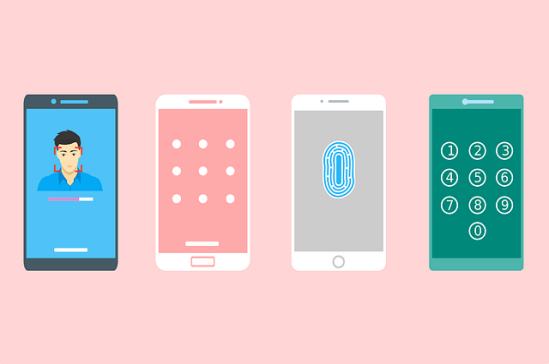
Forcht Bank
A new direction in banking.

#CyberTipTuesday

Two-Factor Authentication

Don't fall victim to cyber crime. Use this technique.



Passwords. They protect our most important information on our phones, computers, accounts, etc. Passwords are a treasure for cyber criminals, who leak login credentials from compromised websites.

Once cyber criminals have your login name and password, they can easily impersonate you online, access your bank accounts, sign online agreements, engage in financial transactions, or change account information.

This is where two-factor authentication comes in.

Two-factor authentication means requiring additional information beyond a password alone to access your online accounts. It's an extra layer of defense to help you avoid falling victim to cyber crime.

Two Steps for Two-Factor Authentication

Step 1: Make your password unique, long, and complicated.

Step 2: Pair that password with one of the following:

- Something you have - for example, a mobile device; you can prove you have the phone by reporting back the PIN code that was sent to it in a text message
- Something you are - a fingerprint or other biometric data.

Your password, plus one of the security methods described above, equal your two-factor authentication.

Source: www.cisecurity.org