Protecting Your Business
Hints & Tips – Passwords

August 2019

CYBERSCOUT®

7580 N Dobson Road, Suite 201
Scottsdale, AZ 85256

888.682.5911
www.CyberScout.com

Scottsdale, AZ / Providence, RI / New York, NY
Montreal, Canada / Galway, Ireland

CYBERSCOUT®

What are some of the most common pitfalls SMEs make when creating passwords for their IT infrastructure?

1. Using the default password – Most technology comes with default administrator or other passwords installed on it. These passwords can either be standard across all of the technology (and therefore looked up on the internet) or can follow set patterns that can easily be deduced by criminals and attackers.

2. Re-Using Passwords – Many corporate and SME attacks occur because attackers are able to find a password from a breach of a previous system that has been repeated with the same or a similar username. Many large-scale breaches worldwide including social networks such as LinkedIn and Yahoo included username and password data.

3. Concentrating on change cadence rather than inherent strength – Having a weak password changed every 30 days is far less effective than a strong password changed every 90 or 120 days. Regular password changes often result in users writing passwords down and modern software can 'crack' a simple password in a few hours.

4. Ignoring 2FA – Many recent technologies have the ability to apply two-factor authentication to the credentials. This means the attackers must 'hack' you for both something you know (a password) and something you have (a mobile phone or a separate authentication device).

What does a weak password look like? How easy is it for cyber criminals to get past weak passwords? How do they do that?

Weak passwords contain single dictionary words, start with a capital letter and end with a number, often with repeated or consecutive numbers to make up the minimum required length. It is also a good idea not to use accurate data about yourself that could be found elsewhere. Topic to be avoided include:

- Partner's name
- Child's name
- Other family member's name
- Pet's name
- Place of birth
- Favorite holiday
- Something connected with your favorite sports team

CYBERSCOUT®

Why are weak passwords so dangerous and costly for SMEs/start-ups? Will these businesses feel the impact of cybercrime more keenly than other types of organizations?

Small businesses and start-ups are generally much more focused on their day-to-day business. Profit margins are low and are further pressured by the need to grow fast. This often leads them under-resourced to resolve incidents when they happen and less room in their bottom line to suffer the costs of remediation.

How does Bring Your Own Device (BYOD) culture fit into this?

For similar reasons, many small businesses allow their staff to access company systems and infrastructure on their own devices. Remember you have no control over the underlying system of these devices; what security is installed; if it is updated to defend against the latest attacks and more importantly what it is used for outside of work hours.

What does a strong password look like?

A good system I often use is to merge three random words together and to add numbers and symbols throughout the resulting password. The words should not be personal details but should mean something in the back of your mind which makes you less likely to forget it. Attackers can often guess if you have common letter-for-number substitutions (such as 5afetyf1rst) so avoid these. Finally, special characters such as $ or £ can be useful as they do not appear on all keyboard formats.

What technology exists to help SMEs manage their passwords?

Many password managers are available online that can create and store military grade password keys that are individual for each account. Most will even work on all of your devices so users have no need to remember more than one strong password. Some of the better ones will even create unique usernames linked to single use email addresses for you which means it is impossible to repeat a username/password combination and if your account is breached, you will know exactly which system was breached.

What role does education play? Is it important to keep staff up to date with cybersecurity issues and to encourage regular reviews of procedure?

Education is essential. We at CyberScout find that education is most impactful when it is part of a constant campaign throughout the year relevant to the specific threats at that time of year: tax return season to warn of the dangers around bogus emails from the tax man, Amazon scams in the lead-up to Christmas and advice on changing default passwords on all your new devices in the new year.