STOP | THINK | CONNECT™

At Chicago Title, cybersecurity is a top priority every moment of every day. Protection of confidential information entrusted to us by our customers and business partners is a responsibility that we take very seriously.

Each October, the U.S. Department of Homeland Security works to raise awareness about the dangers of online attacks through its National Cyber Security Awareness Month campaign - STOP, THINK & CONNECT. We would like to take this opportunity to remind our valued clients of the danger out there and you should always stay active in managing your digital security.

Improving Digital Security with Password Managers

For those of us who use a variety of passwords to access everything from banking and shopping websites to work-related systems and apps, it can be difficult to remember which passwords are associated with each site, much less change them on a regular basis.

The alternative, however, can be much worse – for you, your clients and others. If someone discovers your password and taps into sensitive information of any kind, the damage done can be very expensive – and sometimes it is irreparable.

That is why the use of a password manager is considered to be a best practice to help improve a user's level of security when accessing any digitally stored information. A robust password manager will first and foremost dramatically reduce (hopefully eliminate) the need to write down passwords at all, which is one of the easiest ways passwords are compromised. A password manager can also flag weak passwords or provide an automated password change feature in case of a suspected hack event.

Password managers can either be cloud-based (like LastPass) or offline/local (like KeePass), which exists only on your designated system.

- An offline password manager will maintain an encrypted database of passwords
- An online password manager uses secure communications (HTTPS/TLS) to access password information
- Another option is a hybrid of offline and online, which is downloaded to a local system, but has the ability to synchronize with a server (whereas an offline system typically does not)

Regardless of the type of password manager solution you select, creating a complex master password should be established to access the password manager. The complex master password should:

- Be at least 10 characters in length
- Contain both upper and lower case letters, at least one number and a symbol
- Not form an actual word

To help you decide what kind of password manager might be a good fit for you, additional information is available at the STOP | THINK | CONNECT website - https://www.stopthinkconnect.org

Source: Tech FNTG and www.stopthinkconnect.org

CHICAGO TITLE®