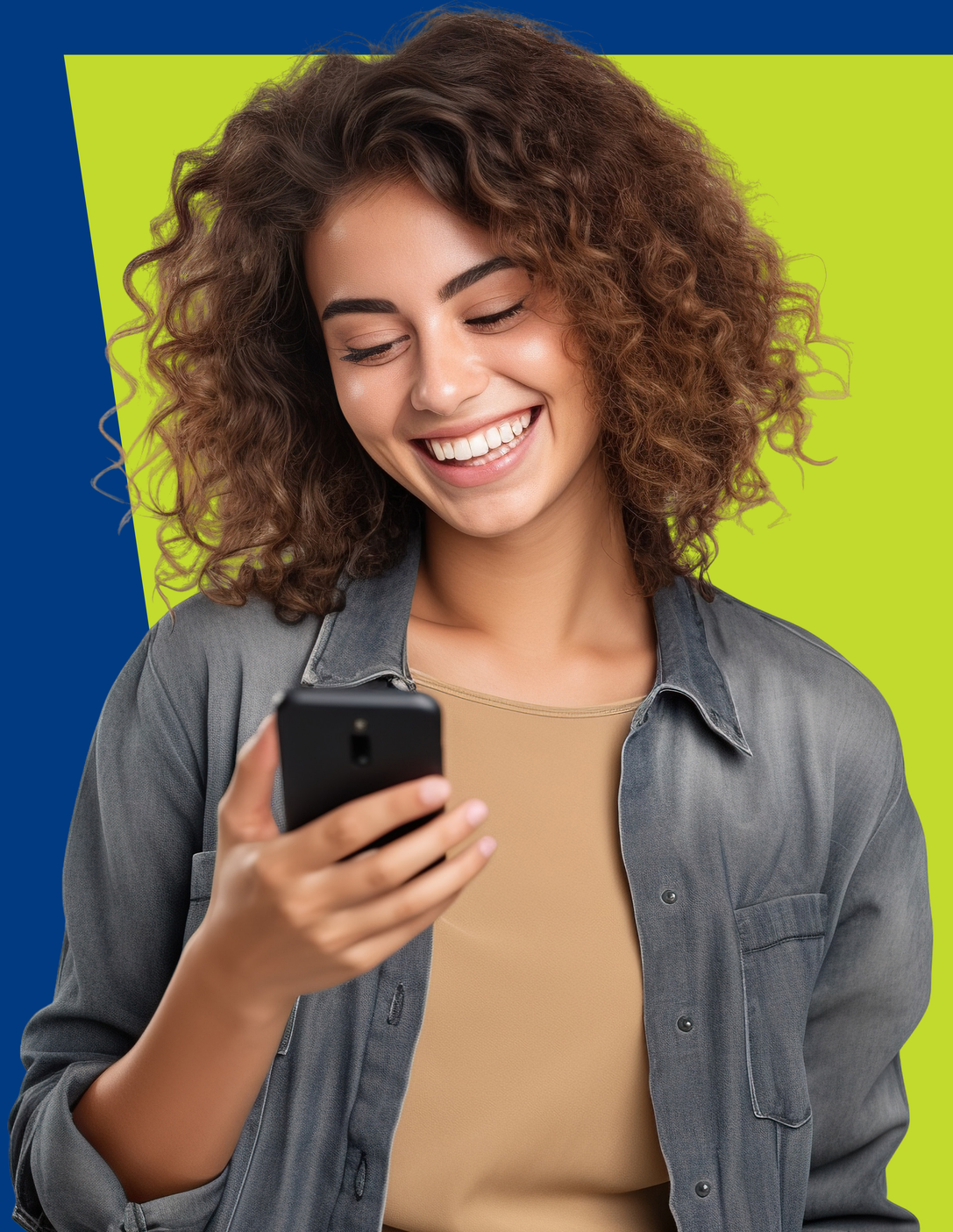
SIKORSKY CREDIT UNION

everyone banks better here

PROTECT YOUR MONEY, STAY SAFE: A GUIDE TO AVOIDING PHISHING SCAMS

As technology evolves, so do the tactics of cyber criminals. Phishing scams target individuals by masquerading as trustworthy entities to trick you into giving away personal information. As your credit union, we're dedicated to helping you safeguard your hard-earned money and personal data.

Let's explore the types of phishing scams, offer practical advice on how to avoid them, and outline steps to take if you fall victim to these malicious schemes.



TYPES OF PHISHING SCAMS

SIKORSKY CREDIT UNION
everyone banks better here

Email Phishing Scams

Scammers send emails that appear legitimate, often impersonating trusted institutions or popular companies like banks or online stores. They may include a sense of urgency to prompt immediate action, like clicking a suspicious link or downloading a harmful attachment.

Text/SMS Phishing Scams

Sometimes referred to as “smishing” (short for SMS phishing), this scam uses text messages to deliver malicious links, often under the guise of confirming an account or payment details.

Phone Phishing Scams

Phone/voice phishing involves scammers calling to impersonate institutions such as government agencies or financial institutions. They typically have a script that makes them sound legitimate but manipulates victims into revealing personal or financial information over the phone.

Payment App Phishing Scams

A payment app phishing scam involves fraudulent attempts to trick users of mobile payment apps like Venmo, Zelle, CashApp, and PayPal into giving away sensitive information like login credentials, bank account details, or to send them money.

ADVICE TO AVOID PHISHING SCAMS

SIKORSKY CREDIT UNION
everyone banks better here

Email Phishing Scams

DON'T CLICK THOSE LINKS
Avoid clicking links in emails that urge actions like verifying credentials or making payments; banks don't request this.

CHECK THE SENDER'S ADDRESS
Review the sender's email address for slight misspellings or discrepancies. Official organizations use domain addresses (e.g., @sikorskycu.org) rather than generic ones like Gmail or Yahoo.

EXAMINE THE MESSAGE
Look for grammatical errors, odd language, uncharacteristic tone, and attachments. Phishing emails often contain subtle yet telltale signs that reveal their fraudulent nature.

HOVER OVER LINKS
Before clicking, hover over links to reveal their true URL destination. If the address doesn't match the stated destination, don't click!

CALL DIRECTLY
When in doubt, call your financial institution directly at the number on the back of your debit card or on their website.

Text/SMS Phishing Scams

DON'T CLICK THOSE LINKS
Avoid clicking links or downloading attachments sent via SMS, especially from unknown sources.

VERIFY THE SOURCE
Call the customer service number of the entity allegedly sending the message to verify the request.

BLOCK AND REPORT
Block unknown numbers and report potential scam messages to your mobile carrier.

BE SKEPTICAL OF URGENCY
Text/SMS phishing messages often convey urgency ("act now!"). Be cautious of such requests.

NEVER SEND PERSONAL INFORMATION
When in doubt, call Your bank will never ask for your password, PIN number, or login code in a text message. If you receive a text message asking for personal information, it's a scam.

ADVICE TO AVOID PHISHING SCAMS

SIKORSKY CREDIT UNION
everyone banks better here

Phone Phishing Scams

HANG UP AND VERIFY
If the caller pressures you for sensitive information, hang up and call the official customer service number directly to verify their legitimacy.

GUARD PERSONAL INFORMATION
Never share personal data over the phone unless you've initiated the call.

REGISTER FOR THE DO NOT CALL LIST
Limit calls from telemarketers and unsolicited numbers by registering with the "Do Not Call" registry at DoNotCall.gov.

BEWARE OF CALLER ID SPOOFING
Scammers can manipulate caller ID to show trusted names. Always verify suspicious calls by other means.

Payment App Phishing Scams

BE A SKEPTIC
Scammers will often pretend to be a family member or friend who's in trouble and needs money for an emergency. Others might say you won a prize or a sweepstakes but need to pay some fees to collect it.

WATCH OUT FOR "ACCIDENTAL" PAYMENTS
If you unexpectedly receive a payment from someone you don't know and then are contacted to send it back, you should proceed with caution. They may have made a payment with a stolen credit card or reported it to the bank in order to "double dip" on the reimbursement.

VERIFY ANYONE YOU SEND MONEY TO
Double check the profile of who you are sending money to. Ensure their username is correct and confirm with them what their profile pic is before you send money.

SIKORSKY CREDIT UNION
everyone banks better here

WHAT TO DO IF YOU'VE FALLEN FOR A PHISHING SCAM

1 ACT FAST

Immediately change passwords for any compromised accounts. If it's an email account, also update other online accounts that use the same email.

2 CONTACT FINANCIAL INSTITUTIONS

Inform your bank or credit union and any credit card companies if your financial date has been compromised. They can help monitor transactions, secure accounts, and issue new cards it needed.

3 REPORT THE INCIDENT

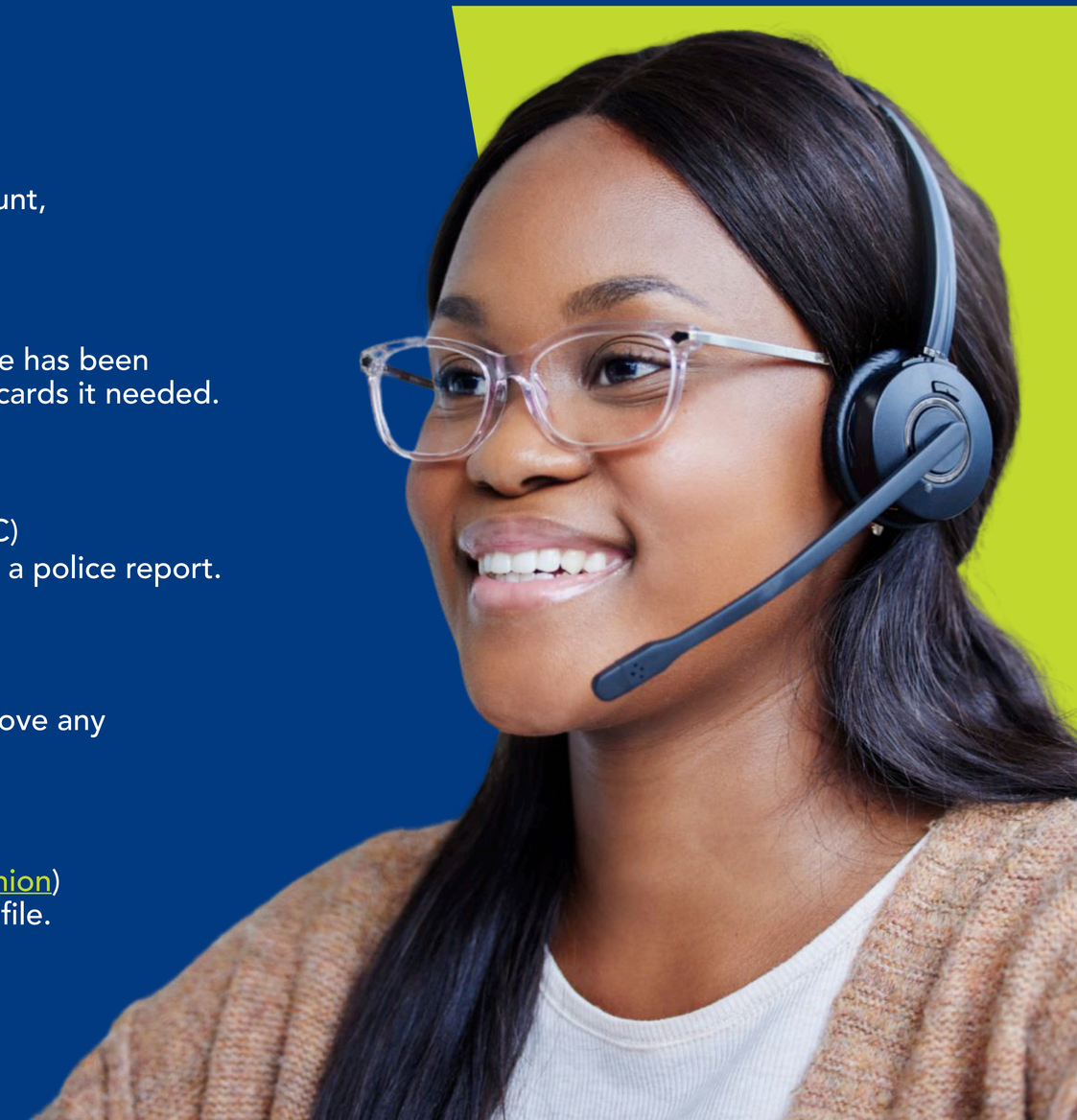
Report the scam to relevant authorities, such as the Federal Trade Commission (FTC) at ReportFraud.ftc.gov or call 1-877-FTC-HELP (382-4357). If you've lost money, file a police report. You can also go to IdentityTheft.gov for guidance on additional steps to take.

4 RUN A SECURITY SCAN

Use antivirus and antimalware software to run a complete scan of your device. Remove any detected threats and update your security software.

5 MONITOR CREDIT REPORTS

Request your credit reports from the major bureaus (Experian, Equifax, and TransUnion) to detect fraudulent activity. Consider placing a fraud alert or credit freeze on your file.



SIKORSKY
CREDIT UNION
everyone banks better here

FINAL THOUGHTS

Phishing scams are increasingly sophisticated, but with a mix of vigilance, education, and proactive measures, you can significantly reduce your risk of falling victim. Our credit union is here to assist with the information and resources you need to protect your finances. Stay informed, stay safe, and always verify before you trust!

For More Information Visit Us at SikorskyCU.org