

## Security

We understand that when it comes to your personal finances, conducting your banking in a safe, secure environment is essential. Whether you are visiting us in person, utilizing TeleBank or conducting a transaction at one of our ATMs, you can rest assured that MOREBANK utilizes state-of-the-art technology to protect your interests. More importantly, we continuously evaluate new technologies and procedures to ensure that your protection continues without interruption. That commitment extends to our Online Banking and Bill Pay services.

### About Our Online Banking Service

Banking via the internet is an established practice in today's society, and the systems available are designed and continuously tested to protect your interests. Our Online Banking solution brings together a combination of industry-approved security technologies to protect bank and customer data. MOREBANK requires that you use a browser that supports 128-bit encryption, providing the most powerful method of scrambling information available.

Also remember that government agencies routinely audit our institution to ensure that sound business practices are in place and that we operate in accordance with state and federal laws.

Only specific browsers provide the right environment for security.

### Keeping Your Information Secure: Some Helpful Hints

- Do not use an obvious number or other accessible information (such as a portion of your phone number) for your Online Banking ID or Personal Identification Number (PIN).
- Do not log onto Online Banking when someone else is watching.
- Avoid Online Banking and Bill Pay when you are using a computer that is not your own.
- If others have access to your computer, clear the browser's cache to eliminate copies of web pages that may be stored on your hard drive.
- Avoid writing down your log-in ID and PIN - try to memorize them.
- Never provide your log-in ID and PIN to anyone.
- Report any unusual activity.
- Never leave your computer unattended when you are logged on.
- Always log out of the system.

### Protecting Against Identity Theft

[FDIC PRESENTS: Don't be an Online Victim: How to Guard Against Internet Thieves & Electronic Scams](#)

#### Phishing

Identity thieves often attempt to steal personal information (such as credit card numbers, bank account information, Social Security numbers and passwords) by sending official-looking, but fraudulent e-mails or pop-up messages.

Phishers typically send a message, claiming to be from a business or organization with which you are associated. For example, the e-mail may purport to be from your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information, and threaten some consequence if you don't respond. The message usually contains a link to what appears to be a legitimate web site, but is in fact a bogus site created to STEAL your identity and account information.

#### Spoofing

Web spoofing allows an attacker to create a "shadow copy" of any legitimate website. Access to the shadow web site is funneled through the attacker's computer, allowing the attacker to monitor all of the victim's activities, including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to web servers in the victim's name, or to the victim in the name of any web server.

In spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the address of that machine. Phishing and spoofing often go hand-in hand in Internet fraud.

### How to Protect Yourself

- Be wary of unsolicited or unexpected emails from all sources.
- If an unsolicited email arrives, be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.

- If you receive an email that warns you, with little or no notice, that your account will be shut down unless you reconfirm certain information, do not click on the email link. Instead, use a phone to contact the business or organization yourself. Clicking on a link that looks legitimate may in fact direct you to a fraudulent website where crooks will steal your personal information. Remember, a legitimate business or government agency will never send you an e-mail asking you to disclose your personal information.
- Before submitting any financial information to a legitimate website, look for the "lock" icon on the browser status bar, or look for "https" in the web address. Both are indications that the information is secure and encrypted 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.
- Make sure your unused checks, bills, credit/debit card receipts, "pre-qualified" credit card solicitations you receive in the mail and statements are shredded before discarding.
- Use Anti-Virus Software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
- Report suspicious activity to the Federal Trade Commission (FTC) Consumer Response Center ([www.ftc.gov](http://www.ftc.gov)).
- You can file a complaint with the FTC against a company or organization that you believe has cheated you by contacting the Consumer Response Center by phone: toll free 877-FTCHELP (382-4357).

Lastly, please remember: MOREBANK will NEVER e-mail or call you with a request to provide account information, log-in ID, password, Social Security number or other confidential, personal information.

**What to do if you fall victim:**

- Contact MOREBANK immediately to alert us of the situation.
- Contact one of the three major credit bureaus to discuss whether you need to place a fraud alert on your file. This will help to prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:
 

Equifax  
800-525-6285  
PO Box 740250  
Atlanta, GA 30374

Experian  
888-680-7289  
PO Box 1017  
Allen, TX 75013

TransUnion  
800-680-7289  
PO Box 6790  
Fullerton, CA 92634
- Report all suspicious contacts to the Federal Trade Commission at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or by calling 1-877-IDTHEFT.

