The privacy of communications between you (your browser) and our servers is ensured via **encryption**. Encryption scrambles messages exchanged between your browser and our online banking server.

How Encryption Works

When visiting online banking's sign-on page, your browser establishes a secure session with our server.

The **secure session** is established using a protocol called **Secure Sockets Layer (SSL)** Encryption. This protocol requires the exchange of what are called public and private **keys**.

Keys are random numbers chosen for that session and are only known between your browser and our server. Once keys are exchanged, your browser will use the numbers to scramble (**encrypt**) the messages sent between your browser and our server.

Both sides require the keys because they need to descramble (**decrypt**) messages received. The SSL protocol assures privacy, but also ensures no other website can "impersonate" your financial institution's website, nor alter information sent.

To learn whether your browser is in **secure mode**, look for the secured lock symbol at the bottom of your browser window.

Encryption Level

The numbers used as encryption keys are similar to combination locks. The strength of encryption is based on the number of possible combinations a lock can have. The more possible combinations, the less likely someone could guess the combination to decrypt the message.

For your protection, our servers require the browser to connect at 128-bit encryption (versus the less-secure 40-bit encryption). Users will be unable to access online banking functions at lesser encryption levels. This may require some end users to upgrade their browser to the stronger encryption level

To determine if your browser supports 128-bit encryption:

Click "Help" in the toolbar of your Internet browser

Click on "About [browser name]"

A pop-up box or window will appear.

- For Internet Explorer: next to "Cipher strength" you should see "128-bit"
- For Netscape: you should see "This version supports high-grade (128-bit) security with RSA Public Key Cryptography"

If your browser does not support 128-bit encryption, you must upgrade to continue to access the website's secure pages.

Firefox and Safari browsers and DI

July 2005

1. **Firefox and Safari - Encryption levels**

   Both browsers recently designated as supported for use with DI products, Firefox 1.0 and Safari 1.2, use strong 128-bit encryption when accessing secure sites, to ensure safe and secure transmittal of private data such as account and payment information.

2. **Firefox and Safari - How end users can determine which levels of encryption they have**

   A. Firefox - In Firefox, this option is not visible until connected to a site. Negotiation occurs between the client browser and the server at run-time. To view the encryption level being used while connected to a specific secure site, you can do the following:

      - Click to the 'Tools' menu
      - Select 'Page Info'
      - Click the 'Security' tab

Or: double-click the yellow 'lock' icon in the lower right corner of the screen while connected to a secure site.

Safari - The Safari browser displays a 'lock' icon at the top right corner of the browser window when you're viewing a secure (https://) site. This symbol is absent when viewing an unsecured (http://) site. Safari can use both 40-bit and 128-bit "strong" encryption; the website determines which level of encryption is used at a given time

Other browsers that support 128-bit encryption also may work. More information on some common browsers is available via these links:

Netscape

Microsoft Internet Explorer

Firefox

Safari

Authorization

It is important to verify that only authorized persons log into online banking. This is achieved by verifying your password. When you submit your password, it is compared with the password we have stored in our secure data center.

We allow you to enter your password incorrectly a limited number of times; too many incorrect passwords will result in the locking of your online banking account until you call us to reinitialize the account. We monitor and record "bad-login" attempts to detect any suspicious activity (i.e. someone trying to guess your password).

You play a crucial role in preventing others from logging on to your account. Never use easy-to-guess passwords. Examples:

- Birth dates
- First names
- Pet names
- Addresses
- Phone numbers
- Social Security numbers

Never reveal your password to another person. You should periodically change your password in the User Option screen of online banking

Network Security

The network architecture used to provide the online banking service was designed by the brightest minds in network technology. The architecture is too complex to explain here, but it is important to convey that the computers storing your actual account information are not linked directly to the Internet.

Transactions initiated through the Internet are received by our online banking Web servers

These servers route your transaction through firewall servers

Firewall servers act as a traffic cop between segments of our online banking network used to store information, and the public Internet.

This configuration isolates the publicly accessible Web servers from data stored on our online banking servers and ensures only authorized requests are processed.

Various access control mechanisms, including intrusion detection and anti-virus, monitor for and protect our systems from potential malicious activity. Additionally, our online banking servers are fault-tolerant, and provide for uninterruptible access, even in the event of various types of failures.

Security Features

We provide a number of additional security features in online banking. For example, online banking will "timeout" after a specified period of inactivity. This prevents curious persons from continuing your online banking session if you left your PC unattended without logging out. You may set the timeout period in online banking's User Options screen. We recommend that you always sign off (log out) when done banking online.

Identity Theft Information

What is 'Phishing'?

phishing (FISH.ing) pp. Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. -phisher n.

Example Citations:
Phishing is the term coined by hackers who imitate legitimate companies in email messages to entice people to share passwords or credit-card numbers. Recent victims include Bank of America, Best Buy and eBay, where people were directed to Web pages that looked nearly identical to the companies' sites

What is 'Spoofing'?

Pretending to be something it is not, whether an email, website, etc...

How to report 'Phishing' or 'Spoofing'

We suggest reporting "phishing" or "spoofed" emails to the following groups:

- Forward the email to reportphishing@antiphishing.org
- Forward the email to the Federal Trade Commission at spam@uce.gov
- Forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
- When forwarding spoofed messages, always include the entire original email with its original header information intact
- Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ic3.gov

Recommended actions if you've become a victim of phishing or other identity theft scam

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

- Report the incident to the card issuer as quickly as possible
- Many companies have toll-free numbers and 24-hour service to deal with such emergencies
- Cancel your account and open a new one
- Review your billing statements carefully after the loss
- If the statements show any unauthorized charges, it's best to send a letter to the card issuer via regular mail (keep a copy for yourself) 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 (many financial services companies have different policies so be sure to check with each of them). 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.

ATM or Debit Card Loss or Fraudulent Transfers

- Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
- You risk unlimited loss if you fail 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 of this information 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 'Trojan Horses' to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames and passwords, Social Security Numbers, etc.

If this happens, it's likely you may not be aware of it.

To minimize this risk, you should:

- Install and/or update anti-virus and personal firewall software
- Update all virus definitions and run a full scan
- If your system appears to have been compromised, fix it and then change your password again, since you may well have transmitted the new one to the hacker
- Check your other accounts! The fraudsters may have helped themselves to many different accounts: eBay account, PayPal, your email ISP, online bank accounts, online trading accounts, and other e-commerce accounts, and everything else for which you use online password

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 out this kind of 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

Identity Theft Info

Equifax - www.equifax.com

- To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241
- To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241
- Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.

Experian - www.experian.com

- To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen TX 75013
- To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen TX 75013 TDD: 1-800-972-0322

Trans Union - www.transunion.com

- To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022
- To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803

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 out 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," a guide that will help you guard against and recover from your theft.
- File a complaint with the Internet Fraud Complaint Center(IFCC) by visiting their website: http://www.ic3.gov/default.aspx
- The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet
- For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.

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

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.ic3.gov/default.aspx

http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm