



# SAFE ONLINE BANKING

- Understanding the threats
- Protecting against account fraud and identity theft
- Securing your Internet transactions

# MAKING ONLINE BANKING SAFE AND SECURE

**W**hen you travel the Internet to access online banking, you want to be assured, first and foremost, that effective safeguards are in place to make your visit safe, secure, and reliable. When you use online banking to visit your bank, whether it's to learn about rates, to review your accounts or to pay your bills, you are entering a secure area. Measures they take include one or more of the following:

## **\* PASSWORD PROTECTION & PIN—**

Your password and PIN (personal identification number) are the first line of defense, and are your unique identifier. Be sure not to share them with anyone—most frauds involving hijacked accounts originate with someone the victim knows.



## **\* MULTI-FACTOR AUTHENTICATION—**

This form of identity verification provides added security by requiring multiple forms of identification, such as something you know (password or PIN) and something you have (ATM card, smart card).

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

✦ **PRIVACY POLICIES**—Bank privacy policies protecting your personal information are stringent. Your confidential information is treated with the utmost care, meeting or exceeding federal and state mandates.

## USING ONLINE BANKING

Whether you are conducting online financial transactions over the Internet or simply “surfing,” some easily implemented precautions can help safeguard your personal information from identity theft and account fraud:



✦ **PASSWORDS**—Security begins with a strong password, which only you, the user, knows. Experts advise a combination of letters and numbers,

## IDENTIFYING THE MOST COMMON ONLINE THREATS

*Understanding what criminals are trying to do over the Internet is the first step in building a good defense.*

Most electronic fraud falls into one of three categories. Experts advise: understand these to understand how best to protect yourself.

✦ **PHISHING**—Fraudulent emails purporting to be from your bank or a similar trusted source lures you to a copy cat website (one that may look just like your bank’s site). Once there you are instructed to “verify” certain personal information, which is then used to hijack your accounts and your identity. If you receive a suspicious email, delete the



message and call your bank to inform them of the email.

✦ **PHARMING**—Also called “domain spoofing,” this cyber crime intercepts Internet traffic and re-routes it to a fraudulent site. Once there, the victim is asked to enter personal information, just as with Phishing.

✦ **MALWARE**—This is software designed to infiltrate or damage a computer system without the owner’s knowledge. Examples of malware (malicious software) include computer viruses, worms, Trojan horses, spyware, and adware.

*See elsewhere in this brochure for tips on protecting yourself...and steps your bank is taking.*

and advise against using easily guessed passwords such as birthdays or home addresses.

**\* ANTI-VIRUS PROTECTION**—Make sure the anti-virus software on your computer is current and scans your email as it is received. This simple step is critical to your personal safety and security when online.

**\* EMAIL COMMUNICATION**—Email is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way. If you receive an unscheduled or unsolicited email purporting to be from your bank be cautious—take the time to call your bank and make sure the email was sent from your banker.



**\* SIGNING OFF**—Always log off by following the bank's secured area exit procedures to ensure the protection of your personal information.

**\* BE AWARE**—Crooks are trying to get your personal information—and they employ some ingenious methods. Don't respond to any unusual requests for personal information—when you opened your bank accounts you already gave it. When in doubt, call your bank.

## LEARNING MORE

Drop by your bank today to learn more about online banking and the security measures that are in place for your protection. Or contact any of these financial industry regulators.

- \* **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>

*Embracing Technology, Preserving Trust*



Presented by the  
American Bankers Association

© FINANCIAL EDUCATION CORPORATION