COVID-19 Fraud Deterrent Messages

Create awareness and educate your members to fight fraud proactively by using the following COVID-19 fraud deterrent tips. Copy and paste this content and customize the messaging in your credit union's tone for use in your various communication channels.

B2C Messaging for Websites/Newsletters/Emails

Scammers are using the COVID-19 pandemic to steal your money and personal information. Educating yourself and following these steps will help protect you from falling prey to their schemes.

Phishing Scams

- You may receive phishing emails impersonating the World Health Organization (WHO), the Centers for Disease Control and Prevention (CDC) and other reputable sources, which likely contain links or attachments that are designed to infect your computer with malicious malware and breach your privacy if you click on them. To defend against these email threats:

    1. Exercise caution with emails from unfamiliar sources and avoid opening anything unsolicited, unless you are sure it is a genuine email from a trusted source.
    2. Do not reply to or forward the email, or click on any links or attachments in the email. Most importantly, do not send out any sensitive information like your credit union credentials, account numbers or passwords.
    3. Delete any suspicious emails you receive.
    4. For accurate information, go straight to the source, such as the WHO and CDC websites.
    5. If you receive an email from <your credit union> that appears to be unusual, call <xxx-xxx-xxxx> to speak with card support to confirm its validity.

    If you've accidentally clicked on a phishing link, visit the cybercrime recovery page at FraudSupport.org.

    If you've accidentally given out sensitive information, like your credit union credentials, account numbers or passwords, call <xxx-xxx-xxxx> to speak with card support to take the necessary steps to prevent any fraud on your account(s).

Charity Scams

- You may receive emails or phone calls from charities that you don't recognize asking for donations related to COVID-19. To defend against charity scam threats:

    1. Verify all charities on the IRS tax exemption site.
    2. Never wire money or send gift cards or checks to strangers, foreign banks or any charity that is not legitimate.

If you've accidentally donated to a fraudulent charity, call <xxx-xxx-xxxx> to speak with card support to take the necessary steps to prevent any fraud on your account(s).

Also, visit the Charity Imposter page at FraudSupport.org for steps to report the fraudulent charity.

Government Relief Check Scams

- Scammers will use email, text and social media to send messages about the COVID-19 economic impact to entice you to click links for government relief checks. The links will take you to a fake website that looks legitimate and will ask you to enter personal information like your social security number, address and account numbers, to steal your money. Additionally, these fake sites also can download malware to your device and use your information for identity theft. To prevent these aforementioned losses, here's what you can do:

    1. Do not reply to suspicious emails, texts or social media messages. Also, don't forward or click on any suspicious links or attachments.
    2. Do not give out sensitive information like your credit union credentials, account numbers or passwords.
    3. Delete any suspicious- texts, emails or social media messages you receive.

Social Media Scams

- False information may increase on various social media platforms. To ensure you are getting accurate information about the COVID-19 crisis, only visit trusted social media profiles for the CDC, WHO, the Federal Trade Commission (FTC) and the Better Business Bureau (BBB).
- Don't assume an offer in a social media message is from a real friend. It's easier for scammers to impersonate real people on social media. Call your friend to verify they contacted you.

Loan Forgiveness Scams

- You may receive phony documents, emails and social media posts advertising loan forgiveness programs in the wake of COVID-19. For legitimate information on state-sponsored or government-sponsored loan forgiveness programs related to COVID-19, visit your state or county government websites.

Pension Scams/Fraud

- If you are retired, or are a caregiver for someone who is, beware of receiving calls or emails from someone impersonating the company that holds you or the individual's pension. They will ask for personal information and use it fraudulently. Do not give out any sensitive information like your credit union credentials, account numbers or passwords. Contact the company that holds the pension directly to verify and report any scams.

In summary, here are some quick tips to stay safe from scams surrounding COVID-19:

- If an offer or opportunity seems too good to be true, it's probably a scam.
- Never wire money, send gift cards or checks to strangers.
- If someone claims to be from a federal agency, call the office directly to confirm.

- Never accept any unsolicited money from strangers.
- If you suspect your credit union accounts have been hacked, change your passwords immediately and contact your credit union's card services department for further action to protect your accounts.