



HOW WE PROTECT YOU

Keeping your financial and personal information secure and confidential remains one of our top priorities.

We keep your information secure in the following ways:

Computer anti-virus protection detects and prevents viruses from entering our computer network.

Firewalls block unauthorized access by individuals or networks. Firewalls are one way we protect our computer systems that interact with the other computers though the internet and the internet itself.

Secure transmissions ensure information remains confidential. We use encryption technology, such as Secure Socket Layer (SSL), to transmit information between you and us. This protects data in three key ways:

1. **Authentication** ensures that you are communicating with us, and prevents another computer from impersonating us.
2. **Encryption** scrambles transferred data so it cannot be read by unauthorized parties.
3. **Data integrity** verifies that the information you send to us is not altered during the transfer. The system detects if data was added or deleted after you sent the message. If any tampering has occurred, the connection is dropped.

Advances in security technology are constantly evaluated by security and technology experts to ensure that we provide the right protection for you.

Secure email is provided through Online Banking, giving you peace of mind that your communications with us are always private.

HOW YOU CAN PROTECT YOURSELF

Studies show time and time again that identity fraud happens much more often offline, than online. However, we feel it is important that you have the information necessary to safely conduct your personal business online. Follow this guide to learn how to prevent, detect, correct and report online fraud and identity theft.

PREVENT

Prevention is the most critical element to avoiding online fraud. See how many of the following you are currently undertaking – and incorporate the rest into your routine.

Prevent: General Online Security

- Shred all financial documents and paperwork with personal information – do not simply throw them in the trash.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write it anywhere. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you are already familiar with. Use firewalls, anti-spyware, and anti-virus software to protect your home/office computer – and keep them current.
- Create passwords that are unusual: do not use your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you employ outside help, have roommates, or are having work done in your house.
- Ordering online? Only use "secure" web pages. (A web page is secure if there is a locked padlock in the lower left-hand corner of your browser).
- Place a "Fraud Alert" on your credit reports, and review the reports carefully.
- The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The

following consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert.

- Choose one of the following:
 - **Equifax:** 1-800-525-6285
 - **Experian:** 1-888-EXPERIAN (397-3742)
 - **TransUnion:** 1-800-680-7289
- When your computer is not in use, shut it down or disconnect it from the Internet.
- Always sign off from your Online Banking session
- Avoid clicking on links provided in emails. It is always better to type the address into you browser.
- Most computer files have filename extensions, such as “.doc” for documents or “.jpg” for images. Any file that appears to have a double extension, like “heythere.doc.pif” is extremely likely to be a dangerous file and should never be opened.
- Never open email attachments that have file endings of .exe, .pif, or .vbs. These are file extensions for executables, and are commonly dangerous files.
- Be careful and selective before providing your email address to a questionable website. Sharing your email address makes you more likely to receive fraudulent emails.

DETECT

Detect: General Online Security

Despite all efforts to prevent it, identity fraud can still occur. The earlier it is detected, however, the swifter we can help you take action to stop it.

Be alert and take immediate action to the following:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you didn't make
- Take advantage of free annual credit reports: Credit reports contain information about what accounts you have and your bill paying history.

Free copies are required by law from the major nationwide consumer reporting companies – Equifax, Experian, and TransUnion. Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- Review your financial and billing statements regularly and look for charges you did not make.
- Keep a list of all your credit card numbers and phone numbers in case of theft, and notify each issuer immediately if theft/loss occurs.

Detect: Online Banking Security

Take advantage of online tools we have that automatically protect you, including:

Balance Alerts

- Check Clear Alerts
- Payment Alerts
- Online Statements
- Account History

Business Online Banking

- Alerts
- Account Reconciliation/PositivePay (Business customers only)

CORRECT

Correct: General Online Security

- Close any accounts that have been tampered with or established fraudulently.
- Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
- Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.

- File a police report. File a report with law enforcement officials to help you with creditors who may want proof of the crime.

REPORT

Report: General Online Security

Report the theft to the Federal Trade Commission. Filing a report helps law enforcement officials across the country in their investigations:

Online: ftc.gov/idtheft

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

By mail: Identity Theft Clearinghouse
Federal Trade Commission
Washington, DC 20580

Report: Online Banking Security

Always report theft and fraudulent activity to your financial institution, no matter if you are a victim or simply suspect the activity.

GLOSSARY

Frequently used online identify theft and online security terminology.

A

AntiVirus Software

A computer software program that detects and responds to viruses and worms, blocking access to infected files and performing frequent updates.

B

Browser

A computer software program that is used to view and interact with Internet material on the World Wide Web. Netscape Navigator and Microsoft Internet Explorer are two of the most popular browsers.

D

Dumpster Diving

Thieves rummage through trash looking for bills or other paper that includes your personal information.

E

Encryption

A process in which data is scrambled before it is transferred so that it cannot be read by unauthorized parties.

Enhanced Security Login

Provides security at login, no matter what computer you sign in from, using additional end user authentication that helps to protect against online fraud.

F

Firewall

A gateway supported by hardware or software that limits access between computer networks. Firewalls can protect your home computer from hackers and your family from web sites that may contain offensive material.

H

Hacker

A person who tries to gain unauthorized access to a computer system. Hackers are known to modify computer programs and security systems that protect home and office computers.

K

Keystroke Capture

A spyware program or device that records what users type on their computer. Also referred to as Keystroke Logger.

M

Malware

Also known as 'malicious software', malware is designed to harm, attack or take unauthorized control over a computer system. See Virus, Trojan and Worm.

O

Opt-In

Permission granted to a business or organization to use your email address for promotional or marketing purposes, or to rent your email address to another organization.

Opt-Out

The opposite of Opt-In- not granting permission for a business or organization to use your email address for promotional or marketing purposes, or to rent your email address to another organization.

P

Patch

A new software release created to update a computer software program. Updates may include security, performance, or usability enhancements.

Pharming

Pharming takes place when users type in a valid URL and you are illegally redirected to a web site that is not legitimate in order to capture personal information through the internet such as credit card numbers, bank account information, Social Security number and other sensitive information.

Phishing

The process of seeking to obtain personal information illegally through email or pop-up messages in order to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Pop-Up Ads

A form of web advertising that appears as a "pop-up" on a computer screen, they are intended to increase web traffic or capture email addresses. However, sometimes popup ads are designed with malicious intent like when they appear as a request for personal information from a financial institution.

Privacy Policy

A standard policy included on most corporate websites that explains how personal information collected about visitors to a company's site is handled.

S

Service Pack

A software program that updates; fixes and/or enhances a software program found on your computer, typically delivered in the form of a single, installable package.

Skimming

When an unauthorized second copy of a credit or debit card is taken by an employee at a store by using a storage device that copies the details held within the card's magnetic strip.

Spam

Unsolicited bulk electronic “junk” messages sent to huge numbers of people via email, instant messaging, Usenet newsgroups, and more.

Spoofing

A form of phishing, a way for cyber criminals to send emails that look legitimate, but are not, to falsely represent a legitimate company or organization. The false email from phishing will include a phony link to what closely resembles a legitimate website address. Once click upon, the victim is asked to provide personal information which is then forwarded to criminals.

Spyware

Loaded onto your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to hackers over the Internet.

I**Trojan Horse**

A malicious program that is disguised or embedded within legitimate software program that, when activated, unwittingly allows hackers to gain unauthorized access to the computer.

V**Virus**

A self-replicating computer program, loaded on to your computer without your knowledge that spreads by making copies of itself and clogging up your computer’s memory.

W**Worm**

Similar to a computer virus, a worm attaches itself to, and becomes part of, another executable program. Able to self-propagate, worms generally harm the network and consume bandwidth.