



The Internet offers the potential for a safe and convenient way to conduct your banking, any day, any time. However, safe banking online involves making good choices – decisions that will help you avoid costly surprises or even scams.

### ***Tips to Protect Your Account Online:***

#### **Check your Account History Regularly**

Consumers have protections under Federal Regulation (Reg E). In order to maximize your protection, contact us immediately as soon as you learn of fraudulent activity. For questions or concerns about your account, please visit a branch location or contact our Customer Care Department at 866.378.9500.

There are specific time frames for reporting fraudulent transactions. You were provided a full description of your rights under Reg E in the Terms and Conditions provided upon your enrollment to Online Banking. If you would like to obtain an additional copy, we will be happy to provide it to you.

#### **Setup Email or Text Alerts**

You can also use Online Banking to set up alerts to inform you of activity on your account. We will send you an email or text alert when the conditions you described occur on your account. There are a variety of alert types and choices of conditions for you to select from. For example, you can select Balance Alerts, Transfer Alerts and Transaction Alerts. Choose the condition under which you would like to be alerted, and you'll receive a text or email if that condition ever occurs on your account.

#### **Type your internet banking URL**

Always access our Online Banking by typing the correct URL, [www.bankoftennessee.com](http://www.bankoftennessee.com), into your browser or save it to your favorites. Never click on a link in an email to take you to a different website or enter personal details either in an email or unknown unsecured website.

#### **Password and PIN Security**

You should always be wary if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. We will never send you an email asking for your online banking credentials, card numbers/PINs, Social Security Number or any other personal information.



### **Your Mother Was Right . . . It Can Be Too Good**

If it sounds too good to be true, it probably is. Emails that offer you a chance to make “easy money by working at home” or informing you of an inheritance, lottery win or other financial windfall are all common schemes used by online criminals to scam you. Avoid replying to these emails.

### **PC Security**

It is important that you install anti-virus software that is updated regularly. Similarly, update your operating system and other software packages as you receive notices. These updates are generated due to new online vulnerabilities in the software and the updates have new protections that are important to keep you from being at risk of obtaining a virus or other malware on your system. Never use online banking over a public Wi-Fi or unprotected network.

### **Secure Connections**

When you are in an online banking session, there are a couple of ways you can verify that you have a secure connection:

- The URL will include “https://”. If you don’t see the “s”, you are not on a secure website.
- You may see a key or padlock to the right of the URL. You can click on this icon and verify the validity of the website owner and their digital certificate.

### **Ensure You Log Off**

When you have completed your online banking session, be sure to log off. Simply closing the internet window may not close your session. If your computer has been infected with certain malware known as a “Trojan”, your session can be hijacked remotely by criminals who can perform fraudulent transactions on your account.

### **Educate Your Family and Other Users**

Anyone who uses your computer can fall prey to online hackers and put your personal information at risk. Be sure that all members of your family, especially children, are educated on how to surf safely. You might consider looking into Parental Control Software for additional safety.

### **Learn More**

You can learn more about identity theft at the following online resources:

[www.ftc.gov/infosecurity](http://www.ftc.gov/infosecurity)  
[www.OnGuardOnline.gov](http://www.OnGuardOnline.gov)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)