



## Tips for Banking Safely Online

Is banking online safe? It can be as long as you take a few simple precautions.

### **Know who you are doing business with**

Online banking is missing the visual cues people are accustomed to when visiting their bank in the real world. They drive to their bank, go to a teller or an ATM, and conduct their business. Online, fraudsters can easily impersonate a bank—it is virtually free to send an email, set up a fake Web site, and collect personal information from unsuspecting victims.

Consumers must use different means to help make sure the financial institution is legitimate and it's safe to transact:

- Banks should not solicit you for passwords, account numbers, or other personal information—if you get an email like this; call them using the number on your statement or credit card, not the one in the email.
- Access the online banking Web site by typing the URL into the address bar, rather than clicking links you might see in an email in an instant message, or on another Web site.
- Always check for the browser "lock" icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate Web site.
- Check for anything that looks unfamiliar, unprofessional, or out of place to you.

### **Secure your PC**

On any PC you use for online banking or commerce:

- Maintain active, up-to-date antivirus, spyware, and firewall protection.
- Keep your operating system (for example, Windows® XP), browser (for example, Internet Explorer), and other applications (such as RealPlayer or iTunes) updated with the latest security patches.
- Avoid transactions at wireless hot spots or Internet cafés.

Never respond to an email, instant message, or phone call asking you to go to a Web site to resolve an account problem. This is called "phishing," a form of identity theft that depends entirely upon the victim's cooperation. These requests are NEVER legitimate.

### **Password protection**

- Use a strong password—at least eight characters, with a combination of numbers, letters, and punctuation symbols.
- Don't use the same password for banking that you use for other online accounts.

- Keep your password safe—don't leave it in a file on your computer or in a sticky note on your monitor.
- Change your password periodically.

### **Practice physical security**

Personal identification data is more likely to be stolen physically than online. Take these precautions:

- Guard your PIN number.
- Secure your mailbox.
- Shred any documents that contain identifying information before disposing of them.
- Don't leave credit cards, bank statements, checks, or other financial documents where service workers can find them.
- Ask your bank and credit card companies not to send you unsolicited checks, credit cards, or credit applications.

### **Check your statements**

Online banking can actually help you protect your identity—log in and check your financial statements regularly. Report unauthorized transactions immediately. Check your free annual credit report to spot accounts that may have been opened without your knowledge.

### **Learning the Lingo**

**Trojans:** Programs that perform malicious actions but have no replication abilities. Like the original Trojan horse, these programs may arrive as seemingly harmless files or applications, but actually have malicious intent within their code. Banking Trojans are specifically designed to gain control and compromise online accounts.

**Phishing:** A form of identity theft in which a scammer uses an authentic-looking e-mail to trick recipients into giving out sensitive personal information, such as a credit card numbers, bank account numbers, Social Security numbers or other sensitive personal information.

**Site spoofing:** Websites that appear professionally designed and legitimate with the purpose of collecting sensitive information from unsuspecting visitors.