Cyber Security
Protect yourself online by securing your passwords

Our lives are online. We have easy access to an amazing world of information and connections at the speed of light, whether it's banking, Facebook, buying a pair of shoes or even a canoe! It is as easy as 1-2-3 to have everything at our fingertips. But so is our password for hackers!

Did you know that some people still use passwords like "password" or "123456"? Needless to say, it's dangerous to use the same simple password for all of your online accounts. Imagine a hacker cracked that one password? To be safe, you should create unique and difficult-to-crack passwords.

Small and midsize businesses that struggle with information security because of resource constraints have particular reason to pay attention. Smart password practices require next to no budget. They don't need to take up much time either, especially once your policies and procedures are in place.

So do you know how to create a good password? Here are some tips and tricks to maintain strong passwords for all of your online accounts.

Know the Characteristics of a Safe Password:

- **It cannot be found in a dictionary**
- **It contains special characters and numbers**
- **It contains a mixture of upper and lowercase letters**
- **It has a minimum length of 10 characters:** Because the length of a password is one of the primary factors in how strong it is, passphrases are much more secure than traditional passwords. At the same time, they are also much easier to remember and type
- **It cannot be guessed easily based on user information** (birthdate, postal code, phone number, etc.)

Here is an example of a well-constructed password: Tl|_|$,BwwB2RFB

There are many different approaches to generating a strong password but one of the best practices is to use a password manager, a software application on your computer or mobile device that generates very strong passwords and stores them in a secure database. You can use a single passphrase to access the database, and then the manager will automatically enter your username and password into a website's login form for you.

LastPass is the leader of the online password managers because it's both easy to use and can be locked down pretty tightly.

Password policy is something that is often overlooked. Here are some steps for safer, stronger passwords both in the real and mobile office.

- **Update your password every few weeks/months:**
    - Change your base password only
    - Change the special character substitutions you're using
    - Reverse use of upper and lower case letters
    - Type the password with **SHIFT** lock turned on

- **Don't reuse passwords:** Employees that use the same password across multiple systems, often both professional and personal, in order to keep things simple can turn a minor, isolated issue into a major security breach.
- **Restrict application settings,** particularly for online and mobile applications, It is a good idea to modify security and privacy settings to the most locked-down options.
- **Consider a password wallet:** One password pitfall is found in password sharing among workgroups and team members. This can lead to weak security habits, both of the analog (Post-it Notes on the monitor, yelling passwords over the cubicle wall) and digital variety (passwords shared via email, IM, and related means). A password manager or wallet application built specifically for teams can automate and secure credentials for systems that require multi-party access.
- **Use a device-lock app:** A lost or stolen device, for starters, can become a nightmare for the unprepared business. Begin by requiring, or at least strongly encouraging, staff to use a device-lock feature or app and set it to time out automatically at one minute or less of inactivity.
- **Do not jailbreak or root phones:** This one is likely to be a particular concern for businesses that encourage employees to bring their own device to work. Users that jailbreak their iPhone or root their Android device could be bringing increased security risks onto the corporate network. Consider a policy restriction that bans such devices for company use.
- **Fully exit apps:** It is recommended that users sign out and exit business apps when not in use rather than leave them running in the background.

This is an important topic for all businesses, which is why there is a cyber security gathering called PasswordsCon in Las Vegas. Sam Crowther unveiled a new option for password security. His application lets you pick a photo on your device as your password to a web service and transmits that as an incredibly long password. If that photo gets deleted, you can just reset the password to another one. This is not a proven theory yet, but a picture is worth a thousand words.

Do not be vulnerable to hackers—update your password!

Submitted by Gina Mercado, vice president of client relations at Big Red Pin (www.bigredpin.com), which provides technology services for event spaces and large public venues; and Nick Pascarella, a partner at TruBambu (www.trubambu.com), a business technology consultancy company.