



## *Personal Safety Tips For* **ONLINE BANKING**

### **1**

#### *Get Serious About Passwords*

- **Storage:** Passwords should be stored safely. Don't use an open file on your computer! There are good password vaults, but do your homework to make sure it is a trusted one. This way, you don't have to remember all your passwords.
- **Mix it up:** Don't use the same password for all your accounts – doing so leaves you more vulnerable.
- **Don't use your dog or other family names:** Create a "strong" password with at least 8 characters that includes a combination of mixed case letters, numbers, and special characters. Choosing passwords just because they are the easy to remember leads to weaker passwords!
- **Don't put personal information, like a Social Security number, into a password.** Keep personal numbers to yourself whenever possible, even in secret passwords. That might be the first thing a hacker tries.

### **2**

#### *Be Careful How & When You Use Online Banking*

- Would you use the dark back alley to get into a business? No! You'd go through the well-lit, safe front door. Do the same on the internet. Don't access your online financial information while using an unsecured public Wi-Fi.
- Don't access your account from a link – always go to the bank's website. Links are easy to spoof, especially if they are in an email or text message, or in an online article. Always go directly to the homepage of the financial institution first, and navigate to Online Banking from there.
- Use the same computer each time, if possible. This increases your security.
- When you're done, log out of Online Banking. Don't leave your computer logged in when you walk away. That sounds obvious, but a lot of people forget.
- Close all your other browser windows. It's safer to only have Online Banking open when you are using it.

### 3

#### *Monitor Your Account – Manually & Automatically*

- **Watch your account like a hawk.** The best way to protect yourself is to monitor your account. Review your transactions frequently, even every day if you can. The sooner you identify a problem, the sooner you can protect yourself from problems.
- **Let the bank monitor things as well.** Look over the account alerts that are available through Online Banking. Set up an alert for the system to send you a text message or email if your balance reaches a certain threshold. Look through all the alert message types and find the right combination to keep you informed.

### 4

#### *Don't Skimp on Protecting Your Equipment*

- **Get good anti-virus and firewall software.** Most people dislike it when their computer stops to download new virus protections, but this is important. Before you purchase one, consider looking at a website from your operating system vendor. Microsoft has some free protection programs for Windows. Apple has protections as well. But the bottom line is, you really need to be protected.
- **Set your protection levels at medium or higher.** Most operating systems have built in security levels. Sure, it's easier to have your computer wide open, but you are wide open to big problems when you do this.
- **Lock down your Wi-Fi.** If you have a home Wi-Fi, you absolutely need to put the protections on and not leave it open to the public. We can't stress this enough. Yes, you have to read the directions that come with your wireless router! But it's worth it. Once you set it up, you won't have to log in again, you connect automatically. By putting in a password, you will prevent someone from parking in front of your house and getting access to your computers. Oh, and don't use the factory password – change it. WPA encryption is best; WEP should only be used if WPA is not available.

### 5

#### *Get Familiar with Consumer Protection Laws*

“**Regulation E**” outlines protections that help consumers avoid losses from fraud. The bank can print off a full copy, or you can find it on [www.fdic.gov](http://www.fdic.gov). The most important thing to understand is that you can avoid losses from many types of electronic fraud if you tell the bank early enough. Provisions of protection may no longer be enforced after 60 days, but protection doesn't completely run out for individuals. Businesses are not covered by Regulation E, so they don't even have this leeway. **The key is this:** check your account often and notify the bank immediately if you see a suspicious transaction.

### 6

#### *When In Doubt (Even Just A Little), Call Us.*

If you have any suspicions, or questions about transactions, please call us immediately. The sooner we know about it, the better able we will be to help you and protect you.

**Customer Service Center:** (207) 839-4796 or (800) 492-8120  
Monday – Friday 7:30am – 5pm; Saturday 7:30am – 12pm

**For all other hours, please call:**  
ATM/Debit Cards (800) 500-1044  
Credit Cards (800) 883-0131