National Cooperative Bank

Customer Education & Security Awareness Notice

Help Prevent Fraud and Identity Theft

Introduction

Protecting privacy, security and personal information is the cornerstone on which National Cooperative Bank, N.A. ("NCB") and your relationship is built. While NCB employs numerous systems and safeguards to protect your information, we need your help to make your accounts and transactions as safe and secure as possible. Listed below are good security practices that you can follow to protect your accounts and personal information while conducting business with us. With your help and NCB's safeguards you can feel confident that your information is being protected.

Most Common Identity Theft Fraud Methods

Social Engineering - is a technique used to obtain or attempt to obtain secure information by tricking an individual into revealing sensitive information. Social engineering is, unfortunately, often successful because most targets (or victims) want to trust people and provide as much help as possible. The basic goal of social engineering is to gain unauthorized access to systems or information to commit fraud, identity theft, or simply to disrupt and compromise computer systems.

What you should do

- ✓ NEVER share your username or password with anyone.
- ✓ NCB will NEVER call you and ask for your username or password.
- ✓ Report spam/fraud relating to your NCB accounts to **security@ncb.coop** or by calling 1-800-322-1251**.**
- ✓ ALWAYS be aware of your surroundings.

Email Scams - Protect yourself from Internet and email scams by keeping your private information secure. It is not a safe practice to send or request confidential account information through email because it is not a secure form of communication. **You should never enter private, personal information in a form that was sent to you by email.** Here are a few ways you can protect yourself from Internet and email fraud (phishing):

- ✓ Never click on links in unexpected emails that request confidential information. If updates to information are needed, always type the address for the institution's website into your browser.
- ✓ Before submitting confidential information through forms, ensure you are using a secure Internet connection. There are two ways of determining if your connection to a website is secure. First, look at the address bar at the top of your browser. If the website address begins with "https://", then you have established a secure connection, but if it begins with "http://", then the connection is NOT secure. Second, look for a "lock" icon in your browser's status bar at the bottom right-hand corner of your browser. The lock verifies that your connection to the website is secure.
- ✓ Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus websites in place. If something does not look right, there is a good chance that it's not.

Fraud Prevention - If you receive a check in the mail that you are not expecting, DO NOT CASH IT. You should call the issuing bank directly to verify that the account is valid, and the check is real. If you think you are the victim of a

counterfeit check cashing scam, submit a complaint at: https://www.fdic.gov/consumers/assistance/filecomplaint.html or file a complaint with the U.S. government Internet Crime Complaint Center at: http://www.ic3.gov/default.aspx.

The FDIC Cyber and Financial Crimes Section can also be contacted at:

FDIC's Cyber Fraud and Financial Crimes Section
550 17th St., NW, Room F-4040,
Washington, D.C. 20429

More Information on Identity Theft

- Federal Deposit Insurance Corporation: https://www.fdic.gov/consumers/assistance/protection/IdTheft.html
- Federal Trade Commission: http://www.consumer.ftc.gov/features/feature-0014-identity-theft
- Social Security Administration: https://www.ssa.gov/pubs/EN-05-10064.pdf
- U. S. Department of the Treasury: https://www.treasury.gov/services/report-fwa/Pages/id_theft.aspx
- U. S. Department of the Treasury/OCC: https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html

NCB will never request a customer's personal information (bank card number, account number, social security number, personal identification number or password) through email or by phone. If you should ever receive an email or phone call requesting your personal, confidential information that appears to be from NCB, DO NOT respond and contact us immediately at 1-800-322-1251.

Corporate Account Takeover Fraud - is a form of corporate identity theft where a business' online banking credentials are stolen by malware. Criminal entities can then initiate fraudulent banking activity, including wire transfers and ACH payments. Corporate Account Takeover Fraud involves compromised identity credentials and is not about compromises to the wire system, ACH Network or other bank systems.[1]

Mail Fishing and Check Washing

Mail Fishing happens when thieves steal outgoing mail from U.S. Postal Service blue drop boxes before it can be picked up. There are several ways to commit mail fishing:

- ✓ Thieves will lodge a catching device inside the box and remove it before the scheduled pick up.
- ✓ Thieves may also apply ultra-strength adhesive to a string, tie it to a water bottle or piece of cardboard, and manually pull up the pieces of mail.
- ✓ Gift cards, replacement debit or credit cards and/or checks (essentially any documents that can be cashed in, forged, or used to steal person information) are stolen.

Check Washing is the process of erasing details from checks to allow them to be rewritten, usually for criminal purposes such as a fraudulent withdrawal from a victim's bank account.

Thieves can also us the account number and routing number from your checks to initiate electronic transfers. What you can do:

- ✓ Make outgoing payments via Bill Payment/ACH/Electronic debit
- ✓ If a check must be issued, follow the below tips to avoid mail fishing:
  - Use the letter slots inside your Post Office or hand your mail directly to your letter carrier.
  - For collection boxes: Drop your mail off as close to possible to collection time. Avoid dropping mail in collection boxes at night or during holiday weekends.
  - Check to see if your mail dropped down into the mailbox and is not hung up on any other surface.
  - When dropping off mail, remain observant of cars and people who appear suspicious.

1 Source: NACHA.org

COVID-19 Related Fraud

Criminals are taking advantage of fears surrounding the COVID-19 pandemic. Scammers are using fake websites direct calls, emails, texts, and social media posts in attempts to get your information. These communications could be promoting awareness and prevention tips, fake information about cases in your neighborhood, promoting fake work from home opportunities, soliciting donations, offering advice on unproven treatments, or providing fake information about government benefits. Here are some tips for Avoiding COVID-19 Scams:

- ✓ Do not respond to calls or texts from unknown numbers, or any others that appear suspicious.
- ✓ Never share your personal or financial information via email, text messages, or over the phone.
- ✓ Be cautious if you are being pressured to share any information or make a payment immediately.
- ✓ Scammers often spoof phone numbers (https://www.fcc.gov/consumers/guides/spoofing-and-caller-id) to trick you into answering or responding. Remember that government agencies will never call you to ask for personal information or money.
- ✓ Scammers will also spoof email addresses and websites. Be wary of emails from government agencies or healthcare organizations. For information go directly to government websites.
- ✓ Do not click any links in a text message or email. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they were not hacked.
- ✓ Always check on a charity (for example, by calling or looking at its actual website) before donating. (Learn more about charity scams (/scam-charities-will-take-your-money-and-run).)

If you think you have been a victim of a coronavirus scam, contact law enforcement immediately. File coronavirus scam complaints online with the Federal Trade Commission (https://reportfraud.ftc.gov/#/).

12 Tips for Protecting Your Mobile Device

As the use of mobile devices continues to climb, cyber criminals are targeting mobile devices more frequently. With the increase in mobile device usage, mobile banking has become more common. It is easy to forget that your mobile device can be vulnerable, but any device connected to the internet is at risk. NCB suggests the following tips:

- ✓ Use the biometric features such as face or fingerprint reader on your smartphone. The use of passcodes should be used on other devices.
- ✓ Log out completely when you finish a mobile banking session.
- ✓ Protect your phone from viruses and malicious software, or malware, just like you do for your computer by installing mobile security software.
- ✓ Use caution when downloading apps. Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary “permissions.”
- ✓ Download the updates for your phone and mobile apps.
- ✓ Avoid storing sensitive information like passwords or a social security number on your mobile device.
- ✓ Tell NCB immediately if you change your phone number or lose your mobile device.
- ✓ Be aware of shoulder surfers. The most basic form of information theft is observation. Be aware of your surroundings especially when you are keying in sensitive information.
- ✓ Wipe your mobile device before you donate, sell, or trade it using specialized software or using the manufacturer’s recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.

- ✓ Beware of mobile phishing. Avoid opening links and attachments in emails and texts, especially from senders you do not know. And be wary of ads (not from your security provider) claiming that your device is infected.
- ✓ Watch out for public Wi-Fi. Public connections are not very secure, so don't perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network. Consider using a Virtual Private Network (VPN) app to secure and encrypt your communications when connecting to a public Wi-Fi network. (See the Federal Trade Commission's tips for selecting a VPN app.)

Report any suspected fraud to NCB immediately. Log into your NCB account often to check your transaction activity and report any suspected fraud to NCB as soon as possible.

How You Can Protect Your Privacy

Identity Theft is one of today's fastest growing crimes. With **identity theft**, a thief uses stolen personal information, such as a Social Security number or bank account number, to open accounts or initiate transactions in your name. Most victims will not discover the fraud until they apply for a loan or receive a call from a collection agency. Clearing your name and erasing the effects of identity theft can take months or even years re-establishing your creditworthiness. Here are some helpful tips to avoid becoming a victim of identity theft:

Personal Identifying Information

- ✓ Always protect personal identifying information, such as your date of birth, Social Security number, credit card numbers, bank account numbers, Personal Identification Numbers (PINs) and passwords.
- ✓ Do not give any of your personal identifying information to any person who is not permitted to have access to your accounts.
- ✓ Do not give any of your personal identifying information over the telephone, through the mail or online unless you have initiated the contact and know and trust the person or company to whom it is given.

Credit, Debit and ATM Cards

- ✓ Limit the number of debit. credit, and ATM cards that you carry.
- ✓ Cancel all cards that you do not use.
- ✓ Retain all receipts from card transactions.
- ✓ Sign new cards as soon as you receive them.
- ✓ Report lost or stolen cards immediately.
- ✓ Report suspicion of fraud to your bank immediately.
- ✓ Sign up for fraud alerts.
- ✓ Download the Card Valet app from the App Store of Google Play to set personal preferences for fraud and other alerts.

Mail

- ✓ Promptly remove mail from your mailbox.
- ✓ Deposit outgoing mail in a post office collection box, hand it to a postal carrier, or take it to a post office instead of leaving it in your doorway or home mailbox, where it can be stolen.
- ✓ Sign up for online banking/electronic statements:
    - To sign up for online banking go to https://www.ncb.coop/personal-banking/online-mobile and click '**Enroll in Online Banking**'.
    - To sign up for mobile banking download the National Coop Bank app from the App Store or Google Play to get started.

To sign up for e-statements log into you online banking and go to 'E-statements' Credit Reports.

- ✓ Order a copy of your credit report annually and review it for accuracy.
- ✓ Check your credit report for unauthorized bank accounts, credit cards and purchases.
- ✓ Look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history.
- ✓ You can obtain your free credit reports as follows:

Online:	**www.AnnualCreditReport.com**
By phone:	(877) 322-8228
By mail:	Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281

Bank Account and Credit Card Statements

- ✓ Contact your financial institution immediately if a bank account or credit card statement does not arrive on time.
- ✓ Review your bank account and credit card statements promptly and immediately report any discrepancy or unauthorized transaction.
- ✓ Sign up for e-statements by logging into your online banking and go to '**E-statements**' to sign up.

Telephone and Internet Solicitations

- ✓ Be suspicious of any unsolicited offer made by telephone, on a website or in an email.
- ✓ Do not respond to an unsolicited email that requests any personal identifying information.
- ✓ Before responding to a telephone or Internet offer, determine if the person or business making the offer is legitimate.

NCB will never request a customer's bank card number, account number, Social Security number, Personal Identification Number (PIN) or password through email. Should you an email requesting such information that appears to be from NCB, do not respond to the email and contact us immediately at 1-800-322-1251.

Home Security

- ✓ Store extra checks, credit cards, documents that list your Social Security number, and similar items in a safe place.
- ✓ Shred all credit card receipts and solicitations, ATM receipts, bank account and credit card statements, canceled checks, and other financial documents before you throw them away.

PINs and Passwords

- ✓ Memorize your PINs and passwords and keep them confidential.
- ✓ Change your passwords periodically.
- ✓ Avoid selecting PINs and passwords that will be easy for an identity thief to figure out.
- ✓ Do not carry PINs and passwords in your wallet or purse or keep them near your checkbook, credit cards, debit cards or ATM cards.

Wallets and Purses

- ✓ Do not carry more checks, credit cards, debit cards, ATM cards and other bank items in your wallet or purse than you really expect to need.
- ✓ Do not carry your Social Security number in your wallet or purse.

Miscellaneous

- ✓ Use common sense and be suspicious when things do not seem right.

- ✓ Be suspicious of any proposed transaction that requires you to send an advance payment or deposit by wire transfer.
- ✓ Make sure that you have installed and run updated anti-virus and anti-malware software. Both viruses and malware can leave your computer vulnerable to attack and intrusion. Anti-virus & anti-malware software is especially important if you are using a broadband Internet connection like DSL, cable, or satellite.
- ✓ Install a firewall, either software or hardware. A firewall will prevent attacks on your computer through the Internet by determining if a requested connection is malicious or not. A firewall is especially important if you are using a broadband Internet connection such as DSL, cable, or satellite.
- ✓ Keep your Internet browser, anti-virus, anti-malware, and firewall up to date by visiting the manufacturer's Website and checking regularly for software and security upgrades.

Call us immediately at 1-800-322-1251 if you believe that you are a victim of identity theft involving one of your NCB accounts.

How NCB Protects You

NCB uses several techniques and technologies to protect your personal information and privacy. Listed below are safeguards that have been implemented to help protect our customers:

- ✓ **Individualized Passwords -** When you sign up for online access, NCB asks you to create your own username to access your accounts. We now allow you to select your own, personal username to sign on, instead of your Social Security number. We strongly recommend that you do not use your Social Security number as a username.
- ✓ **Security Questions -** We ask Online Banking customers to select three security questions and provide answers. If your computer is not recognized upon login, you will be asked to confirm answers to your security questions. Your correct answers to security questions will help us verify your identity.
- ✓ **Timed Log-off -** Our system will automatically log you off from online banking after 10 minutes of inactivity. This reduces the risk of others accessing your information from your computer.
- ✓ **Firewall -** Our computer systems are protected 24 hours a day by a firewall that blocks unauthorized entry. To gain access to authorized information, the Web Browser you are using must know the proper protocol, or language, and even then, only select information is available.
- ✓ **Encryption -** From the moment account information leaves your computer to the time it enters our system, all online access and Bill Pay sessions are encrypted.
- ✓ **Technology updates -** To resist constantly evolving online threats, we have adopted proven industry standards for technology to protect your account security.
- ✓ **Constant Surveillance -** Our security teams maintain and monitor our security systems to increase the security of your accounts.
- ✓ **Additional Security Measures -** Our layered approach to online security extends beyond a unique username and password, encryption, firewalls, technology updates, and continuous surveillance. We have additional security measures that may be activated in response to certain activities or events. If we are suspicious of any online behavior, we may restrict online access to accounts or prevent certain types of transactions. These measures safeguard your identity and your accounts. Further proof of identity may be required before online access is restored.

Should you have any questions or concerns, or believe you are a victim of fraud involving one of your NCB accounts, please contact our Internet Banking team at 1-800-322-1251.