Password security tips to keep in mind

> **"Don't use combinations of birthdays, anniversaries, pets, 'password,' or other information that is available in the public records, LinkedIn, Facebook, or other social media sites when creating a password."**

CATHERINE WENDT

Perhaps the following story is familiar to you. Recently, a friend of mine was tricked by what seemed to be an email from a known vendor. The vendor was asking my friend to confirm the password for a business account.

My friend clicked the link, typed in the user name and password, and that was the beginning of a very big ordeal. You see, my friend had just given a hacker the password for all of his bank sites, credits cards, and so on.

What a nightmare.

Of course, my friend now knows not to ever give out a password or login information through an email. It could easily be a hacker trying to get your data.

The second mistake was having one password for all of his accounts.

There are best practices in creating your passwords for your secure websites and app functions:

• **Best Practice No. 1:** Use a different password for every site and account you have. Yes, it's a pain! But it's so very important in keeping your security intact.

• **Best Practice No. 2:** Don't re-use a password within 18 months, minimum. This makes it much more difficult for hackers to reach into your world and steal your information. If an account sends you a password reset and won't let you type in a reused password, don't grumble. Be thankful for the reminder.

• **Best Practice No. 3:** Use a 'strong' password. A strong password has at least 8 characters, upper and lowercase letters, numbers, and at least one special character. The more complex, the better! Remember, you are helping yourself stay safe.

Now a word about passwords at your office — for your network, there is an administrator account that is required to perform specific functions, and it is also has rights to change any user's password, including the person who handles your IT.

The administrator password is to be a strong password and safeguarded at all times. Users should be required to create a strong password for their accounts and forced to change them every 90 days or so.

Service accounts should have random-generated passwords to withstand brute-force hacking attempts. This is when someone, often a computer program, randomly attempts to log in through these seemingly unimportant accounts by trying combinations over and over until they stumble on one that will work.

Lastly, don't use combinations of birthdays, anniversaries, pets, 'password,' or other information that is available in the public records, LinkedIn, Facebook, or other social media sites when creating a password.

• *Catherine Wendt is president of Syscon Inc., a technology solutions business based in Hinsdale.*