

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

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 in order to commit fraud, identity theft, or simply to disrupt and compromise computer systems.

#### What you can do:

- \* NEVER share your user name or password with anyone.
- \* NCB will NEVER call you and ask for your user name or password.
- \* Report spam/fraud relating to your NCB accounts to [security@ncb.coop](mailto:security@ncb.coop) or 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 you 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 Web site into your browser.
- \* Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus Web sites in place. If something doesn't look right, there is a good chance that it's not.
- \* Before submitting confidential information through forms, make sure that you are using a secure Internet connection. There are two ways of determining if your connection to a Web site is secure. *First*, look at the address bar at the top of your browser. If the Web site 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 Web site is secure.

## 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 [www.fdic.gov/consumers/assistance/filecomplaint.html](http://www.fdic.gov/consumers/assistance/filecomplaint.html) or file a complaint with the U.S. government Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov). 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 & Fraud Prevention***

- \* **Federal Deposit Insurance Corporation**  
[www.fdic.gov/consumers/consumer/guard/index.html](http://www.fdic.gov/consumers/consumer/guard/index.html)
- \* **Federal Trade Commission**  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- \* **Social Security Administration**  
[www.ssa.gov/pubs/idtheft.htm](http://www.ssa.gov/pubs/idtheft.htm)
- \* **U.S. Department of the Treasury**  
[www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml](http://www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml)
- \* **U.S. Department of the Treasury/OCC**  
<http://www.occ.treas.gov/Consumer/phishing.htm>

**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 **(800) 322-1251**.

## Corporate Account Takeover Fraud

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.<sup>1</sup>

---

<sup>1</sup> Source: NACHA.org

# 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.

---

## BANK ACCOUNT & 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.

---

## TELEPHONE & INTERNET SOLICITATIONS

- \* Be suspicious of any unsolicited offer made by telephone, on a Web site or in an email.
- \* Before responding to a telephone or Internet offer, determine if the person or business making the offer is legitimate.
- \* Do not respond to an unsolicited email that requests any personal identifying information.
- \* NCB will never request a customer's bank card number, account number, Social Security number, Personal Identification Number (PIN) or password through email. If you should receive an email requesting such information that appears to be from NCB, do not respond to the email and contact us immediately at **(800) 322-1251**.

## CREDIT, DEBIT AND ATM CARDS

- \* Limit the number of credit, debit 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.

---

## 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.

---

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

## 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 & 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 & 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-spyware software. Both viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus & anti-spyware 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 like DSL, cable or satellite.
- \* Keep your Internet browser, anti-virus, anti-spyware and firewall up to date by visiting the manufacturer's Web site and checking regularly for software and security upgrades.

***Call us immediately at (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 PASSWORD**

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. In order 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

In an effort to resist constantly evolving online threats, we have adopted proven industry standards for technology to protect your account security.

## CONSTANT SURVEILLANCE

Our security team maintains and monitors 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 (800) 322-1251.***