It's no secret that people are bad at passwords. Whether it's your bank account, work login or personal email, passwords alone just aren't as secure as they used to be, especially with the simple logins that most people choose. Anyone can access your personal information and wreak havoc on your life just by obtaining your password.

Additionally, password hackers have stepped up their techniques by identifying patterns and common practices that people use when creating their password. Add in the fact that faster hardware has become inexpensive and you now have a computer that can try billions of password combinations in a second.

Fortunately, there are a lot of tools and practical advice to protect yourself or your business against hackers and identity theft. Improve your password and step up your security by employing some of the points below.

<h2>Use Stronger Passwords</h2>

Most of us create our passwords in the same way, especially when we are required to have uppercase and lowercase characters, numbers or symbols. People tend to use common words or names as well as these techniques:

- Capitalize only the first letter. Example: Spot
- Add a number only at the end. Example Spot1
- Use a common symbol only at the end. Example Spot1!

These patterns are obvious to hackers. Even substituting a number for a letter (Sp0t1!) and adding a word (Sp0tD0g!) doesn't help because hackers use these statistics against us as while as utilizing master crack lists.

So what constitutes a strong password? Don't use the common practices above. Instead, use a mix of character types including spaces. Don't use a single dictionary word, names or dates, but try to make your password as long as possible. Multiple unrelated words make great passwords, especially if you stay away from common quotes, phrases, titles or lyrics

Try using Howsecureismypassword to check the strength of your login..

<h2>Use Different Passwords for Different Accounts</h2>

This is one of the most important security strategies that you can use because it limits the damage that can occur if one of your accounts is compromised. Remember when 6.5 million passwords were stolen from LinkedIn? If any of the members with a breached account used

the same password elsewhere on the internet, hackers could have easily committed identity theft on an astronomically large scale.

It it is hard for you to remember different passwords for all of your accounts, trying using a password manager (see next bullet).

<h2>Use a Password Manager</h2>

Not many of us are skilled enough to remember several alphanumeric passwords for different accounts. This is where password managers save the day. These tools securely store all of your passwords and can function as automated web form fillers. Secured by a single ultra strong password and accessible across multiple platforms or devices, password managers definitely are a great choice to stepping up your security.

LastPass is a popular option that is also compatible with two-factor authentication.

<h2>Use Two-Factor Authentication</h2>

The best way anyone can keep their online privacy secure is through multi factor authentication. While it might sound complicated, it is just an added step on the login process. Usually, it is a unique code that is generated for you and retrieved via text message, mobile app or email. So when logging in, you would enter your strong password and the unique code.

This added step can make a huge difference in keeping snoopers out of your accounts. While two-factor authentication might be overkill for accounts that contain no personal information, it should be used for any account that would cause significant suffering if hacked (bank, email, stocks etc).

<h2>Conclusion</h2>

In the era of the Digital Age, password security is just the beginning for protecting yourself against identity theft and fraud. Ask yourself, "Is my mobile device secure? How much personal information can be stolen from my social media accounts? What sites do you visit when browsing on a public network?"

Try this digital security quiz to find out what you need to do to protect yourself.