From the desk of
Peter S. Muffoletto, C.P.A.

Creating Strong Passwords Can Protect from Identity Theft

Strong passwords go a long way to protect online accounts and digital devices from data theft.

Taking a few simple steps to protect your passwords can help protect your money and your sensitive financial information from identity thieves.

Common mistakes can increase the risk having sensitive financial and tax data stolen by identity thieves.

There have been some important changes many people can overlook.

Protecting access to digital devices is so critical that some now feature fingerprint or facial recognition technology, but passwords remain common for many people.

Given the sensitivity of many of these online accounts people should consider these passwords tips to protect devices or online accounts:

- Use a minimum of eight characters; longer is better.
- Use a combination of letters, numbers and symbols in password phrases, i.e., UsePasswordPhrase@30.
- Avoid personal information or common passwords; use phrases instead.
- Change default or temporary passwords that come with accounts or devices.
- Do not reuse or update passwords. Changing Bgood!17 to Bgood!18 is not good enough. Use unique usernames and passwords for accounts and devices.
- Do not use email addresses as usernames if that is an option.
- Store any password list in a secure location such as a safe or locked file cabinet.
- Do not disclose passwords to anyone for any reason.
- When available, a password manager program can help track passwords for numerous accounts.

Whenever it is an option for a password-protected account users also should opt for a multi-factor authentication process.

Many email providers, financial institutions and social media sites now offer customers two-factor authentication protections.

Two-factor authentication helps by adding an extra layer of protection.

Two-factor authentication means the returning user must enter their credentials (username and password) plus another step, such as entering a security code sent via text to a mobile phone.

Another example is confirming “yes” to a text to the phone that users are accessing the account on.

The idea behind multi-factor authentication is that a thief may be able to steal usernames and passwords, but highly unlikely they also would have access to the mobile phone to receive a security code or confirmation to actually complete the log-in process.

In recent years cybersecurity experts’ recommendations on what constitutes a strong password has changed.

They now suggest that people use word phrases that are easy to remember rather than random letters, characters and numbers that cannot be easily recalled.

For example, experts previously suggested something like “PXro#)30,” but now are suggesting a longer phrase like “SomethingYouCanRemember@30.”

By using a phrase users do not have to write down their password and expose it to additional risk.

Additionally people may be more willing to use strong, longer password if it is a phrase rather than random characters that are harder to remember.

Some measures of precaution now can save you from serious problems later.

We here at Muffoletto & Company believe that the more informed you are in regards to the rules and regulations that affect you the more we can be of service.
Should you have questions relating to any tax or financial matters call at
(818) 346-2160,
or you can visit us on the web at
www.petemcpa.com!

Providing individuals, small businesses, corporations, partnerships, professionals, and other business entities with the necessary guidance and answers for a complex world.

IMPORTANT NOTICE

The contents of this email and any attachments to it may contain privileged and confidential information from Muffoletto & Company.

This information is only for the viewing or use of the intended recipient. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of, or the taking of any action in reliance upon, the information contained in this e-mail, or any of the attachments to this e-mail, is strictly prohibited and that this e-mail and all of the attachments to this e-mail, if any, must be immediately returned to Muffoletto & Company or destroyed and, in either case, this e-mail and all attachments to this e-mail must be immediately deleted from your computer without making any copies hereof.

If you have received this e-mail in error, please notify Muffoletto & Company by e-mail immediately.

To ensure compliance with Treasury Department regulations, we wish to inform you that, unless expressly stated otherwise in this communication (including any attachments) any tax advice that may be contained in this communication is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code or applicable state or local tax law provisions or (ii) promoting, marketing or recommending to another party any tax-related matters addressed herein.

If you prefer not to remain on our email lists, please let us know.We will remove you as soon as you notify us.

You may do so by emailing us at

pete@petemcpa.com