Computer, Online, Smartphone and Email Security Tips

Below are some tips and suggestions to assist in keeping your online accounts and transactions secure.

COMPUTER SECURITY TIPS

COMPUTER SECURITY IS THE FIRST LINE OF DEFENSE AGAINST CYBERCRIME.

- Keep your Operating System and all applications updated and patched.
- Protect your computer with security suite software.

Suggested Features for Security Suite Software	
Antivirus Antispyware	Firewall Password Protection

- Turn off your computer when not in use for long periods of time, such as at night; not only will you save energy, but you will lessen the possibility of your computer being maliciously accessed.
- Control physical access to your computer to prevent unauthorized software installations and access to personal information.
- Use screen locking features within the operating system to prevent unauthorized access to system.
- To assist in keeping software current on your PC, Secunia offers free software to notify you when updates are available for computer. Click here to view Secunia.
- If Security Suite or antivirus software is not already installed, Microsoft offers free security software called Security Essentials which offers antivirus, antispyware, and other malicious software protection. Click here to view Security Essentials.

SMARTPHONE SECURITY TIPS

SMARTPHONE (IPHONE, BLACKBERRY, ETC) TIPS TO PROTECT YOUR INFORMATION

- Install Smartphone security software.

Suggested Features for Security Suite Software	
Antivirus Antispyware	Firewall Password Protection

- Use the keypad or phone lock functions available on your mobile device. The locking function should occur after at least five minutes of inactivity or when holstering.
- Encrypt your data on your mobile device. For example, Blackberry offers content protection that encrypts the device.
- Turn off Bluetooth when not in use.
- Download and install software from trusted sources only.

Computer, Online, Smartphone and Email Security Tips

EMAIL SECURITY TIPS

FOLLOWING THE BELOW TIPS CAN HELP PREVENT INFORMATION FROM GETTING INTO THE WRONG HANDS.

- Be suspicious of any email that appears from a reputable business, **but that you did not request or have a prior business relationship**. Fraudsters use email links to divert customers to fraudulent or malicious websites. If you desire to find out more about a company's products or services, do a search using Google, Yahoo, or BING for the company's website. Even if the e-mail appears to be from a company with which you are familiar, don't click through links within the e-mail. Go through the browser to access their website.
- Be suspicious of emails containing:
  - Bad grammar
  - Misspelled words
  - Awkward greetings (Does not mention your name specifically or incorrect title)
  - Strange links
  - Urgent language (Such as, click link immediately to prevent loss)
- Do not send your personal information in an email unless you are using email encryption.
- Do not open attachments from unknown senders.
- Submitting your email address on questionable website forms could produce more fraudulent email activity.
- Use caution opening attachments. Look for the following:

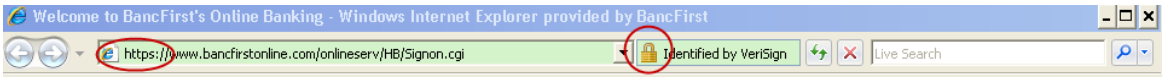
Suspicious Attachment Characteristics	Action
Attachments with two extensions, such as readme.**doc.exe** or familyphoto.**jpg.vbs**	Do not open and delete email
Attachments that have file extensions with .exe, .vbs, and .com. These extension are executable and can be used in emails to carry malicious software	Do not open and delete email

Computer, Online, Smartphone and Email Security Tips

ONLINE SECURITY TIPS

BELOW ARE HELPFUL GUIDELINES TO USE WHEN SHOPPING OR BANKING ONLINE.

- Use current and up-to-date web browsers. New technology has been added to web browsers to help thwart fraudulent websites.
- Protect your passwords and security question answers by:
  - not sharing them with anyone
  - making the password difficult to guess
  - not using the same password or security question answers for every website account
- Shop and bank at websites that use encryption to transfer your information. To identify these sites, look for :
  - An "S" after the http in the address bar of the browser - HTTP**S**://
  - A lock icon should appear on the browser either on the top near the address bar or on the bottom of the web browser.
  - Some browsers will turn the address bar green for sites with enhanced security, such as www.bancfirst.com.



- Logoff from online banking or merchant sites when session is complete.
- Never provide sensitive information, such as username, password, Social Security Number or other identifiable information, unless you have initiated a connection with a website and the page is secure.
- Follow alerts and warnings received by the browser. For example, if your browser reports that the site is a known phishing site, then do not continue to the site and type in your information.
- Change passwords at regular intervals for all online sites, such as online banking, merchant sites, and email accounts.
- Close web browser when not in use.
- Trusteer offers free software to help protect online activity from malicious software. Click here to view Trusteer.

Additional Information About Protecting Your Computer

Video created for the FDIC about identity theft and online activities:
http://edgecastcdn.net/00003F/anon.vodium/fdic/identitytheft/fdic_player.swf
Practical security tips from the federal government includes security tips, security games, and security videos:
http://www.onguardonline.gov/
http://edgecastcdn.net/00003F/anon.vodium/fdic/identitytheft/docs/stop_think_click.pdf
http://www.fdic.gov/consumers/consumer/news/cnwin0910/online_banking.html
Computer security tips from New York state fraud advisory
https://www.bancfirst.com/pdfs/Wire-transfer-fraud-recommendations-2010.pdf
OS specific security tips and instructions: XP, Vista, Windows 7.