Digital Banking Business Protection Tips

BANK
NEWPORT®

© 2019 BankNewport All rights reserved.

Additional Security Procedures

In addition to the Security Provisions provided for in the bank's Digital Banking and Mobile Banking Terms and Conditions Agreements, BankNewport advises that the following controls are put in place to strengthen controls and to mitigate the risks associated with Digital Banking and Mobile Banking access. Any elections you make to change or waive security procedures recommended by us are at your own risk.

User Access Reviews by Company System Administrator

It is suggested that your company System Administrator perform a related risk assessment and controls evaluation periodically. This consists, in part, of User Access Reviews to determine that staff given access to business Digital Banking has appropriate levels of access; and a review of actual access and transactions that users may have conducted over the period being reviewed. Never allow users to share a common UserId. Users should always use secure passwords. A secure password consists of upper and lower case letters, numbers and special characters.

It is suggested that whenever possible, business customers implement dual control routines over higher risk functions that employees are allowed to perform online.

Determine which websites need to be made available to employees in order to conduct business activities. Consider blocking access to file sharing, social media and personal email sites.

Dedicate a computer to be used solely for all online banking activities. If that is not feasible, restrict the use of personal web browsing, emailing and social networking on any computer used for online banking activities. If you need assistance restricting the IP address, you may contact our Digital Banking Center by calling 401.845.8616 or toll free at 877.709.2265 (option 4) outside the Newport County area, Monday through Friday between the hours of 8:00 a.m. and 4:30 p.m. and Saturday between 9:00 a.m. and 12:00 p.m.

Firewall

A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings. A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers. Even if you think there is nothing on your computer that would interest anyone, a worm could completely disable your computer, or someone could use your computer to help spread worms or viruses to other computers without your knowledge.

A firewall cannot prevent:

- **Email viruses –** Email viruses are attached to email messages. A firewall can't determine the contents of email, so it can't protect you from these types of viruses. You should use an antivirus program to scan and delete suspicious attachments from an email before you open it. Even when you have an antivirus program, you should not open an email attachment if you're not positive it's safe. If you have any doubts about the authenticity of an email, attach any suspicious email you may receive to a new email and send them to abuse@banknewport.com. Then, be sure to delete the suspicious emails from your mailbox. Do not open the email or click on links or attachments, especially if they tell you the problem is urgent.

© 2019 BankNewport All rights reserved.

- **Phishing scams –** Phishing is a technique used to trick computer users into revealing personal or financial information, such as a bank account password. A common online phishing scam starts with an email message that appears to come from a trusted source but actually directs recipients to provide information to a fraudulent website. As discussed above, firewalls can't determine the contents of email, so they can't protect you from this type of attack.

Anti-virus Software Updates

Anti-virus software is protective software designed to defend your computer against malicious software. Malicious software or "malware" includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents. **In order to be an effective defense, your antivirus software needs to run in the background at all times, and should be kept updated so it recognizes new versions of malicious software.**

Keep your computer's operating system and your web browser software up to date by installing the most recent version. Consider disabling CD, DVD and USB drives on all computers where these drives are not needed.

Patch Updates

A patch is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. It is suggested that your company System Administrator adopt a patch management strategy. Windows patches can be set to automatically download and install or they can be manually done.

To protect your phone:

No matter what kind of mobile banking method you use, reduce fraud and protect your money by following a few common-sense precautions:

Keep your phone's operating system up to date by installing the most recent version.

- Mobile devices are actually small computers with software that you need to update just like on a PC or laptop. Make sure all your mobile devices (including laptops, tablets, and smartphones) have the latest security protection. Check the website of your device's manufacturer or mobile carrier for the latest software updates.

Guard your Personal Information

- Protect your phone or tablet device just as you would your computer. Set the phone to require a password to power on the device or unlock it. Use bio-metrics if available, and be cautious about the sites you visit and the information you release.
- Whether you're using the mobile Web or a mobile app, don't let it automatically log you in to your bank account. Otherwise, if your phone is lost or stolen, someone will have free access to your money. Some programs can store sensitive information on the phone itself and can allow the user to remain logged in for extended periods of time. This can be hazardous if a lost phone ends up in the wrong hands. If you use such an application, disable these options if possible.

© 2019 BankNewport All rights reserved.

- Avoid sharing your password, account number, PIN, answers to secret questions or other such information. Don't save this information anywhere on your handset. Immediately tell BankNewport or your mobile operator if you lose your phone.
- Mobile phones and tablets are equipped with a remote wipe to clear all content on your device if it were to be stolen.

Protect your Money

- When banking and shopping on your mobile device, check to be sure the sites are secure. Look for web addresses with https: in the address. This means the site takes extra measures to help secure your information. Many sites now feature a color-coded browser. If you see a green highlighted browser, this is a safe site. However, yellow and red sites should be avoided.

When in doubt, don't respond

- Fraudulent texting, calling and voicemails are on the rise. Just like in fraudulent email, requests for personal information or a call for immediate action are almost always a scam.

Think before you download an App

- Before you download an app on your device, review the privacy policy and understand what specific data the app can access. Only download apps from reputable sources.

Stay informed

- Follow mobile security issues in the news and discuss them with friends, family and colleagues. Explore online resources that provide comprehensive information about topics such as identity theft and safe online behavior.

© 2019 BankNewport All rights reserved.

Member FDIC

© 2019 BankNewport All rights reserved. v.10-29-19