SEPTEMBER 2016

Security focus

- **Stop**.....Stop and consider the risks associated with using the Internet, as well as the steps to identifying potential threats, before going online.
- **Think**.....Slow down and watch for warning signs; and always consider your online activity and how it impacts your safety.
- **Connect**.....Take the right steps and follow security best practices to protect yourself, enjoy the Internet, and keep the web secure for everyone.

CYBER SECURITY : BEST PRACTICES

EMAIL MALWARE
The most common way to spread malware today is through email. Do not open email from people or a source you do not know and are not expecting. Delete spam email without opening it.

PHISHING EMAILS
Phishing emails will try to convince users into clicking on a link within the email. The link will take the user to a website that will either try to make the user manually install malware or will perform a “drive-by” download to install the malware.

MEDIA PLAYERS
A popular source of malware is a website media player download. When a user wants to play a video, the website will ask to install a video codec or other required software. No matter how enticing the video, only install media software from trusted websites such as Apple.com, Microsoft.com, or Adobe.com.

EMAIL ATTACHMENTS
One of the oldest ways to spread malware is through email attachments. Do not open attachments from people you do not know. If a friend sends you an attachment that looks suspicious, contact them first to confirm the validity before opening the attachment. Never open unknown email attachments that end in .exe, .bat, .com, or .vbs.

WEBSITE ADS
Many ads are designed to persuade the user to click on the ad or to click on a Close button in the ad. When the user clicks on the ad or Close button, a “drive-by” download is initiated and malware is installed. Do not click on advertisements or Close buttons. Instead, close the window through the (X) in the upper right corner of the window.

SOCIAL ENGINEERING PHONE CALLS
Hackers may try to extract usernames and passwords and other confidential information by posing as an IT or service person via phone that needs access to your computer for the purpose of maintenance or service. Never give out your username, password or other confidential information over the phone to any person you do not know.

EMAIL CREDENTIALS
Use different email addresses for various types of logins. Create different passwords for each. Example, use one email for your online banking and a separate email for social media sites. Do not use business email addresses for personal logins or vice versa.

DRIVE-BY DOWNLOADS
When visiting websites, data on the site can secretly process and install malware. Avoid suspicious websites. Make sure your anti-virus, operating system, and web browser is up-to-date.

FREE GAMES AND APPLICATIONS
Many free applications and games are simply vehicles designed to install malware. Even if the application itself is functional, malware may still be installed on your computer. Only download applications from trusted websites.

SPEAR PHISHING EMAILS
Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, usernames, passwords, and the financial information on your computer. Spear phishers use publicly available information to trick people into giving away confidential information that can be used to compromise your computer and network.

WEBSITE POPUP ALERTS
Web Popup alerts falsely tell the user that their machine is infected with a virus or has some other problem that needs to be fixed. The user will click on the alert and either be asked to install the software (really malware in disguise) that is purported to fix the problem or a “drive-by” download will be initiated. Do not click or engage with the popup window. Close the window by either closing the browser completely or through the (x) in the upper right corner of the window.

RANSOMWARE THREAT
The biggest malware threat today is Ransomware malware. You can get Ransomware malware maliciously installed on your computer by clicking on links in emails, downloading unknown attachments or by web surfing to compromised sites. Ransomware encrypts files on your computer and network shares and holds the files hostage until a ransom is paid to the hackers. Sometimes even if a ransom is paid, the files are not recoverable. Follow all previous guidance to reduce the chances of getting Ransomware installed on your computer.

Your BANK working for YOU

If you have any questions or concerns regarding your account please stop by or contact your local Monterey County Bank branch for additional assistance during regular business hours.
If at any time you have questions regarding security or possible fraud, please contact our main office at: (831) 649-4600 or you may send an email to electronic_banking@montereycountybank.com.

MONTEREY COUNTY BANK
The Business Bank

Alvarez Technology Group

Cyber Security information provided in association with Alvarez Technology Group, Inc.