# CONNECT

CONNECTING WITH TFCU BUSINESS PARTNERS / Q3 / 2023

protect your business

# Prevent fraud

## Protect your business from common scams

It seems like fraudsters are always coming up with new ways to try and trick us into giving up sensitive information. Now, more than ever, we need to be careful to protect ourselves *and* our businesses. Here are some of the most common ways businesses are being scammed, according to the Federal Trade Commission.

**Phishing and malware.** These are common tactics that are used to target anyone, so the same red flags to watch for can be applied to your business setting as well. In these scenarios, scammers try to trick people into disclosing sensitive information by posing as a trusted source. Their communication often creates a sense of urgency and comes in the form of an email with prompts to click on dangerous links or attachments. Email addresses with suspicious domains, email misspellings and grammar errors can be a tell-tale sign that someone may be trying to access your sensitive information.

**Fake invoices.** Make sure you and your staff are always checking invoices closely to verify you're being billed for items you actually ordered and received, especially if the invoice is for something critical like keeping your website up and running. A sense of urgency is always a red flag for a scam.

**Directory and advertising scams.** Scammers could try to fool you into paying for advertising or a directory listing that doesn't exist. They might ask you to provide contact information for a

[continued on page 2]

## Protect your business from common scams

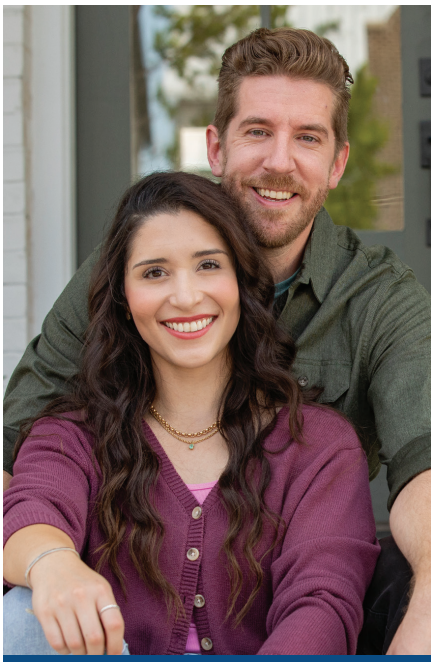
[continued]

free listing or try to confirm your information for an existing order. Then, they could use the details you provided to produce a bill and pressure you for payment.

**Tech support scams.** The goal of these scams is to catch you off guard with a call or email about your computer or internet security. They may ask you for sensitive data like passwords or try to get you to pay for a useless security system to a fix a problem you don't actually have.

**Government agency imposter scams.** Some businesses have been tricked by scammers impersonating government agents by threatening to suspend business licenses or impose fines. It should be common practice for you and your employees to be vigilant in verifying the legitimacy of emails and phone calls.

To see the full list from the Federal Trade Commission, click here to read their article. NN







## TinkerFCU.org/Partners

## Connect with us


**Walton Chan**
Business Development Officer
(405) 319-2183
1-800-456-4828, ext. 2183
chanw@tinkerfcu.org

**SayVon Milton**
Community Engagement Representative
(405) 319-2182
1-800-456-4828, ext. 2182
miltons@tinkerfcu.org

**Thurman Relerford**
Business Development Officer
(405) 319-2181
1-800-456-4828, ext. 2181
relerfordt@tinkerfcu.org

**Blake Roberts**
Community Engagement Representative
(405) 319-2077
1-800-456-4828, ext. 2077
robertsm@tinkerfcu.org

**Sarah Roberts**
Business Development Officer
(405) 319-2179
1-800-456-4828, ext. 2179
robertss@tinkerfcu.org

**Grace Silvers**
Community Engagement Representative
(405) 319-2174
1-800-456-4828, ext. 2174
silversg@tinkerfcu.org

**Samantha Strealy**
Business Development Officer
(405) 319-2184
1-800-456-4828, ext. 2184
strealys@tinkerfcu.org

**Kristy Viravong Portis**
AVP/Manager, Business & Community Engagement
(405) 319-2187
1-800-456-4828, ext. 2187
viravongk@tinkerfcu.org


TFCU
Tinker Federal Credit Union