

SAFE ONLINE BANKING



**Online
Banking,
Data
& Security
You**

**Your Partnership for
Safe Online Banking**

Partnering for Online Security

Online banking has grown rapidly from a niche service to a major new way to bank. In fact, some surveys show that far more people prefer to bank online than in the traditional ways. This phenomenal growth was made possible by increases in technology, of course, but even more so by increases in the *safety and security measures undertaken by banks and their customers*. This **partnership for safe online banking** means that you can access your account whenever and wherever you want. But care should be taken because cyber-criminals are always looking for new ways to electronically break into the bank and steal your money.

Safe online banking depends *on continuing and strengthening this safe online partnership*:

◆ THE BANK'S ROLE

Banks Invest Substantially in Security Technology and Training

Lawmakers, regulators and the banking industry have forged substantive standards for safeguarding customers' "nonpublic personal information." Security programs developed from these standards are designed to

- **Ensure the security and confidentiality** of customer information
- **Protect against any anticipated threats** to the security of customer information
- **Protect against unauthorized access** that would result in substantial harm or inconvenience to any customer.

Uniform examination procedures are in place to monitor and enforce these standards, and bank examiners regularly go on-site to assess how

bank security measures are being implemented, understanding that each bank has a different menu of products and services, and therefore differing security requirements. For example, a federal regulator will typically review a bank's internal controls and policies, with a view to establishing whether the institution considered the following controls, and adopted those it considered appropriate:

- **Access controls** ensuring customer information can be accessed only by authorized persons.
- **Physical restrictions** and computer facilities that permit access to authorized persons only.
- **Data Encryption** of electronically transmitted and stored customer information
- **Modification procedures** to ensure that changes are consistent with the approved security program.
- **Dual control procedures**, segregation of duties, and employee background checks.
- **Monitoring procedures** to detect actual and attempted intrusions into customer information.
- **Response programs** specifying actions to be taken by specific individuals when the institution suspects unauthorized access.

- **Environmental hazard protections** against physical damage or technology failures.

◆ THE CUSTOMER'S ROLE

Banks Partner With You, the Customer

Your bank has security measures to protect your account information, but they can't be effective without your help and cooperation. After all, the gold in Fort Knox won't be safe if someone leaves the back door open! And that's an analogy that works for your computer—many account hijacking attempts come as a result of hacking into individual user accounts, and from there electronically breaking into the bank using your information and security codes!

Some common sense and easily implemented precautions can help you safeguard your personal information from identity theft and account fraud:

- **Strong Passwords**—Security begins with a strong password, which only you know. Experts advise a combination of letters and numbers, and advise against using easily guessed passwords such as birthdays or home addresses.

IDENTIFYING THE MOST COMMON ONLINE THREATS

Understanding what criminals are trying to do over the Internet is the first step to 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.

- **Anti-Virus Protections**—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 Safety**—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.
- **Sign Off and Log Out**—Always log off by following the bank's secured area exit procedures to ensure the protection of your personal information.
- **Don't Get Phished**—Crooks are always trying to get your personal information, and they employ some ingenious methods. Don't respond to any unusual email requests for personal information—when you opened your bank accounts you already gave it. When in doubt, call your bank.
- **Monitor Your Accounts**—When you check your accounts regularly, you can let your bank know immediately if you encounter anything that does not seem right. Doing this has the added benefit of keeping you aware of recurrent transactions going through your account for services you no longer use, such as a gym membership or club.

◆ **RECOMMENDATIONS FOR BUSINESS CAN BE EFFECTIVE FOR CONSUMERS, TOO**

Some bank security experts now recommend that businesses use a dedicated computer for online transactions. This advice can be weighed against the convenience and cost savings of having access to online banking, versus time spent on the phone

or traveling to and from a bank to conduct your business, say these experts. Several guidelines for businesses might also work well for you, too:

■ **Email Confirmations**

See if your bank can send email confirmations of online transactions to provide you with an early warning of any fraudulent activity.

■ **End of Day Balances**

Automated Clearing House (ACH) transactions are not usually completed until the next business day. If you catch a fraudulent transaction at the end of a business day, you may be able to cancel it before any funds are transferred.

■ **Don't "Friend" Strangers**

Beware of "friending" strangers on social networking sites, because they could be scammers. Scammers know that your guard goes down when you are on Facebook, Myspace, etc.