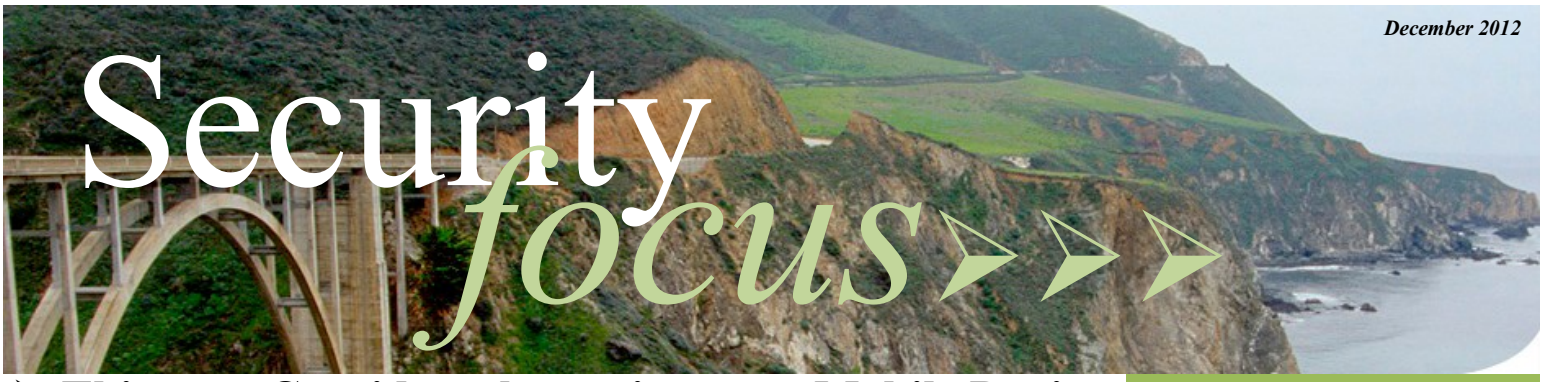

December 2012

Security focus

➢ Things to Consider when using your Mobile Device

With the ever-increasing usage of smart phones and mobile devices, users must learn to take extra pre-caution in addition to the standard safety measures of a personal computer when handling personal and account information in an electronic environment. As many Financial Institutions begin to enter the world of Mobile Banking and consumers become more dependent on the convenience of accessing or storing personal information on their mobile devices, security experts are noticing a rising trend in mobile malware attacks, thus, also increasing the potential risk for consumer identity theft and financial fraud.

➢ The DO's and DON'Ts

The Federal Bureau of Investigation has released the following safety guidelines to help mobile users minimize their potential risk exposure and protect their mobile devices.

1. When purchasing a smartphone, know the features of the device, including the default settings. Turn off features of the device not needed, to minimize the attack surface of the device.
2. Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft.
3. With the growth of the application market for mobile devices, users should look at the reviews of the developer/company who published the application.
4. Review and understand the permissions you are giving when you download applications.
5. Passcode protect your mobile device. This is the first layer of physical security to protect the contents of the device. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
6. Obtain malware protection for your mobile device. Look for applications that specialize in anti-virus or file integrity that helps protect your device from rogue applications and malware.
7. Be aware of applications that enable geo-location. The application will track the user's location anywhere. This application can be used for marketing, but can also be used by malicious actors, raising concerns of assisting a possible stalker and/or burglaries.
8. Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime an application or service runs in "unrestricted" or "system" level within an operation system, it allows any compromise to take full control of the device.
9. Do not allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
10. If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
11. Smartphones require updates to run applications and firmware. If users neglect this, it increases the risk of having their device hacked or compromised.
12. Avoid clicking on or otherwise downloading software or links from unknown sources.
13. Use the same precautions on your mobile phone as you would on your computer when using the Internet.

➢ Your BANK working for YOU

Please rest assured Monterey County Bank is taking extra precautions to maintain your identity and secure your personal information by taking additional steps to validate account requests received in a non-face-to-face manner. Please know we are implementing these measures for additional security of your account. We will continue to work on your behalf to reduce identity theft and account fraud.

If you have any questions or concerns regarding your account please stop by or contact your local branch for additional assistance.
Lobby hours are Monday - Thursday, 9:00am - 4:00pm (PST) and Friday, 9:00am - 6:00pm (PST).

For questions regarding Internet Banking please contact our Merchant Services Department at:
(831) 625-2345 during regular business hours: Monday - Friday, 8:00am - 5:00pm (PST).

Visit our website at: **www.montereycountybank.com** for important bank news and consumer alerts.

FBI Warning to Consumers

The following Mobile Malware Trojans have been reported in a recent FBI Consumer Alert released in October 2012.

➢ **Loozfon:**
Steals a mobile user's phone number and address book information by luring the consumer to fraudulent links and websites where the malware is installed to the device unknowingly.

➢ **FinFisher:**
Is a spyware which grants thieves access and control of the compromised device, thus allowing thieves to monitor the user's activity and steal personal information.

➢ **For additional information**
Visit the FBI's Internet Crime Complaint Center (IC3) at: **www.ic3.gov**
Or for the latest e-scam news and consumer alerts issued by the FBI visit:
www.fbi.gov/scams-safety/e-scams

MONTEREY COUNTY BANK
The Business Bank

Monterey County Bank is the oldest locally owned, locally managed bank servicing the Monterey County for over 35 years with locations in:

Monterey
601 Munras Avenue
Monterey, CA 93940
(P): 831-649-4600

Carmel Rancho
3785 Via Nona Marie
Carmel, CA 93923
(P): 831-625-4300

Pacific Grove
542 Lighthouse Avenue
Pacific Grove, CA 93950
(P): 831-655-4300

Salinas
1127 South Main Street
Salinas, CA 93901
(P): 831-422-4600