bizwomen
THE BUSINESS JOURNALS

ADT CHANNEL

Password security demands attention, vigilance

ADT
Mar 30, 2014, 10:33pm EDT Updated: Mar 31, 2014, 10:05am EDT

Only two generations ago a password was something that got you into a speakeasy or was a tool used by government agents in arranging clandestine meetings. Today the humble password is the ubiquitous key that opens doors to more personal and business data than most of us often realize.

Safeguarding passwords is a discipline that should be prioritized in even the smallest of businesses.

The owner of a small business today may have dozens or even more than 100 different accounts requiring password access. A typical week may see her accessing her personal and business bank accounts, brokerage accounts, multiple email accounts, airline mileage accounts, personal and company websites, photo storage accounts, online bill-pay for multiple utilities, alumni associations and more – much more.

With an ever growing number of access portals requiring passwords for entry to secure data, the level of opportunities for compromise increases.

“Smaller organizations tend not to have the IT resources or the focus on data security that larger companies do,” said Heinan Landa, CEO of Optimal Networks, a Washington, D.C.-based IT services firm. “Passwords and data security may be seen as technical matters that are not necessarily a company’s top priority. This lack of emphasis may leave them vulnerable.”

Recent data suggests that traditional practices for securing passwords by changing them every 90 days can actually lead to greater exposure to hacking,

according to Landa. Though it may seem counter-intuitive, changing passwords frequently in many instances leads people to forget them more easily and write them down or use the same password for multiple accounts – a practice that most experts agree is dangerous.

"Today's sophisticated cybercriminals have determined several strategies to take advantage of weak login information and easily decodable password hints," said Andreas Baumhof, chief technology officer at ThreatMetrix, a cybercrime protection firm. "The risk of relying on passwords is that once account login information is compromised, cybercriminals gain access to personal data and identities that can be used for fraudulent retail transactions."

Here are some steps to take to mitigate risks:

- **Multi-step authentication:** Small businesses can set up two- or three-step verification procedures to access company websites and online accounts. Beyond login accounts and passwords, systems can be established that require additional access hurdles, such as knowledge-based questions or even fobs with randomly generated numbers that must be entered. Baumhof noted that many popular websites such as Google, LinkedIn and Twitter make two-factor authentication available to account holders.

- **Educate yourself and your workforce:** Landa said business owners should consider an IT security audit. "I'm always surprised at the number of employees, when contacted professionally and simply asked for login and password information, readily give it up with no questions asked," Landa said. "Password security policies must be put in place and regular, direct communication must take place about how to safeguard password information and data security."

- **Use multiple passwords with long character strings that incorporate numbers and letters:** Avoid phone numbers, birthdays, social security numbers, pet, children or spouse names, or other easily hacked

password identifiers. Do not write passwords down, rather invest in password management software to help safeguard and catalogue your passwords. Most offer auto-fill features and remote access and integration capabilities with multiple browsers. Operating systems RoboForm Everywhere, Sticky Password Pro, and DataVault are recommended products for individual password management.

Plus, when traveling or on the road, be diligent about securing your laptop or portable devices and be certain your data is encrypted.

No systems are infallible, but with awareness, education and some basic precautionary measures, keeping your passwords secure is a major step in protecting your sensitive data.