

## Identity Theft

Illinois National Bank wants to offer you something we hope you never have to use. This page offers information about what to do if you become a victim of a phishing scam or identity theft.

Phishing, of course, involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Illinois National Bank recommends that you never respond to email messages asking you to verify personal information. But accidents happen, and the following information could be useful if you've been scammed.

### If you have given out your credit, debit or ATM card information:

- Report the incident to the card issuer immediately
- Cancel your account and open a new one
- Review billing statements carefully after the incident
- If the statements show unauthorized charges, send a letter to the card issuer via regular mail (keep a copy) describing each questionable charge

### Credit Card Loss or Fraudulent Charges

Your maximum liability under federal law for unauthorized use of your credit card is \$50 (policies vary). If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use; in general, you may only be liable for a very small amount but always check with your individual card company for their exact policy.

Your liability depends on how quickly the loss is reported. You risk unlimited loss by failing to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you.

### If you have given out your bank account information:

- Report the theft to the bank as quickly as possible
- Cancel your account and open a new one

### If you have downloaded a virus or 'Trojan Horse':

- Some phishing attacks use viruses and/or a 'Trojan Horse' to install programs called "key loggers" on your computer. These programs capture and distribute any information you type to the phisher, including credit card numbers, usernames and passwords, Social Security Numbers, etc.
- If this occurs, you likely may not be aware.
- To minimize this risk, you should:
  - Install and/or update anti-virus, personal firewall, and anti-spyware software
  - Update all virus and spyware definitions and run a full scan
  - If your system still appears compromised, fix it and then change your password again.

Check your other accounts – suspects may have accessed different accounts: eBay account, PayPal, your email ISP, online bank accounts, and other e-commerce accounts.

If you have given out your personal identification information:

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have given this information to a phisher, you should do the following:

- Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:
  - Request that they place a fraud alert and a victim's statement in your file
  - Request a FREE copy of your credit report to check whether any accounts were opened without your consent
  - Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft

Major Credit Bureaus:

Equifax - [www.equifax.com](http://www.equifax.com)

Experian - [www.experian.com](http://www.experian.com)

Trans Union - [www.transunion.com](http://www.transunion.com)

Identify Theft Resources:

<http://www.consumer.gov/idtheft/>

<http://www.identity-theft-help.us/>

<http://www.identitytheft.org/>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

<http://www.ifccfbi.gov/index.asp>

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

Notify your bank(s) and ask them to flag your account and contact you regarding any unusual activity: If bank accounts were set up without your consent, close them; If your ATM card was stolen, get a new card, account number and PIN; Contact your local police department to file a criminal report; Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information; Notify the Department of Motor Vehicles of your identity theft; Check to see whether an unauthorized license number has been issued in your name; Notify the passport office to watch for anyone ordering a passport in your name; File a complaint with the Federal Trade Commission; Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name"; File a complaint with the Internet Fraud Complaint Center(IFCC) by visiting their website: <http://www.ifccfbi.gov/index.asp>.

For victims of Internet fraud, IFCC provides a convenient and easy reporting mechanism that alerts authorities of suspected criminal or civil violations.

Document the names and phone numbers of everyone you speak with regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.

If you see a suspicious-looking email message claiming to be from Illinois National Bank, please let us know by email at [abuse@illinoisnationalbank.com](mailto:abuse@illinoisnationalbank.com) or you may also contact our customer service department by email at [customerservice@illinoisnationalbank.com](mailto:customerservice@illinoisnationalbank.com) or by phone at 217-747-8766. We continually monitor such reports and act on them promptly. Additionally, also consider contacting the FBI's Internet Fraud Complaint Center at [www.ifccfbi.gov](http://www.ifccfbi.gov).