



ELECTRONIC BANKING & ONLINE AUTHENTICATION

- **How Internet fraudsters are trying to trick you**
- **What you can do to stop them**
- **How *multi-factor authentication* and other new techniques can help**

HELPING YOU STAY SAFE ONLINE

Your community bank, along with the banking industry, recognizes that as the electronic financial world gets more complex, online fraudsters become more sophisticated as well. In response, the banking industry has taken a comprehensive approach to meeting this growing threat.

The first step involved a complete “risk assessment” of current electronic security measures. From this assessment came two objectives:

- **Educate customers** about the current electronic banking threats so they can understand the risks and take measures to protect themselves.
- **Implement new authentication methods** where appropriate to help assure customers’ online security.

IDENTIFYING THE THREATS

Most electronic fraud falls into one of three categories:

Phishing—Fraudulent e-mails, appearing to be from a trusted source such as your bank, direct you to websites. Once there, you are asked to verify personal information such as name, account and credit card numbers, passwords and the like. These sites are often designed to look exactly like the site they are imitating. The information you provide is used to hijack your accounts and your identity. E-mails that warn you, with little or no notice, that your account will be shut down unless you reconfirm certain information, are very

likely to be phishing. Delete the message and use a phone number or website address you know to be legitimate to check the source.

Pharming—or “domain spoofing” is an attack in which a user can be redirected from a legitimate site to a fraudulent site and then fooled into entering sensitive data such as a password or credit card number. The fraudulent site often looks like the legitimate site (e.g., your bank). It is different from **phishing** in that the attacker does not have to rely on having the user click a link in an email

to deceive the user—even if the user correctly enters a web address into a browser’s address bar, the attacker can still redirect the user to a malicious web site.

Malware— is software designed to infiltrate or damage a computer system without the owner’s knowledge or consent. It is a **blend** of the words “**malicious**” and “**software**.” It includes **computer viruses, worms, trojan horses, spyware, adware**, and other malicious and unwanted software.

Understanding MULTI-FACTOR AUTHENTICATION

New ways to verify identities should make web banking safer than ever

Your bank wants to be sure that the level of authentication (i.e., the way you identify yourself and the security measures you employ) in a particular transaction is appropriate to the level of risk in that application. As a result, you might begin to experience some changes in how you identify yourself and gain access to your accounts over the internet. These **authentication changes** will help make you safer than ever before from account hijacking and identity theft.

Today’s authentication methods involve one or more basic “factors”:

- Something the user **knows** (e.g., password, PIN)
- Something the user **has** (e.g., ATM card, smart card)
- Something the user **is** (e.g., biometric characteristic, such as a fingerprint)

Single-factor authentication uses **one** of these methods; **multi-factor** authentication uses **more than one**. When you log on with a password, you are using single-factor authentication; when you use your ATM, you are using multi-factor authentication: Factor number one is something you have, your ATM card; factor number two is something you know, your PIN.

In addition to single and multi-factor authentication, your bank may also rely on several **layers of control** to assure your Internet safety. These layers might include

- Utilizing multiple verification procedures, especially when opening accounts online.
- Searching suspicious patterns in banking transactions.
- Establishing dollar limits that require manual intervention to exceed a preset limit.
- Other methods that allow your bank to establish appropriate security levels for the transactions you are conducting.

Regardless of the types of authentication employed, you can be assured that your bank is working to make your online transactions safer and more convenient than ever before.

DEFENDING AGAINST FRAUD

While no defense can protect against every threat, you can enhance your security online with some healthy skepticism:

- **Don't Judge by Initial Appearances.** The ready availability of software means that criminals can make their Web sites look just like a legitimate business.
- **Safeguard Your Personal Data Online.** If you receive e-mails from someone you don't know asking for personal data – don't send the data without knowing more about who's asking.
- **Watch out for Phishing.** Be suspicious of any unsolicited email requesting personal information. Remember: your bank will never ask you to click on a link and go to a site to “verify” or enter personal information. When in doubt, log on to the official website instead of “linking” to it from an unsolicited email.
- **Be Wary of unsolicited emails.** An e-mail using a mail header that has no useful identifying data can be an indication that the person is hiding something. Contact the actual business that supposedly sent the email to verify that the email is genuine.

RESOURCES

The following links can help you find useful information and guidance:

- **Department of Justice**
www.usdoj.gov/criminal/fraud/idtheft.html
Learn about identity theft and other frauds.

■ **Internet Crime Complaint Center**

<http://www.ic3.gov>

Allows consumers to report Internet fraud.

■ **Federal Trade Commission**

www.consumer.gov/idtheft/

You can file a complaint with the FTC against a company or organization that you believe has cheated you.

■ **FirstGov**

www.usa.gov

A centralized place to find information from local, state, and U.S. Government Agency websites.

■ **Identity Theft Resource Center**

www.idtheftcenter.org

A non-profit organization with many resources to assist identity theft victims.

Embracing Technology, Preserving Trust



Presented by the
American Bankers Association

© FINANCIAL EDUCATION CORPORATION