November 2012

Security focus

The rising incidences of Identity Theft and Account Compromises are a major concern for all participants in the banking industry. Becoming more prevalent are cases of theft due to online scams. As a direct result of these thefts, consumers and financial institutions suffer fraud losses, unanticipated operational expenses, and consumers are inconvenienced significantly. The following information is provided to enhance your awareness, minimize potential risk, and protect you and your personal account information.

➢ The ATTACK of the CITADEL TROJAN

Cybersecurity experts are becoming more aware and familiar with a wide-spreading computer virus known as Citadel. The Citadel Trojan is an advanced Malware virus specifically designed to infect a computer and track Internet Banking login access ID and password credentials by tracking a user's keystrokes. The thieves utilize the stolen credentials to gain access to financial account information online as well as process unauthorized transfers or transactions from the account. The Citadel Trojan has been gaining ground since it first debuted in January 2012.

In August 2012, the Federal Bureau of Investigation issued a public warning to advise of a Citadel Trojan attack containing highly developed ransomware. The user is re-directed to a web-site where the ransomware is unknowingly installed on the computer causing it to lock and freeze from further use. A warning notification is displayed claiming that the FBI has logged the computer's IP address and that the user has violated a United States federal law. The user is then directed to pay a fine to the Department of Justice via a fraudulent money card service in order to have their computer unlocked. During this attempt to extort money, the Citadel continues to run in the background collecting personal and financial information although the computer is locked.

➢ The DO's and DON'Ts

DO	Keep your anti-virus software up to date and run full system scans on a regular basis.
DO	Have a computer expert evaluate your computer if it has been infected to ensure the Malware and all of it's components are fully removed properly.
DO	If your infected computer is connected to other computers via a Network, disconnect from the network to prevent the virus from spreading to other systems.
DO	File a complaint with the FBI's Internet Crime Complaint Center (IC3) if you have been a victim on online fraud. Visit www.IC3.gov for additional information.
DON'T	Pay money or provide personal/financial information to unknown sources.
DON'T	Assume that if you are able to unlock/unfreeze your computer yourself, that your computer is safe. Spyware may still be running in the background gathering information.

➢ 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.

COMMON FORMS OF MALWARE TO BE AWARE OF…

- **What is Malware?**
  Harmful programs that install & infect computers that are designed to corrupt systems & steal personal or account information.
- **Trojan:**
  A program designed to imitate a legitimate computer file or program that grants thieves access to computer information when installed.
- **Ransomware:**
  Restricts a user from accessing their system. It may claim the user was involved in illegal online activities & are required to pay a fine prior to regaining access to their system.
- **Spyware:**
  Installs to a computer undetected with no immediate effect. The program is designed to gather user information that is sent back to the hacker.

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