GOOD SECURITY TIPS

TIPS

- Add your phone numbers to the national Do Not Call Registry at www.donotcall.gov or by calling 1-888-382-1222. Since February 2008, these registered telephone numbers will no longer expire off the list.
- Examine your financial institution statements immediately upon receipt to determine whether there were any unauthorized transactions. Report any unauthorized transactions that you find immediately to **your bank or financial institution.**

ANNUALLY

- Each year, you are entitled to one free credit report through www.annualcreditreport.com or by calling 1-877-322-8228.
- Request a copy of your Social Security statements at www.ssa.gov/mystatement to be sure that no one else is using your social security number for employment.

EVERY 5 YEARS

- Opt out of pre-screened credit offers by calling 1-888-567-8688 or at www.optoutprescreen.com.

Please read the other sections below to learn about the different types of fraud and how to prevent them, from spyware and other computer fraud to mail and phone fraud to email phishing and web spoofing. Our Fraud Summary page provides more tips on how to protect yourself.

Fraud Summary

Identity Theft is the most popular and profitable form of consumer fraud. It 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.

Common way's identity theft can happen:

"OLD FASHIONED" STEALING

- Thieves typically steal wallets and purses. They also steal mail such as credit card and bank statements, pre-approved credit card offers, check orders and other financial mail.

DUMPSTER DIVING

- Thieves dig through trash looking for bills, financial or other personal information.

CHANGE OF ADDRESS

- Thieves modify or redirect your billing statements to another address by completing a "change of address" form.

PHISHING

- Thieves may send unsolicited Emails, pretending to be a financial institution or a company, asking you to click a link to update or confirm your personal or login information. The link is directed to a "spoof" website designed to look like a legitimate site.

SKIMMING

- Thieves may use a card reader device to copy the card's magnetic strip to duplicate without the card owner's knowledge.

MONITOR YOUR ACCOUNTS

Keep track of transactions on your accounts by logging in to your bank or financial institution's Online Banking, where you can view your activity as it is posted.

PROTECT YOUR PERSONAL INFORMATION

- Do not carry your Social Security card in your wallet.
- Do not have personal information such as your Social Security number and driver's license number printed on your checks.
- Keep your new and cancelled checks in a safe place.
- Do not leave your purse, wallet, checkbook, or any other forms of identification in your car
- Shred or tear up any documents containing banking or credit information, especially pre-approved credit offers, before you throw them away. To opt out of pre-approved credit card offers, call 1-888-567-8688.
- Keep your PINs and passwords a secret. Do not write them down or share them with anyone.

COMPUTER PROTECTION TIPS:

- Update your computer operating system on a regular basis.
- Keep your browser current with the latest security updates.
- Use updated anti-virus software.

- Use updated anti-spyware software and consider using more than one, to ensure the most thorough scan.
- Change your passwords on a regular basis, as a good practice to help prevent unauthorized access.
- Download free software only from websites you know and trust.
- Do not install software without knowing exactly what it is or what it will do (read the end-user license agreement).
- Close pop-up ads by clicking on the "X" instead of clicking within the advertisement itself.
- Review your browser security settings and set them to a high enough level to help detect unauthorized downloads. (Click your browser's "Help" menu for steps).
- Do not click link inside of spam email. Especially emails claiming to offer anti-spyware software.
- Install a personal firewall on your computer. A firewall works like a filter that prevents access to information on your computer.
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.

Mail & Phone Security

We recommend you learn ways to protect yourself from common fraud schemes.

Vishing

Vishing scams target consumers by “spoofing” text or voicemail messages that ask you to call a phone number and give your personal information. Here is how it works:

- You receive a "spoof" email, text message, or voicemail about suspicious account activity.
- The email, text message, or voicemail message will ask you to call a “customer service” number.
- When you call the customer service number, a recording will ask you to provide personal information such as account numbers, passwords, a social security number, or other critical information.
- The recording may not mention the company’s name and could potentially be an indication the call is being used for fraud.
- In a variation of this scam, you may receive a phone call.
- The call could be a “live” person or a recorded message.
- The caller may already have your personal information, which may seem as if the call is legitimate.

Smishing

Smishing is when consumers' cell phones and other mobile devices are targeted with mobile spam. The spam, or text messages, attempt to trick consumers into providing personal information. Here is how it works:

- You receive a fake text message, which may include a fraudulent link, asking you to register for an online service.
- The scammer attempts to load a virus onto your cell phone or mobile device.
- The scammer may also send a message 'warning' you that your account will be charged unless you cancel your supposed online order.
- When you attempt to log on to the website, the scammer extracts your credit card number and other personal information.
- In turn, your information is used to duplicate credit, debit, and ATM cards.
- Scammers may also send you a text message again 'warning' you that your bank account has been closed due to suspicious activity.
- The text message will ask you to call a 'customer service' number to reactivate your account.
- When you call the number, you are taken to an automated voice mail box that prompts you to key in your credit card, debit card or ATM card number, expiration date and PIN to verify your information.
- Again, your information is used to duplicate credit, debit, and ATM cards.

Lottery/Sweepstakes Scams

Lottery/Sweepstakes scams target consumers by a notification, which arrives through the mail, by email, or by an unsolicited telephone call. Here's how it works:

- The notification advises you have won a prize, but you did not enter in any type of lottery or sweepstake by the promoter contacting you.
- The promoter will ask you to send payment to cover the cost of redeeming the prize when the prize does not exist.
- In this type of scam, you may rarely if ever receive any winnings in return.

Check Overpayment Scams

Check Overpayment scams target consumers who sell items through an online auction site or a classified ad. Here is how it works:

- The seller takes a big loss when the 'buyer' passes a counterfeit cashier's check, money order, corporate or personal check as payment.
- The counterfeit check is written for more than the agreed price.

- The 'buyer' will ask the consumer to wire back the difference after the check has been deposited.
- The check will more than likely bounce, and the consumer becomes liable for the entire amount.

Tips for the mailbox

- Deposit outgoing mail at the Post Office.
- Remove incoming mail from your personal mailbox as soon as possible, or use a P.O. Box or locked, secure mailbox.
- Request a mail hold from the United States Postal Service or call them at 1-800-275-8777 if you plan to be away from home for an extended period.
- Know your billing cycles. If bills are late or missing, contact your creditors.
- Switch to a more secure way of receiving your account statement. When you sign up for **Online** E-Statements, your statement will no longer sit in your mailbox. Instead, we will send you an email when your statement is available through your secure Online Banking account.

Tips for the phone

- Do not give out personal information, such as your account numbers, card numbers, Social Security, tax identification numbers, passwords, or PINs, unless you have initiated the call.
- We will not make an unsolicited call requesting your personal information.
- If you ever believe you are not talking to a representative of a legitimate company, hang up and call the phone number listed in the telephone book.

Phishing & Spoofing

Phishing scams target consumers by “spoofing” emails and websites. Here’s how it works:

- You receive an email message, asking you to click on a link to update some sensitive personal information.
- The link will redirect you to a "spoofed" website, which is designed to look like a legitimate website.
- The website will ask you to input personal information such as your account numbers, PINs, or a social security number.

Email protection tips

- Do not click links in Emails to log in, or to update or confirm your sensitive information
- Do not fill out forms in Emails
- Be cautious about opening attachments or downloading files, regardless of who sent them
- 'Spam', or mass email messages, often contain links to phishing websites and other unsavory websites.
- Many phishing scams originate outside of the United States. Be wary of emails from people or sources you do not know or trust.
- Poor grammar and misspelled words from unknown sources asking you for personal information are clear warning signs of a phishing scam being operated outside of the United States.
- Legitimate companies or organizations will never ask you to divulge any personal information over email.
- Phishing emails may also be fake contests or offerings, asking you to input personal information.
- If an offer or email you receive is too good to be true, it most likely is.

Bank Error Messages

One of the newest schemes by fraudsters involves spoofing bank error messages. Here's how it works:

- Fraudsters will send you an email message about a data or site maintenance error f or any of your banks.
- The email will ask you to click on a link, which will redirect you to a site and will install malware on your computer.
- This malware allows scammers to intercept your password and bypass the dual authentication system many financial institutions use.
- The next time you attempt to log in to your online banking service, scammers attempt to steal your password and may quickly drain your account.