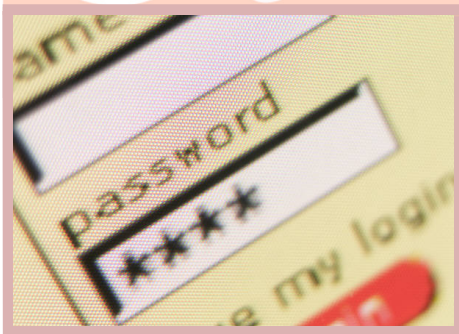
April 2014

Security focus



Online login credentials and security questions are the first line of defense in protecting your personal information. Whether it be internet banking, e-mail, purchasing accounts, or social media sites, information contained within these sources can be used against you when found in the wrong hands. The following information has been provided to enhance consumer awareness for best practices to minimize risk of online identity theft and potential financial loss.

Online Security Tips To Keep Login Credentials Safe

1	Avoid using the same ID and/or Password for multiple online accounts. If one online account becomes compromised, you risk your other accounts being compromised as well.
2	Avoid using "Remember Me" or "Store My Password" features. Allowing a website or computer to remember your login credentials increases the risk of unauthorized activity if the device is accessed or hacked by an unauthorized individual.
3	Do not use default or factory set passwords. When issued temporary passwords, log in to your account immediately to create unique login credentials.
4	Avoid using common personal details to create IDs or passwords, such as a combination of significant names, addresses, phone numbers or dates that can be easily guessed. For example: Spouse's name and date of anniversary or child's name and date of birth. Avoid using alpha numeric sequences, adjacent letters on the keyboard, or simple coding. For example: 11111, 12345, abcde, QWERTY, ASDF, p@ssw0rd, password1,
5	Prioritize your login accounts by importance. Keeping track of login credentials is a task all in itself. With millions of websites at your fingertips, it is not always practical to create a unique ID or password for every online account. Create stronger passwords for accounts where sensitive information may accessible, such as email accounts, financial accounts or social network profiles.
6	Consider changing your password every sixty to ninety days if you are not automatically required to update your log in credentials on a regular basis.
7	Length and complexity are the keys to strong passwords. Websites may establish certain requirements for when you create login credentials. Create IDs and Passwords that utilize as many characters as possible. Use a combination of letters (upper case and lower case), numbers and special characters when possible.
8	Always properly "Log Off" of your online account versus closing the browser window.
9	Do not share your personal account login credentials with other individuals. When necessary, request separate logins be created for additional users authorized to access your information. Contact your bank or the business immediately when there is a change in authorization.
10	Always ensure your anti-virus software is current and a full system scan is ran regularly. Whether intentionally or inadvertently, be cautious of the programs installed on your computer. Some programs are created to mask harmful software. Keylogger is a form of malicious spyware that records your keystrokes when you type on a computer. Fraudsters use this spyware to steal a user's passwords, logins, account numbers and other sensitive information.
11	IF YOU SUSPECT YOUR ACCOUNT OR LOGIN CREDENTIALS MAY HAVE BEEN COMPROMISED, CHANGE YOUR LOGIN CREDENTIALS AS SOON AS POSSIBLE AND CONTACT YOUR FINANCIAL INSTITUTION OR THE BUSINESS IMMEDIATELY TO ENSURE THERE IS NO LOSS OR FRAUD ON YOUR ACCOUNT.

Your BANK working for YOU

If you have any questions or concerns regarding your account please stop by or contact your local branch for additional assistance.

We encourage you to review our website, www.montereycountybank.com, for security tips and consumer alerts. If at any time you have questions regarding security or potential fraud, please contact our main office at (831) 649-4600 or you may send an email to electronic_banking@montereycountybank.com.

HOW SECURE ARE YOUR SECURITY QUESTIONS?

Consider the difficulty when answering the security questions you have selected for your account. While many websites usually provide pre-defined questions, avoid selecting basic questions such as: Mother's maiden name? Favorite color? Favorite sports team? Your Pet's Name?

Think of the general information you might share with an individual who is getting to know you or information that you would share on a social media profile. Any of this information may be easily obtained, guessed or researched online by others.

Providing simple answers to common questions used for security make hacking in to your online accounts easier for thieves.

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
☎ (831) 649-4600

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

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

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

EQUAL HOUSING LENDER

Member FDIC