S&T Bank strategy academy

Two-Factor Authentication Code Identification Scams: The New Trick Fraudsters Are Using

What is a fake 2FA identification scam?

Fake two-factor authentication (2FA) identification scams can trick people into handing over the security codes meant to protect their accounts. Scammers pretend to be from a bank, a phone company or another business you trust. They claim to need a code sent to your phone or email to help fix a problem or verify your identity. That code lets them break into your account without ever needing your password.

How the Scam Works

The scam starts when a fraudster enters your email or phone number on a website's login page and clicks "Forgot Password." This pushes a 2FA code to your phone or email. The scammer then reaches out, often pretending to be from your bank or a familiar company, asking for the code to confirm your identity or fix an account issue. Their goal is to make you believe the request is legitimate so that you share the code. Once they have it, they use it to access your account and often change the password so you can't get back in.

Example of This Scam

Ross receives a text that says his account needs verification, followed by a call from someone claiming to be on his bank's fraud team. They warn that suspicious activity was detected and ask Ross to read back the 2FA code just sent to his phone. He does, unknowingly handing over the keys to his account. Minutes later, the fraudster changes his password and locks Ross out.

Tips to Protect Yourself From the Fake 2FA Identification Scam:

- **Never share verification codes.** No legitimate organization will ask for a 2FA code sent to your device.
- **Be suspicious of urgent calls or texts.** Scammers often create a sense of urgency to pressure you into acting without thinking.
- **Initiate contact yourself.** If you're unsure whether a request is real, contact the company using a phone number or website you trust.
- **Use app-based 2FA when possible.** Authentication apps are generally more secure than text message codes, which can be intercepted or spoofed.
- **Monitor your accounts closely.** Turn on alerts to get immediately notified of logins or account changes.

If You Think You've Been Scammed

Follow these essential tips:

- **Contact us.** If you've provided financial information, report the fraud to us to potentially stop unauthorized transactions.
- **Report the scam to the proper authorities.** File a report with the Federal Trade Commission at ReportFraud.FTC.gov. Find your state's attorney general at NAAG.org and inform their office about the scam. Also, report the incident to local law enforcement.
- **Warn others.** Share what happened with friends and family to help others recognize and avoid this scam.

###