Fraud Awareness and Prevention
Social Media Communications

CROSS FINANCIAL

Fraud Awareness and Prevention Social Media Communications

The topic of fraud is being discussed in virtually every community bank in the United States.The following pages include a number of content ideas that could be used to support your customer education communications related to fraud awareness and prevention. The prominent focus is social media messaging, however, many of the ideas could easily be adapted for use with customer emails, handout materials, and newsletter articles.

We hope the ideas provide a catalyst for your fraud prevention communications and customer education activities.

CROSS FINANCIAL

Lincoln, Nebraska
crossfinancial.com
402.441.3131

Fraud Awareness and Prevention

12 Week Social Media Campaign

Here is an outline for a 12-week social media campaign for community banks. The weekly messages focus on awareness, recognition, response, and prevention. Each post includes:

- Headline
- Short copy
- Simple tip
- Suggested visual

Campaign Theme Options

Fraud Awareness: Protecting Your Money and Identity
Fraud Prevention Fridays
Stay Safe Online Series

Post 1

Fraud Is More Common Than You Think

Headline

Fraud Is On the Rise. Stay Alert.

Post Copy

Financial scams are becoming more sophisticated every year. Criminals target everyday consumers through text messages, emails, phone calls, and social media. The good news? Awareness is one of the best defenses.

At [bank name], protecting your money and personal information is a top priority and that starts with helping you recognize the warning signs of fraud.

Tip

If something feels urgent, unusual, or too good to be true…pause before you respond.

Fraud Awareness and Prevention

Visual Idea
Graphic with text: Fraud Prevention Tip #1: Awareness Is Your First Line of Defense

Post 2
The Most Common Consumer Scams

Headline
The 4 Most Common Consumer Scams Today

Post Copy
Fraudsters often rely on the same types of scams. These scams are designed to trick you into sharing personal or banking information. The most common include:

- Phishing emails
- Fake text alerts about your bank account
- Phone calls pretending to be your bank
- Online marketplace or payment scams

Tip
Never provide passwords, PINs, or verification codes to anyone who contacts you unexpectedly.

Visual Idea
Simple infographic listing the four scam types.

Post 3
What Is Phishing?

Headline
What Is Phishing?

Post Copy
Phishing scams use emails or texts that look like they come from legitimate companies, including banks. These messages often include links asking you to:

- Verify account information
- Reset passwords
- Confirm transactions

Fraud Awareness and Prevention

Clicking the link can lead to a fake website designed to steal your information.

Tip
Always go directly to our bank's website or mobile app rather than clicking links in messages.

Visual Idea
Graphic comparing "Real Bank Message vs Phishing Message"

Post 4
Watch Out for Fake Urgency

Headline
Fraudsters Use Urgency to Pressure You

Post Copy
Fraudsters want you to panic and act quickly without thinking. Many scams create a false sense of urgency:

- Your account will be locked!
- Suspicious activity detected!
- Act now to prevent fraud!

Tip
Pause and verify before responding to urgent messages. When in doubt, contact us at [phone number] or use the telephone number listed on our website.

Visual Idea
Graphic showing warning words: URGENT, ACT NOW, VERIFY IMMEDIATELY

Post 5
Red Flags of Fraud

Headline
5 Warning Signs of a Scam

Fraud Awareness and Prevention

Post Copy
Watch for these common red flags:

- Requests for passwords or personal identification numbers
- Unexpected verification codes
- Requests for gift cards or wire transfers
- Poor grammar or unusual links
- Messages asking you to confirm personal information

Tip
Banks will never ask for your full password or PIN.

Visual Idea
Checklist style graphic.

Post 6
Text Message Scams (Smishing)

Headline
Don’t Fall for Smishing Scams

Post Copy
“Smishing” is phishing by text message. These texts often include links to fake websites. Examples include messages saying:

- Your debit card has been locked.
- Click here to verify a transaction.

Tip
Never click suspicious links in text messages. Instead, log in using our online banking or mobile banking app.

Visual Idea
Phone screenshot graphic with suspicious message.

Fraud Awareness and Prevention

Post 7
Phone Call Scams

Headline
Fraudsters Can Fake Caller ID

Post Copy
Some scammers pretend to be your bank by spoofing our telephone number. They may say they need to:

- Verify account information
- Confirm a transaction
- Reset your login credentials

Tip
Hang up and call us directly at [telephone number] or using the number on our bank website.

Visual Idea
Graphic: Caller ID Can Be Faked

Post 8
Protect Your Personal Information

Headline
Your Personal Information Is Valuable

Post Copy
Protecting your information is critical to preventing identity theft. Fraudsters use stolen information like:

- Social Security numbers
- Account numbers
- Birthdates
- Online banking credentials

Fraud Awareness and Prevention

Tip
Never share personal or banking information through email, text, or social media.

Visual Idea
Lock icon protecting personal information.

Post 9
What To Do If You Suspect Fraud

Headline
Think You've Been Targeted by a Scam?

Post Copy
We can help monitor your account and take steps to protect your money. If you believe a scammer contacted you:

1. Stop communication immediately
2. Do not click links or send information
3. Contact us at [telephone number] right away

Tip
If you suspect fraud, contact us at [telephone number], or using the telephone number on your debit card or our official website. Do not use the telephone number in the suspicious message.

Visual Idea
3 Steps to Take If You Suspect Fraud

Post 10
What To Do If Fraud Happens

Headline
Act Fast If Fraud Occurs

Fraud Awareness and Prevention

Post Copy
The sooner fraud is reported, the faster steps can be taken to limit potential losses. If you notice suspicious transactions:

1. Contact us immediately
2. Change online banking passwords
3. Monitor your account activity

Tip
Regularly review your account activity through online banking.

Visual Idea
Checklist style graphic.

Post 11
Simple Ways to Protect Yourself

Headline
5 Simple Fraud Prevention Habits

Post Copy
Small steps can make a big difference in protecting your finances. Protect yourself with these smart habits:

1. Use strong passwords
2. Enable account alerts
3. Monitor account activity
4. Avoid public Wi-Fi for banking
5. Keep your devices updated

Tip
Set up transaction alerts through our online banking or mobile app so you are notified anytime money moves in or out of your account.

Visual Idea
Five shield icons representing the tips.

Fraud Awareness and Prevention

Post 12

We Are Here to Help

Headline
[Bank name] Is Your Partner in Fraud Prevention

Post Copy
Protecting your accounts is a partnership. We actively monitor for suspicious activity and provide tools to help keep your accounts safe. If something doesn't look right, contact us right away at [customer service number]. We're here to help.

Tip
Save our customer service telephone numbers in your phone so you can quickly reach us if needed.

Visual Idea
Friendly community bank image with headline:
We're Here to Help Protect Your Money

(fraud prevention handout #1)

Protect Yourself From Fraud

Simple Steps to Safeguard Your Money and Personal Information

Financial scams and identity theft are increasing across the country. Criminals often target consumers through emails, text messages, phone calls, and online marketplaces.

The good news is that many scams can be avoided by knowing what to watch for and taking a few simple precautions. We are committed to helping you recognize fraud and protect your financial accounts.

Fraud Awareness and Prevention

Common Types of Fraud

Consumers today most frequently encounter scams such as:

Phishing Emails

Fraudulent emails that appear to come from legitimate companies asking you to click links or verify account information.

Text Message Scams (Smishing)

Messages claiming there is a problem with your account or asking you to click a link to verify a transaction.

Phone Call Scams

Fraudsters may impersonate banks, government agencies, or businesses and ask for personal information.

Online Marketplace and Payment App Scams

Criminals may use online marketplaces or payment apps to trick consumers into sending money for items that never arrive.

Warning Signs of a Scam

Be cautious if you receive messages that:

- Create a sense of urgency or panic
- Ask for passwords, PINs, or verification codes
- Request payment using gift cards, wire transfers, or payment apps
- Contain suspicious links or unusual email addresses
- Ask you to confirm personal or financial information

Remember: We will never ask for your password, PIN, or full security codes.

Fraud Awareness and Prevention

Smart Habits That Help Prevent Fraud

Protect yourself with these simple steps:

- Regularly review your bank and credit card transactions
- Use strong, unique passwords for online accounts
- Enable account alerts and online banking notifications
- Avoid conducting financial transactions on public Wi-Fi
- Keep your phone, computer, and apps updated
- Shred documents containing personal information

What To Do If You Suspect Fraud

If something doesn't seem right, act quickly. Quick action can help prevent or minimize potential losses.

1. Stop communication with the suspected scammer
2. Do not click links or provide information
3. Contact us immediately at [telephone number]
4. Monitor your accounts for suspicious activity
5. Change online banking passwords if needed

We Are Here to Help

We actively monitor accounts and provide tools to help keep your finances secure. If you ever receive a suspicious message or notice unusual account activity, please contact us right away.

[Bank Name]
[Customer service or fraud hotline numbers]
[Website address]
[List of branch locations and telephone numbers]

When in doubt, pause and verify before responding to any unexpected request involving your financial information. We are proud to be a partner in protecting your financial security.

Fraud Awareness and Prevention

(fraud prevention handout #2)

Simple Fraud Prevention Tips for Bank Customers

Account Security

- Use strong passwords that include a mix of letters, numbers, and symbols.
- Use different passwords for your banking, email, and financial accounts.
- Enable two-factor authentication whenever it is available.
- Change your passwords periodically, especially if you suspect a security issue.
- Avoid saving banking passwords on shared or public computers.

Monitoring and Alerts

- Review your bank and credit card transactions regularly.
- Enable account alerts for large transactions or suspicious activity.
- Check your account activity through your bank's mobile app.
- Review your monthly bank statements carefully.
- Report any unauthorized transactions immediately.

Protecting Personal Information

- Never share your PIN, passwords, or security codes.
- Shred documents that contain personal or financial information.
- Do not send personal information through email or text messages.
- Be cautious about what personal information you share on social media.
- Store important financial documents in a secure location.

Avoiding Online and Phone Scams

- Do not click suspicious links in emails or text messages.
- Be cautious of messages that create urgency or pressure you to act quickly.
- Never send money to someone you have not met in person.
- Hang up on suspicious callers claiming to represent your bank.
- Always verify requests for money or personal information.

Fraud Awareness and Prevention

Safe Technology Habits

- Avoid logging into banking apps on public Wi-Fi networks.
- Keep your phone, computer, and apps updated.
- Install security updates as soon as they become available.
- Use a passcode or biometric lock on your phone.
- Log out of financial accounts when using shared devices.

(fraud prevention handout #3)
This handout can also be used for short reminders and customer email content.

50 Fraud Prevention Tips for Bank Customers

Simple Ways to Protect Your Money and Personal Information

Financial scams and identity theft are becoming more common. These simple habits can help protect your accounts, your identity, and your finances.

1. Use strong passwords with letters, numbers, and symbols.
2. Avoid using the same password for multiple accounts.
3. Change passwords periodically.
4. Never share your password with anyone.
5. Do not store passwords where others can easily find them.
6. Avoid saving banking passwords on shared computers.
7. Use a password manager to store passwords securely.
8. Never send passwords through email or text messages.
9. Log out of accounts when using shared devices.
10. Enable two-factor authentication whenever available.
11. Check your bank account activity regularly.
12. Review monthly bank statements carefully.
13. Set up transaction alerts for withdrawals and purchases.
14. Monitor your credit card activity frequently.
15. Contact your bank immediately if you notice unusual activity.
16. Review your credit report annually.
17. Watch for small “test transactions” you don’t recognize.

Fraud Awareness and Prevention

18. Use your bank's mobile app to monitor transactions.
19. Verify transactions before approving alerts or confirmations.
20. Report lost or stolen debit cards immediately.
21. Be cautious of messages creating urgency.
22. Be suspicious of offers that seem too good to be true.
23. Do not trust unexpected requests for personal information.
24. Be wary of messages asking you to "verify" account details.
25. Fraudsters may impersonate banks, government agencies, or businesses.
26. Caller ID numbers can be spoofed.
27. Emails and texts can look official but still be fake.
28. Scammers may pressure you to act quickly.
29. Fraudsters often ask for gift cards or wire transfers.
30. Always verify requests before sending money.
31. Avoid accessing banking websites on public Wi-Fi.
32. Use secure home networks when conducting financial transactions.
33. Keep your phone, computer, and apps updated.
34. Install software updates promptly.
35. Use antivirus and security software on your devices.
36. Do not click suspicious links in emails or texts.
37. Only download apps from trusted app stores.
38. Lock your phone with a passcode or biometric login.
39. Log out of financial apps when using shared devices.
40. Avoid conducting financial transactions on public computers.
41. Shred documents containing personal information.
42. Keep Social Security numbers and account numbers secure.
43. Limit the personal information you share on social media.
44. Store important financial documents in a secure location.
45. Do not carry unnecessary personal documents in your wallet.
46. Be cautious when sharing personal details online.
47. Stop communicating with the suspected scammer.
48. Do not click links or provide additional information.
49. Contact your bank immediately if something seems suspicious.
50. Monitor your accounts closely for unusual activity.

CROSS
FINANCIAL

Lincoln, Nebraska
crossfinancial.com
402.441.3131