



INTERNET SECURITY PRACTICES

Phishing

“ Phishing” is a relatively new term for the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Responding to “phishing” emails puts your accounts at risk. Cyber-criminals include exciting or upsetting statements in their e-mails to encourage unsuspecting people to react immediately and respond with the desired information, such as personal IDs, passwords, card numbers and PINs. This information is then sold to other criminals who use it for financial gain. They can also access a customer’s accounts through online banking, set up false bill payments that send checks to the criminal or a conspirator, or transfer funds from all available customer accounts.

Email

- Be alert for fraudulent emails. These are sometimes called “phishing” emails. They may appear to come from a reputable business or a trusted friend but are actually designed to trick you into disclosing personal or sensitive information. Please see the section below for more information on “phishing”.
- Immediately delete any email that requests your personal information; do not reply to it. Reputable businesses never request your PIN, credit card number or social security number.
- Never send your personal information via unsecured email.
- If an email from an unknown - or unsolicited - sender contains an attachment of any kind, do not open it. Delete the email immediately.
- Be cautious when clicking on a link in an email that you receive. It may be fraudulent, even though the link appears to be identical to the actual company's Web site. To check the ownership of the destination page, open a new browser window (Internet Explorer or Netscape) and manually type in the URL provided in the email. If they don't match, immediately delete the email with the suspicious link.

Online Security

- If you suspect a Web site is not what it claims to be, leave it immediately. Do not follow any of the instructions it presents.
- Only do business with the companies you know and trust.

- Be aware! Phony "look-alike" Web sites are designed to trick consumers and collect their personal information. Make sure the sites you transact business on post their privacy and security statements. Review the statements carefully. Please see Nashville Bank & Trust's privacy statement.
- Provide sensitive personal or financial information only when you have initiated it and only if the page is secure. (Look for the padlock in the lower right side of your browser window.)
- Make sure the Web site is certified with a digital security certificate by clicking on the "closed lock" or "solid key" image located in the bottom bar of your browser window. A small frame with site security information will appear. Click the word 'Subject' for Internet Explorer to verify you are on the correct Web site, and make sure the registered owner matches the site. To verify the site certification authority, click the 'Issuer' tab. For Netscape, click on "View Certificate" to view subject and issuer details.
- Choose passwords or Personal Identification Numbers (PINs) that are difficult for others to guess (NOT your birthday or street address or the last four digits of your Social Security number), and use a different password for each of your Internet accounts. Change these passwords frequently. Use both letters and numbers and a combination of lower- and upper-case letters if the passwords are case-sensitive.

Virus Protection

- Maintain current versions of your computer's operating system and Internet browsers.
- When you're not online, always disconnect from the Internet.
- Always back up the files on your computer.
- Install a personal firewall to help prevent unauthorized access to your home computer, especially if you connect to the Internet via a cable modem or a digital subscriber line (DSL) modem.
- Keep your anti-virus software up-to-date. Anti-virus software needs frequent updates to guard against new viruses. Download the anti-virus updates as soon as you're notified that a download is available. Some anti-virus programs offer an "auto-update" feature, where regular updates are made automatically for you.

These sites below have detailed instructions about the steps an individual should take, if he or she has been a victim of Identity Theft.

Federal Trade Commission Identity Theft Web Site: www.ftc.gov/idtheft

Office of Tennessee Attorney General: <http://www.tn.gov/attorneygeneral/>

Identity Theft Resource Center: <http://www.idtheftcenter.org/>

In addition, you should call to notify the credit bureaus that your financial information may have been stolen. This is an automated phone system and it will allow you to acquire

a copy of your credit report so you may review it for unknown or unusual activity or queries.

This number is 1-800-680-7289.

There are also 3 ways to request your free credit report, or find out when you are eligible for a free one.

Visit www.annualcreditreport.com

Call 877-322-8228

Write to:

Annual Credit Report Request Service

P.O. Box 105283

Atlanta, GA 30348-5283