

What Makes a Good Password?

By Bethany K. Lusby, CPA



Creating passwords for your computer and online accounts is obviously important. When choosing a password, though, you are seldom given tips and hints on what makes a strong password versus a weak one. With the ever-increasing online presences of you, your company and your employees, strong passwords are more vital than ever before.

Recently, a hacker posted to a website more than 32 million passwords that he or she hacked from individual, personal accounts. Aside from the alarmingly high number of passwords posted, the most shocking aspect of this post were the sheer numbers of weak passwords. Weak passwords are easier to crack; a fact that is not new but seems to be ignored regularly. Weak passwords lead to security vulnerabilities for your company.

The most common password in the list of 32 million was: 123456. Second place went to 12345. Creative and complex passwords seem to be in short supply these days. Choosing a strong password is not difficult in itself, but it seems that unless users are forced to adhere to rules about passwords, the threat of hacking alone will not prompt them to take necessary precautions. Generally, strong passwords are at least eight characters in length and will include uppercase, lowercase, symbol and numerical characters. This will help to ramp up the complexity of the password, making it more difficult to hack. Also, by following these guidelines, you will eliminate every word in the dictionary. Hackers oftentimes use databases that contain dictionary words, common first names and other information as a starting point in their hacking efforts.

Password risks do not stop at the complexity of the password, however. Many users, and indeed your employees could, use the same password for multiple accounts. Therefore, if a hacker compromises one account, he or she may have access to several other accounts. An employee uses the same password for his or her personal e-mail account and their log-on for their work-related remote network access. If someone compromises the personal e-mail account, your remote network may be compromised as well.

In order to combat any password issues your company may have, we recommend that you begin by educating your employees on the importance of having strong passwords. Give them examples of how to create strong passwords, what a strong password requires and if you deal with sensitive data, what types of files should be protected by a password. Moreover, employees should be reminded that they need to use a different password for each account they have. If they have trouble remembering multiple passwords, they may want to use mnemonic devices for their passwords and use an unabbreviated version to assist them in remembering it. Finally, remind them of perhaps the most common sense password rule: Do not share your passwords with anyone.

As an employer, you can institute some policies to ensure that your systems are not put at unnecessary risk due to weak passwords. One of the best methods to ensure strong passwords is to eliminate employees' ability to create weak ones. Speak with your network administrator about creating password rules that enforce the provisions above. Without these rules, there is a very

good chance that your employees will continue to choose weak passwords. Also, be sure that your site is run through a secure server and that your passwords are encrypted before being sent over the Internet. You could also employ anti-hacking mechanisms that require users to input text or perform mathematical computations when logging on. These mechanisms are good tools to thwart the software programs used by hackers. We also believe that you should change your passwords on a regular basis – perhaps every three to six months.

SHAREHOLDERS

Martin R. Glickstein, CPA
mglickstein@glccpa.com

Rodney S. Laval, CPA
 of Counsel
rlaval@glccpa.com

W. Neal Carris, CPA
ncarris@glccpa.com

James M. Loomis, CPA
jloomis@glccpa.com

Mary C. Dantuma, CPA
mdantuma@glccpa.com

Bethany K. Lusby, CPA
blusby@glccpa.com

Richard M. Ornstein, CPA
ronstein@glccpa.com

J. Russell Hamlin, CPA
rhamlin@glccpa.com

PRINCIPAL

T. Shepard Burr, CPA
sburr@glccpa.com