



# **ONLINE & BANKING & INTERNET SAFETY**

- What your bank is doing to protect you
- What you can do to safeguard yourself

## Online Banking

### *"The Future Is Now"*

**U**sing the convenience of banking online is one of the major advantages of our new financial technology. In fact, banking online is just as safe and reliable as going to the bank in person. Consider these advantages:

■ **CONVENIENT**—Bank anytime and just about anywhere. As long as you have a computer with an Internet connection, our "online bank" is open 24/7—that's convenience!

■ **SAFE & SECURE**—By banking online, you can actually increase the safety and security of your financial information because you can check your accounts frequently, not just once a month or once a quarter. If someone has illegally accessed your account, you will know it quickly and can take immediate action. Frequent monitoring is the best protection for your personal information.

■ **RELIABLE**—Your online banking transactions offer the same accuracy and reliability as doing business via telephone or through an ATM. You can get real-time balances and immediate transfers between accounts.

Whether conducting online transactions at your bank or simply "surfing" the Internet, common sense precautions can help safeguard your personal information from identity theft and account fraud.

#### **WHAT YOUR BANK IS DOING**

■ **GETTING STARTED**—You must first apply for online banking in order to access your financial information online. Talk to a representative at your bank to learn more.

■ **SECURE AREA**—In order to conduct business such as reviewing your accounts or paying bills with your bank online, you must first enter a secure area on your bank's website. The Internet browser on your home computer must be able to support the level of encryption required by your financial institution's secure online banking system. If your browser cannot support this encryption, you may be required to install a more secure version of your browser.

■ **PASSWORD PROTECTION**—Before using online banking services, you must first create a user I.D. and secret password. This assures that you, and only you, have access to your accounts.

■ **ENCRYPTION**—Once online with your bank, your transactions and personal information are secured by encryption software that converts the information into code readable by only you and your bank.

■ **PRIVACY POLICIES**—Bank privacy policies protecting your personal and financial information are stringent and enforced. Each customer's confidential information is treated with the utmost care, meeting or exceeding federal and state mandates. Your trust is our business.

## **WHAT YOU CAN DO**

There are security procedures that you can follow with your home computer to ensure a safe online banking experience:

### **THE FOLLOWING PROCEDURES SHOULD BE IMPLEMENTED BEFORE ACCESSING ONLINE BANKING.**

■ **ANTI-VIRUS SOFTWARE**—Anti-virus software should be installed on all Internet-connected computers. And because new viruses are emerging daily, it is essential to configure

your anti-virus software to both check for and update your anti-virus signatures daily.

■ **PATCH MANAGEMENT**—Most home computers run an operating system and productivity software created by Microsoft. Home computers connected to the Internet have the ability to check for available patches to fix known exploits in these programs and operating systems. Home computers can also be configured to automatically be notified of new patches, as Microsoft makes them available.

■ **ANTI-SPYWARE SOFTWARE**—The term “spyware” covers a broad category of malicious software designed to intercept or take partial control of a computer’s operating system without the informed consent of that machine’s owner or legitimate user. All home computers connected to the internet should have a reliable program to scan for the presence of spyware on their computers.

■ **FIREWALLS**—A firewall is a protective layer between your computer and the rest of the Internet. There are a number of subscription-based products that are offered (McAfee, Norton, etc. as well as some free products (ZoneAlarm, Microsoft firewall available with Windows XP Service Pack 2, etc.) At a minimum, you should have a software firewall installed on your home computer to prevent an outside intruder from gaining access.

## **USING ONLINE BANKING**

■ **PASSWORDS**—Your password is the key that allows access to your financial information. Don’t use a password that is easy for others to guess e.g. birth dates, social security numbers, mother’s maiden name, child or pet names. Instead, use a password that contains a variety of letters, numbers and

symbols and change it regularly. Do not tape it to your computer monitor and do not file it in your rolodex under "Password."

■ **ENCRYPTION**—If you access your financial accounts through a secure web page with your bank, the information you transmit is almost certainly encrypted. However, email is frequently unencrypted, so even if you access it from a secured web page, be wary of sending sensitive information such as account numbers, passwords and other personal information through email.

■ **DISCONNECT**—Always log off properly after you have completed your online business. Follow the secure area exit instructions to ensure the protection of your financial information.

■ **SPAM WITH VIRUSES**—Before opening emails or attachments, make sure they are free of any viruses or known exploits. The best way to do this is to make sure your anti-virus software is current and scans your email as it is received.

■ **PHISHING**—Fraudsters will design fake websites that use a web address deceptively close to that of a genuine business. Their goal is to lure you into giving them personal information, such as your account number and password. The crooks can then put charges on your credit card, steal from your accounts and even steal your identity. Always ensure that you are really on your bank's website before logging on. When in doubt call your bank.

## **LEARNING MORE**

- Federal Deposit Insurance Corporation  
<http://www.fdic.gov>
- Board of Governors of the Federal Reserve System  
<http://www.federalreserve.gov>

- Office of the Comptroller of the Currency  
<http://www.occ.treas.gov>
- Office of Thrift Supervision  
<http://www.ots.treas.gov>
- Federal Trade Commission  
<http://www.ftc.gov>

### **ANTI-VIRUS RESOURCES**

- McAfee Anti-virus (by Network Associates)  
<http://www.mcafee.com>
- Norton Anti-virus (by Symantec)  
<http://www.symantec.com>

### **FIREWALL RESOURCES**

- ZoneAlarm (by ZoneLabs)  
<http://www.zonelabs.com>

### **ANTI-SPYWARE**

- AdAware (by Lavasoft)  
<http://www.adaware.com>
- Microsoft AntiSpyware  
<http://www.microsoft.com>  
(search on antispyware)



**New Millennium**  
**BANK**  
[www.nmbonline.com](http://www.nmbonline.com)



[www.AmericasCommunityBankers.com](http://www.AmericasCommunityBankers.com)