

National Consumer Protection Week

March 2 - 8, 2025

Consumer Scam Education

As part of our ongoing commitment to your security, we want to bring your attention to the continued prevalence of phishing attacks and scams - providing education to help you avoid being a victim.

Here are some important reminders to help recognize and avoid phishing scams:

- **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 Messaging Spoofing/SMS Phishing (Smishing):** Scammers are sending phishing text messages which often impersonate legitimate organizations, including fake Fraud Alerts tricking your customers 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 Smishing attempt is from state turnpike authority's indicating you have unpaid invoices which need paid immediately to avoid a ticket or late fees.

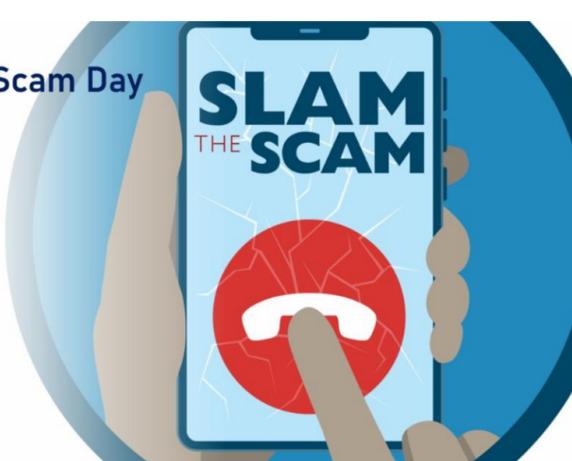
- **Trust Building Tactics:** Scammers may use tactics to build trust, such as starting with harmless requests before escalating to more invasive demands. Remain skeptical of any unsolicited communication, especially if it involves requests for sensitive information or unusual actions.

Source: DCI Security Bulletin - DCI Documentation Department, Data Center Inc.

National Slam the Scam Day

#SlamTheScam

MARCH 6, 2025



It's National Consumer Protection Week!

Visit ftc.gov/ncpw

or

<https://www.fidelitytopeka.com/additional-services/avoiding-fraud-common-scams/>

for free resources

#ConsumerProtection #NCPW2025

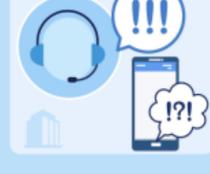
The following 2 resources are available as PDF Downloads from the bank's website:

<https://www.fidelitytopeka.com/additional-services/avoiding-fraud-common-scams/>

How Scammers Try To Steal Your Life Savings

People are losing big money to scammers running complicated scams.

Here's how the scam works:



A scammer pretending to be from a company you know contacts you, saying they supposedly spotted fraud on one of your accounts and your money isn't safe.



They connect you with someone else to supposedly help you move your money to "protect" it.



The "helper"— who often claims to work for the government — is really a scammer trying to steal your money.

If someone tells you to do any of these things, it's a scam.

- "Put your money in a secure account to protect it." **That's a scam.**
- "Transfer your money to a cryptocurrency account to protect it." **That's a scam.**
- "Get cash and I'll send a driver to pick it up." **That's a scam.**
- "Deposit cash at a Bitcoin ATM to protect your money." **That's a scam.**
- "Buy gold and a driver will come get it." **That's a scam.**

No one from the government will tell you to do these things. **Only a scammer will.**

Never transfer or send money, cryptocurrency, cash, or gold to someone you don't know in response to an unexpected call or message.



FEDERAL TRADE COMMISSION

More at ftc.gov/imposters

Report scams to the Federal Trade Commission at ReportFraud.ftc.gov

November 2024

Scammers Impersonate the Government

You get a call, email, or text message...

- ▶ They say they're from the Social Security Administration and your benefits will end unless you pay.
- ▶ They say they're from the IRS and you owe taxes.
- ▶ They say you need to give your Medicare number to get a new card.



STOP!

These are all scams.

Government agencies won't call, email, or text you and ask for money or personal information. Only a scammer will do that.

Report the scam to the FTC at

ReportFraud.ftc.gov



FEDERAL TRADE COMMISSION



Main Bank
600 S. Kansas Avenue
Topeka KS 66603
785-295-2100



Westridge Location
5926 SW 21st Street
Topeka KS 66604
785-228-8440

We do business Right here at home

"Follow" and "Like" us on social media



www.fidelitytopeka.com

