Customer Education List

What to know

Online Banking Security

- use strong, unique passwords and update them often
- enable multi-factor authentication for extra protection
- access accounts only through the official website or app
- avoid logging on or making transactions using public Wi-Fi
- log out completely after each session

Identity Theft

- monitor accounts and credit reports regularly
- shred or properly discard personal documents
- keep personal info private, especially online
- report suspicious activity right away
- limit what you share in public or on social media

Lost or Stolen Cards

- lock your card in the app or contact us to report the loss
- review transactions for unauthorized charges
- request a replacement card quickly
- set up transaction alerts
- keep card numbers and PINs confidential

Scam & Fraud Awareness

- be cautious of unexpected calls asking for personal information
- banks will never ask for PINS or codes by phone
- hang up and call your bank directly if unsure
- watch for urgency or threats, these are common scam tactics
- stay informed about new scam trends

Online Shopping Safety

- Only shop on secure websites (look for “http://”
- Avoid public Wi-Fi when checking out
- Turn on transaction alerts to get notified the moment your card is used
- Watch for prices that seem too good to be true
- Always track your orders directly through the retailer’s website

Text Message Scams

- We will never text asking for PIN, password, or full account info.
- Avoid clicking links in texts you were not expecting.
- Don’t share one-time codes with anyone.
- Fraudsters often impersonate trusted businesses or numbers.
- When in doubt, delete the message and call us directly!

Phone Call Scams

- Don’t give personal info to unsolicited callers.
- We will never call asking for your online banking login or PIN.
- Hang up and call the official bank number directly if unsure.
- Scammers often create fake “urgent” situations to pressure you.
- Always verify before you trust - even if the caller ID looks local

What to do if you suspect fraud

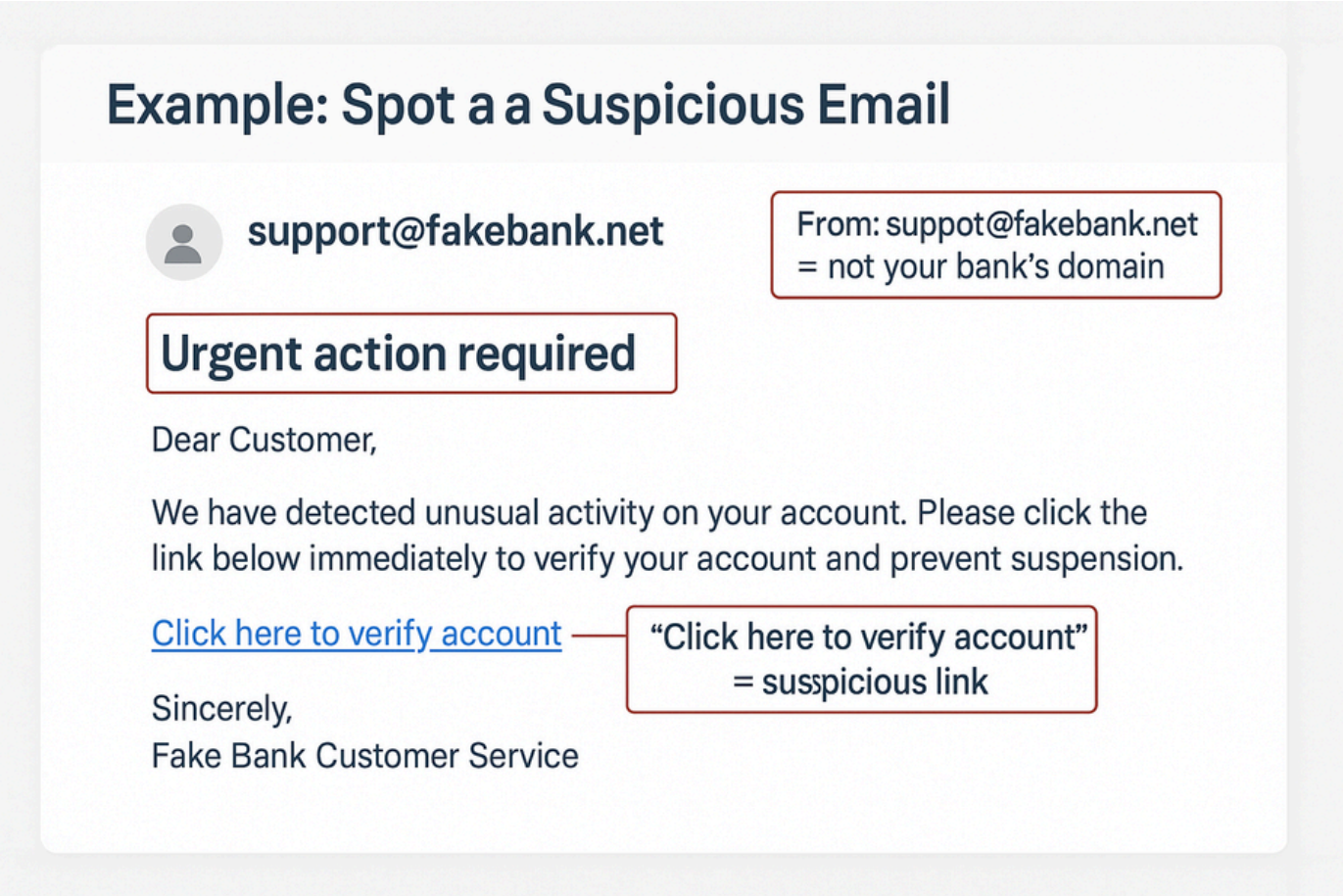
- Contact the bank immediately @ (615)446-2822.
- Visit your local branch.
- If you have online banking lock your card in the app.

Steps to lock your card

1. On the homepage scroll down to Card Management.
2. Click the associated card number.
3. In the top right-hand corner click the on and off switch. 
4. Select “YES” to confirm.

Transactions will be denied, but recurring payments may continue. Any credits or deposits to the cards associated account will be allowed.

Spot a Suspicious Email



Spotting Scam Emails

- "Urgent action required" is a scare tactic.
- "Click here to verify account" typically a suspicious link.
- Your name is spelt incorrectly.
- Any grammar errors.

Example

- From: support@fakebank.net (or anything that is not your banks domain).