Column: Better Technology for Better Clients

Jan. 01, 2007

From the January-March 2007 Issue & 2007 Tax Season Survival Guide

Login please and enter your password. It's that demand you see so many times every day. Want to log onto your computer? Enter your password. Check e-mail? Enter your password. Login to your secure company website? Accessing Instant Messaging? Enter your password. At times, it is all that stands between your vital business information and intruders, both outsiders and nosy insiders. Our passwords are supposed to make our data secure. But do they? Truth be told, many of our practices are often anything but protective.

What is often overlooked is that the user of the password is human, and we all know humans don't operate with that same programmed routine as computers. So what's the answer?

Let's take a realistic look at how we behave and some simple changes that can help protect that vital data. See if you can relate to any of these typical office happenings:

> **Problem**: You walk into an office and the person that usually sits behind the desk is gone. Bathroom? Water cooler? At lunch? It doesn't matter, but what does is that the computer is still on and all their programs are wide open on the desktop. Anyone that walks in — anyone — now has full access to everything from e-mails to accounting.

Solution: It's simple.

to help you fix an error. You shared your password with a co-worker who helped you out by doing some work on your system.

Solution: Develop password replacement policies to follow when passwords become known. Make sure you train your team to request new passwords when people learn theirs. They need to understand it protects them, too. Your administrator also needs to turn on Windows server password options that force users to change their passwords regularly. In our office, we require a change in password every 30 days. And just so you won't get lazy, it won't let you repeat the latest ones you have used.

Problem: You have limited access to your critical internal systems areas to your administrators. Then, life happens and a non-administrator (either internal or external) is given the password to address a real-time business need.

Solution: Have a policy in place that requires the issuing of a new Administrator password within 24 hours once it is compromised. Make sure you notify all the key players securely.

Problem: Your co-worker stands over your shoulder whenever you are logging in. You are concerned they will learn your password.

Solution: Teach them "Password

- www.securitystats.com/tools/password.php
- www.microsoft.com/athome/security/privacy/password_checker.mspx

Also remember to use common sense. If your password doesn't look secure to you, no matter what the checker says, it probably isn't.

Problem: Your Office Administrator is on vacation, and it's time to order office supplies online. Your website manager is out sick, and you must make changes to your website. Both require a password. Now what?

Solution: Have backup access for non-critical areas when a "stand-in" helps out. More importantly, make sure you develop and maintain a process of storing vital passwords that management can access for just such a circumstance.

Problem: Turnover. It's been a month since the last two employees left, and their passwords are still active. And it's not just internally, they also still have active passwords with your primary vendors. How do you spell exposure?

Solution: Create a master list of who has access and to what they have access. That way, it's easier to be sure you are removing their access to all areas where they may have had free reign. Think about it. We so often overlook our external business relationships. Team members may have access, on the business's behalf, to your customers, your vendors and suppliers, payroll services, online banking and more. It is

absolutely critical that you be sure someone removes the ex-employee as a user

it. If your computer is on, anyone can run any program for which you have saved an automatic login. Just how secure is that employee information for which you are responsible?

Solution: Save the automatic sign-ins for non-critical needs. Make sure they are really non-critical, and don't give access to private business information. For everything else, don't ever accept that free pass to keep your User ID and password.

In the end, even if you are following all the solutions outlined above, it comes down to just how strong is your password. There are lots of thoughts and tools for you to improve password creation. There is no one right answer. Using a secure, memorable password that is easy for you to remember and hard for others to guess is the goal. Here's some sound password tips:

- Passwords should be at least eight letters; the longer the stronger. Don't forget to balance your team's need for security with the ability for people to remember their passwords. Also include at least three of the following elements: uppercase letters, lowercase letters, numbers and symbols. Pick your letters, numbers and symbols from all over the keyboard.
- Don't use the same password for everything. If it becomes compromised and someone finds it, then the rest of your identity is at risk.
- If you have lots of passwords to remember, establish your own internal rules that will help you remember them, suggests Gina Trapani, editor of LifeHacker.
  For example, choose something like "asdf" as your base and then some formula that combines the service name. So your password for Yahoo! might be ASDFYHAO, and your password for eBay would be ASDFBYEA.

- For another option, take the first letter of each word of a memorable sentence

- forget password etiquette to help on this.
- DO NOT write a password on sticky notes, desk blotters, calendars or store it online where it can be accessed by others. Contrary to popular belief, there is nothing wrong with writing passwords down. They just need to be adequately
  protected in order to remain secure and effective. In general, passwords written on a piece of paper safely stored are more difficult to compromise.

Passwords today are a fact of life. Like good nutrition, the right passwords and processes can enhance your feelings of security and well being. Don't let them overwhelm you, but do take them seriously. And pledge to start now by following these easy rules. Now there's a New Year's resolution that you can keep!

Lisa is President of L. Kianoff & Associates, Inc., which she founded in 1986. Her computer consulting firm has been a leader in helping companies strengthen their business performance with award-winning accounting and business management systems.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.