed information related to your account(s).

Regularly monitoring your account activity or enabling transaction alerts is a good way to detect fraudulent activity.

If you notice unauthorized account activity, notify us immediately.

HOW TO REPORT

If you need to report suspicious activity, please contact:

TXN Bank
ORGANIZATION NAME

830-426-3066
PHONE NUMBER

https://www.txn.bank/
WEB ADDRESS