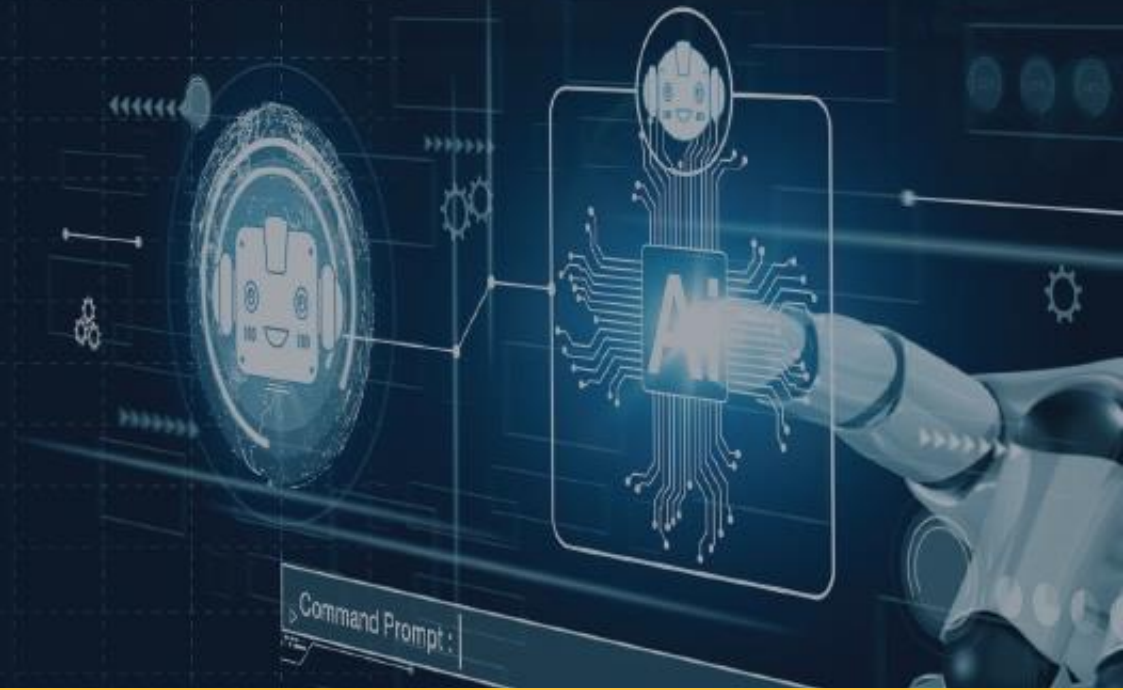


Fighting Fraud in the Age of AI Scams



first[®]

first financial bank

Presenters

■ Caroline Bove – Director Public Funds

- Worked exclusively with FP Entities for 8+ years at First Financial Bank
- Caroline.bove@bankatfirst.com / 513-415-9233 (cell)



■ Justin Laubach – VP, Public Funds

- Worked in the financial industry for 16 years
- Justin.Laubach@bankatfirst.com / 330-418-1877 (cell)



Agenda

- The State of Fraud
- Common Fraud Attacks
- How to Protect your County
 - Technology / Team / Training
- AI Scams
- How to protect your County from AI Scams



The State of Fraud

first[®]

first financial bank

Fraud: It's not "if," it's "when"

An average of 80% of organizations are victims of payments fraud attacks every year.¹

Fraud attacks and technology are always evolving. The 2024 Internet Crime Report² details losses exceeding \$16 billion — a 33% increase in losses from 2023.

Do you know what you're up against?

Common Fraud Attacks:

- Phishing
- Social engineering
- AI and deepfakes
- Payment fraud – Check & ACH



¹"2025 AFP Payments Fraud and Control Survey Report;" Association for Financial Professionals. <https://www.afponline.org/training-resources/resources/survey-research-economic-data/details/payments-fraud>.

²"2024 Internet Crime Report," Federal Bureau of Investigation. <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>

Common Fraud Attacks

Phishing

- An email or text that looks like it is from someone you know, asking you to click a link
 - 📌 The link may request that you provide confidential information such as account numbers or passwords
 - 📌 The link may also install **malware** (malicious software) without your knowledge which can record your sensitive information, and infect entire systems and networks



Beware of unsolicited communications that require clicking on unknown links, particularly those conveying urgency.

The image illustrates a phishing attack through an email and a subsequent website. The email, from 'firstfinancialbank.com@gmail.com', is addressed to 'John Doe' and includes '+ 34 Others' in the recipient list. The subject is 'First Financial Bank sent a message'. The body text contains a typo: 'There has been suspicious acitivty on your First Financial Bank deposit account.' A blue link is provided: 'Please click here to log in and verify this charge.' Below the email, a browser window shows a website with the URL 'change-address-post.com' and a page titled 'ADDRESS CHANGE WITH THE USPS(TM)'. The page features a 'Select Move Type' section with two buttons: 'Permanent Address Change' and 'Temporary Address Change'.

1. Others included on an email (when it includes specific account information).
2. Emails from unofficial email addresses.
3. Typos and grammar mistakes.
4. Emails requiring unsolicited link clicks.
5. Websites with incorrect domain names.
6. Poor quality images or web design.

Anatomy of a Phishing Email

Response required - Message (HTML)

File Message Tell me what you want to do

service@intl.paypal.com <service.epaypal@outlook.com>

Response required

1/29/2015

Actual sender not from company and not from displayed name

Trying to give a false sense of urgency

Often vaguely worded or with bad grammar and spelling

Hover over links to see actual URL

Response required.

Dear [redacted],

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

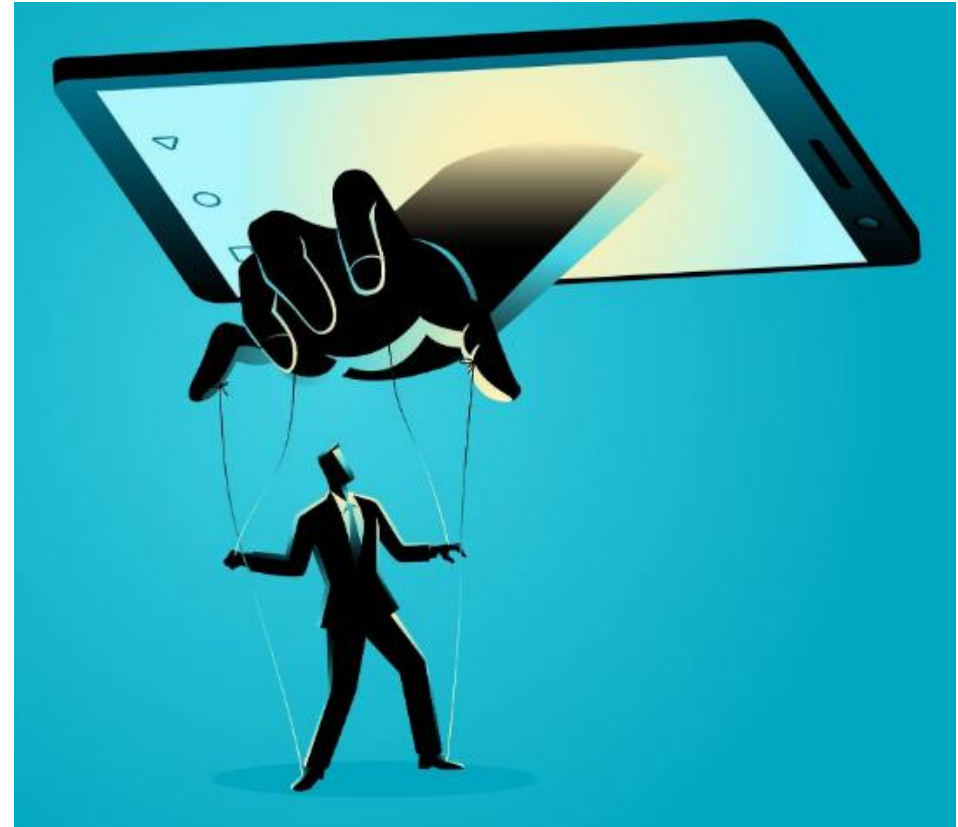
Common Fraud Attacks

■ Social engineering

- When scammers believably pose as someone you would trust to access personal information or account credentials
 - **Example:** Calling from a spoofed number that looks like your bank and pretending to be an associate, then asking for usernames, passwords, or verification codes.




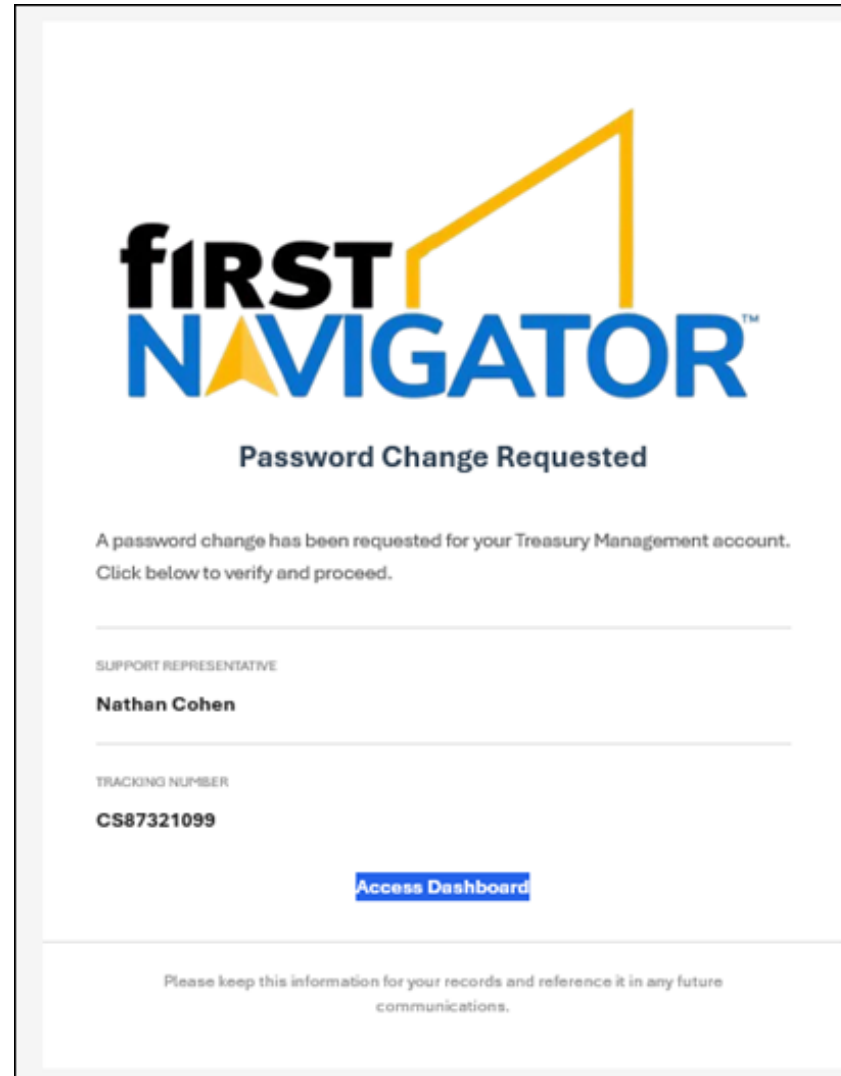
First Financial Bank will **NEVER**, under any circumstances, ask clients to provide full credit card numbers, login credentials, or verification codes.



Social Engineering Example



 First Financial Bank will **NEVER**, under any circumstances, ask clients to provide full credit card numbers, login credentials, or verification codes.



Common Fraud Attacks

AI & Deepfakes

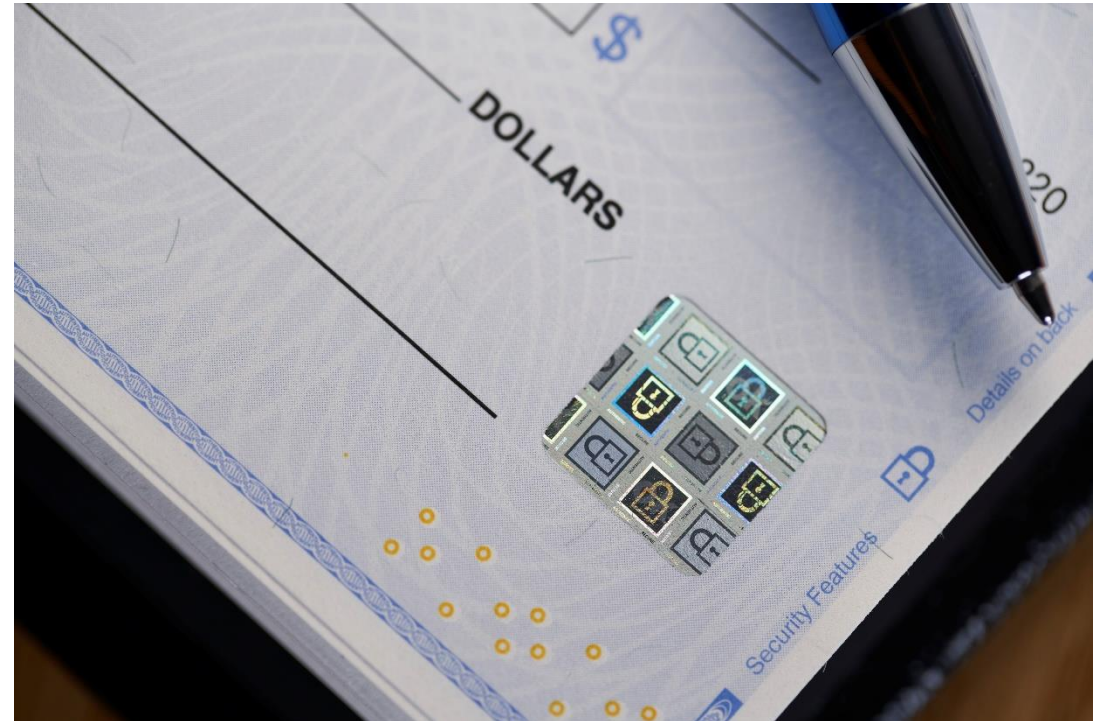
- Artificial intelligence tools are more advanced, easier to find, and often free. They allow criminals to deceive targets better than ever before. Watch out for:
 - Images, videos, and voice calls impersonating executives, managers, or clients you are working with.
 - AI-generated invoices, contracts, or fraud alerts that aim to capture sensitive info
 - Fake websites posing as institutions you have relationships with



Common Fraud Attacks

Payment Fraud

- 1 **Check washing** - stealing a check, erasing the ink, and either writing a higher value to a different recipient or duplicating and selling the blank checks.
- 1 **Counterfeit checks** - when someone gains access to your routing and account number and accesses your funds without your consent.
- 1 **Mail theft** - when criminals access account numbers or other personal information that can then grant them unauthorized access to accounts and funds.
- 1 **Deposit theft** - when criminals take a legitimate check and deposits it into a bogus business.



Common Fraud Attacks

▀ Payment Fraud

- ▀ ACH Fraud – 24 hour rule!



Protect Yourself

- Protect your login credentials
- **DO NOT** comply with requests for sensitive information through unsolicited phone calls, emails, social media messages, or text messages
- Be suspicious of unsolicited and overly urgent requests
- Do not use email to send or receive payment instruction
- Establish secret phrases to confirm the identity of the person and the validity of their request
- Adopt dual controls so that no one individual can perform a request for scammers
- Validate all requests for payment or passwords with the person who made the request by contacting them directly using information you already have on file



Whenever in doubt, contact your trusted financial contact directly using a known or official phone number.

Protect Yourself

The best defense against fraud is preparedness. Are your current processes and procedures enough to protect your business?

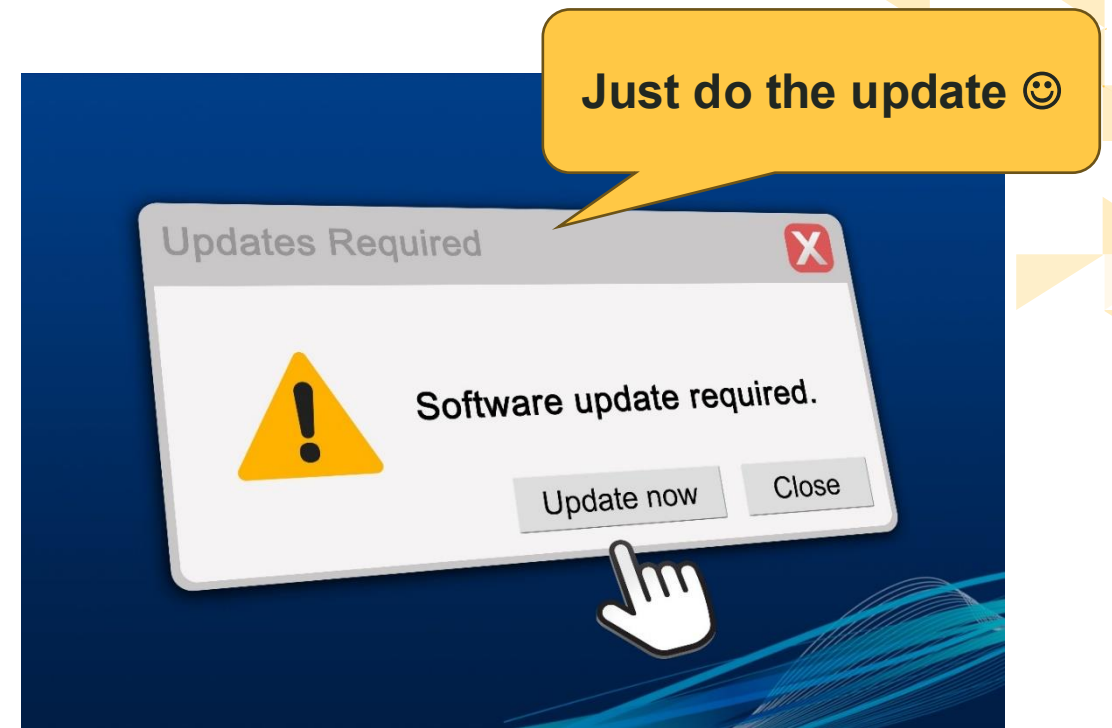
Key Elements:

- Technology
- Teams
- Training



Technology

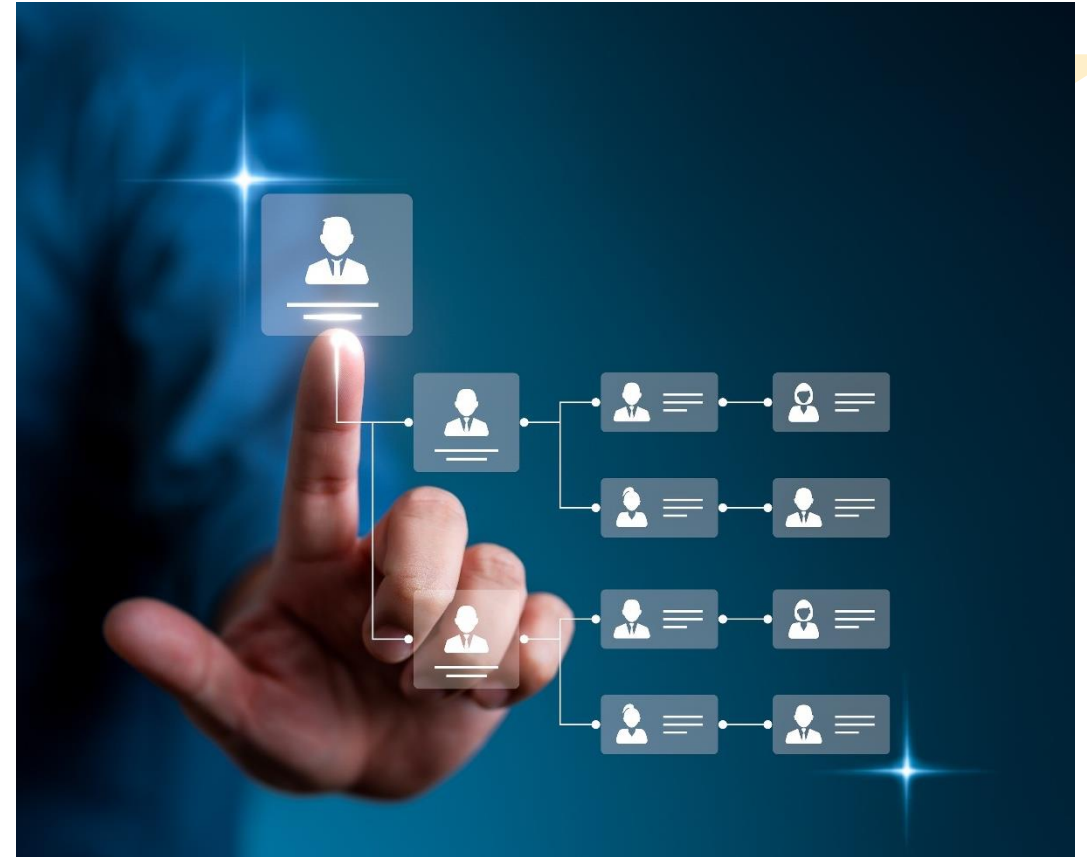
- **Update** antivirus software, firewalls, and browsers, and disable unnecessary plugins or cloud access.
- Implement **two-factor authentication** on any systems and programs possible.
- Implement or reinforce **dual control** on company payments.
- Move away from paper checks and use **electronic payments** and other fraud protection services
 - i.e. ACH positive pay AND Payee Check Positive Pay



Why does it matter? Common scams involve gaining access to an email account and sending fraudulent payment requests to trusted contacts, who don't realize that the sender's account has been compromised. Requiring two sets of credentials makes it much more difficult for fraud actors to take advantage of your payment process because more people will have to consider the likelihood that the fraudulent request is valid.

Team

- Conduct an **annual review** of accounts, access, and systems.
- Clearly **define roles** and responsibilities.
- Create or identify roles **dedicated to fraud prevention.**
- Consult with a **third-party risk management company** to identify potential vulnerabilities in your systems.



Training

Your employees are your greatest vulnerability, and your greatest tool. Training and education should be a regular part of your operations, and remember the 4 C's:

Consistent

- Annual trainings to keep information fresh and share new trends

Compulsory

- Mandatory and part of an employee's annual performance review

Customized

- Different jobs have different risks

Chronicled

- Documenting preventative efforts can help insurance claims



Learn more about how to fight fraud
at bankatfirst.com/fraud-awareness

first[®] first financial bank

EQUAL
OPPORTUNITY
LENDER

 EQUAL
HOUSING
LENDER

FDIC

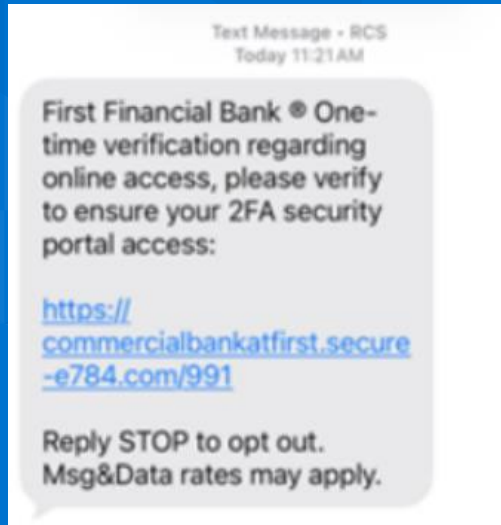
Sample AI Scams



first[®]
first financial bank

Sample AI Scams

- Texts from “your bank”



- Calls from “your bank”
 - Fraud department
 - ACH / Wire department



first[®]

first financial bank

Protect your County from AI Scams

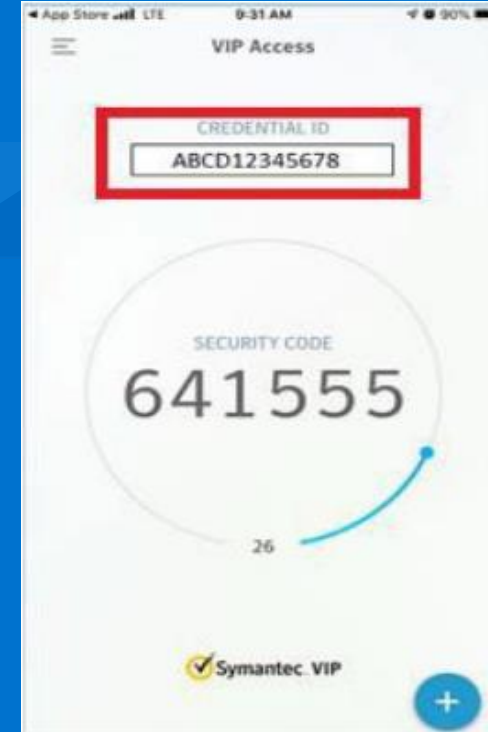
NEVER give out:

- Your login information
- Your security token code



NEVER click on:

- Links asking you to sign in to your online banking / change passwords



first[®]

first financial bank

Protect your County from AI Scams

▮ If suspicious, ALWAYS:

▮ PAUSE!

▮ Hang up

▮ Contact your bank / bank rep / vendor at KNOWN number

first[®]

first financial bank



first[®]
first financial bank

- ✦ Caroline.bove@bankatfirst.com / 513-415-9233 (cell)
- ✦ Justin.Laubach@bankatfirst.com / 330-418-1877 (cell)