



Beware of Phishing Scams

Phishing is the fraudulent practice of sending calls, texts, or emails impersonating legitimate companies. The goal is to trick you into providing your personal information or to click on a malicious link.

Caller ID Spoofing:

Caller ID can be manipulated by scammers to display false information, making it appear as if the call is coming from a trusted source. Always exercise caution when receiving unexpected calls, even if the caller ID appears legitimate.

Email Spoofing:

Scammers can easily forge email addresses to make them appear genuine. Even if an email seems official or is from a known contact, be wary of clicking on links or providing personal information without verifying the sender's identity.

Text Message Spoofing:

Scammers are sending phishing text messages which often impersonate legitimate organizations, including fake fraud alerts attempting to trick you into providing personal information or clicking malicious links. Remember, reputable companies won't ask for sensitive data via text. If you receive suspicious messages, don't respond or click any links.

Recently, the United States Postal Service issued a media release warning against unsolicited text messages claiming that a USPS delivery needs immediate response. Another common example is from state turnpike authorities indicating you have unpaid invoices which must be paid immediately to avoid a ticket or late fees.

Trust Building Tactics:

Scammers may use tactics to build trust, such as starting with harmless requests before escalating to more invasive demands. Remain skeptical of any unsolicited communication, especially if it involves requests for sensitive information or unusual actions.