

## Online Banking Security

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.

### Safeguarding Tips on the Internet

- Beware of fraudulent emails or websites known as "phishing" or "web spoofing" that appear to be from THE BANK – Oldham County or other legitimate sites. Always go directly to THE BANK – Oldham County's website by typing [www.thebankoc.com](http://www.thebankoc.com) directly into the browser address bar. You should never access THE BANK'S website from a link provided by a third party.
- Our financial institution will never request confidential information, such as account numbers, passwords, or PIN's via email. Should you ever receive such a request please report to us immediately
- Maintain and run updated virus protection software. Ensure that your browser is up to date and security patches are promptly applied.
- Be cautious about opening email attachments from unknown parties or downloading files from unverified locations. Many of these files contain spyware or key-logging programs that can send information back to a malicious site.

### What is 'Phishing'?

phishing (FISH.ing). 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.

#### *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 practice 'safe computing'**

The number and sophistication of phishing and spoofing scams sent out to consumers is continuing to increase dramatically. While online banking is widely considered to be as safe or safer than in-branch or ATM banking, as a general rule you should be careful about giving out your personal financial information over the Internet. Below is a list of recommendations you can use to avoid becoming a victim of these scams:

1. Be suspicious of any email with urgent requests for personal financial information
2. Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
3. They typically ask for information such as usernames, passwords, credit card numbers, Social Security numbers, etc.
4. Phisher emails typically are not as personalized and may contain spelling errors while valid messages from your bank or e-commerce company generally are accurate in the way they spell your name and your financial institution's name.
5. Don't use the links in an email to get to any Web page, if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
6. Avoid filling out forms in email messages that ask for personal financial information
7. Only communicate information such as credit card numbers or account information via a secure website or the telephone
8. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
9. A secure Web server designation can be found by checking the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://"

### **How Not to Get Hooked by a 'Phishing' Scam**

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing." Phishing, also called "carding," is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.

Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.

Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

## **Identity Theft**

How can someone steal your identity? 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 think your identity has been stolen, here's what to do now:

Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.

Close the accounts that you know or believe have been tampered with or opened fraudulently.

File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

### **Equifax – [www.equifax.com](http://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](http://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](http://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

## 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 through the internet.

**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.

## 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.

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 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 your 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](http://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 Request 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 card issuer immediately if theft occurs.

### **Detect: Online Banking Security**

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

- Balance Alerts
- Check Clear Alerts
- Account History
- Check Images

### **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 [www.ftc.gov/idtheft](http://www.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: [www.ftc.gov/idtheft](http://www.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 suspect the activity.