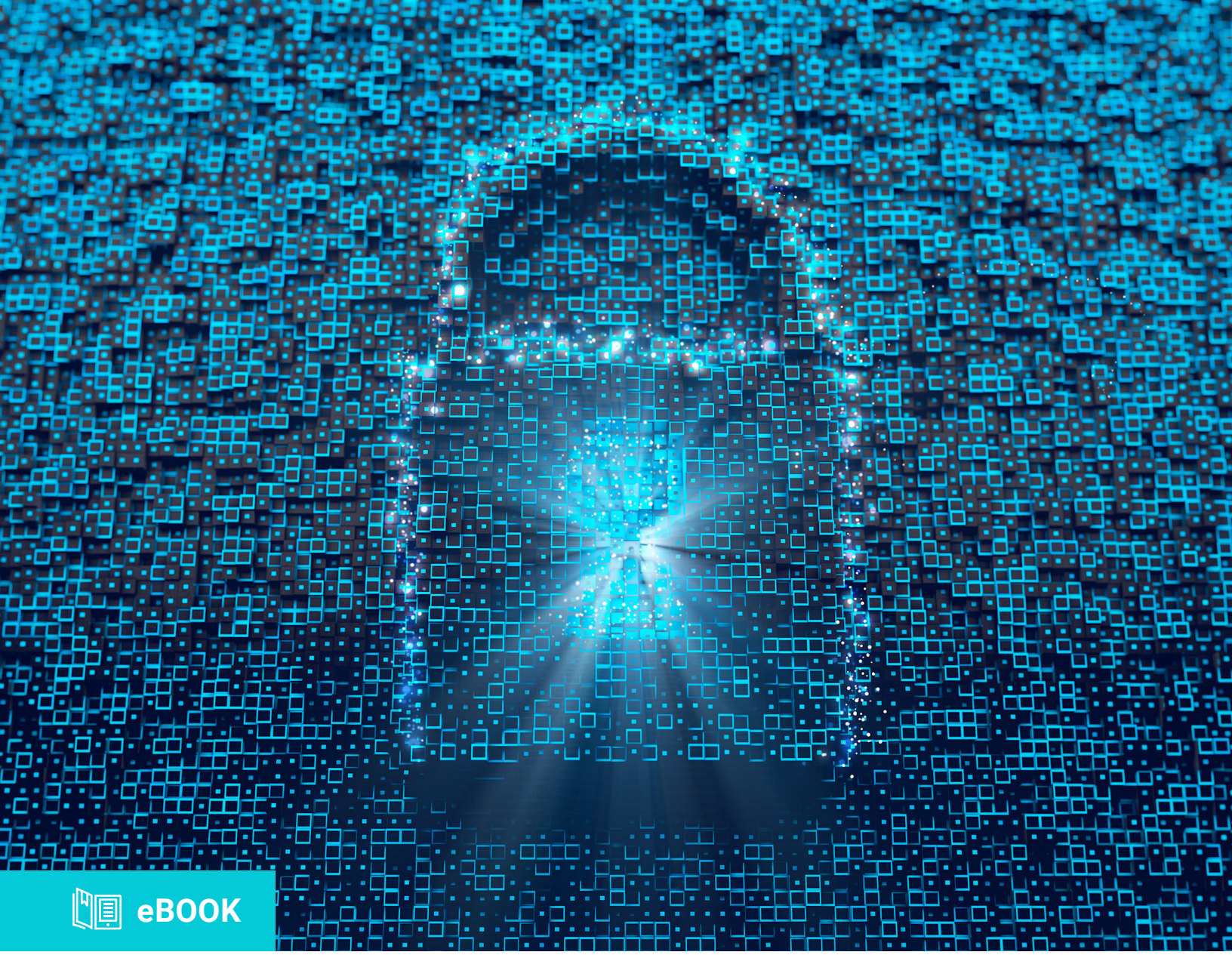
1CS
Computer Services

PASSWORD MANAGEMENT - EBOOK

WWW.1COMPUTERSERVICES.COM



eBOOK

Be Your Own Best Defense Against Cybercrime

How you can help us protect your business by taking a strong stance on passwords.

1CS

Think cybercriminals won't attack your business? Think again.

If you use digital tools and connect to the internet, you're vulnerable to cybercrime. It doesn't matter the size, sector, or location of your business.

As your managed IT services provider, we're committed to doing everything we can to keep the bad guys from getting into your network: we set up firewalls, detect and block malware, patch servers and systems, and a lot more. But even the best protections can be foiled if a hacker gets their handson passwords that give them access to all your systems and data —and for small- and medium-sized businesses (SMBs), the financial consequences of a data breach can be devastating.

~70%

of hacking-related data breaches are due to weak or stolen passwords[1].

$3,533

is the average per-employee cost of a data breach for companies with fewer than 1,000 employees[2].

HOW'S YOUR "PASSWORD HYGIENE"?

For many businesses, the honest answer is, "Not great" . But poor password management can seriously undermine other security measures you have in place. It's like having the biggest, strongest locks on your front doors—but leaving the windows wide open.

While we've got most things covered related to IT security, it's impossible to do it all on our own. There are some areas, like password management, where the power is in your hands.

As a partner in your own security, you can help us protect your business by:

- **Making your passwords strong**
- **Changing your passwords often (ensuring they are still strong and unique)**
- **Keeping tight control over who can access your systems and data**

If that sounds like a lot of work, don't worry! Today's password management tools make it easy to implement good password hygiene without a lot of effort.

1 "2019 Data Breach Investigations Report," Verizon. https://enterprise.verizon.com/resources/reports/dbir/ (Accessed October 2019).
2 "2019 Cost of a Data Breach Report," IBM, Ponemon Institute. https://www.ibm.com/security/data-breach (Accessed October 2019).

PROTECTION POINT

Make Strong Passwords Company Policy

The first thing you can do to help us protect your business is make sure everyone in your company uses strong passwords to access devices, services, and applications.

There are four main characteristics of strong passwords:

1 THEY'RE UNIQUE

People often use the same password across all their business accounts—and sometimes their personal ones, too, like email and online shopping—because it's easy to remember. But that means a hacker needs just that one password to do damage. (Hackers will try compromised social media email/password combos on banking websites, for instance, hoping for a match.) When every account has its own unique password, even if one falls into the wrong hands, hackers can't do much with it.

51%

of people re-use passwords for business and personal accounts[3].

2 THEY'RE COMPLEX

Mixing uppercase and lowercase letters, numbers, and symbols makes your passwords stronger.

Try to avoid using obvious combinations and placements, though. These include putting uppercase letters at the start of the password and symbols at the end, using "@" as the letter "a" or adding "123" after an otherwise common word. Hackers know these patterns and use them when structuring their attacks.

3 THEY'RE UNCOMMON

Many hackers start their attacks using online databases of popular passwords. These passwords often include:

- Unaltered dictionary words (sunshine, princess, monkey, football)
- Sports and pop culture terms (brady12, starwars)
- Repetitive or sequential characters (qwerty, 123456)
- Reverse spellings (drowssap).

Avoid using personal details like birthdates, phone numbers, or ID numbers—they're not as confidential as you might think.

And it should go without saying, but please don't use "password" or "admin!"

3 "2019 State of Password and Authentication Security Behaviors Report," Ponemon Institute. https://www.yubico.com/authentication-report/ (Accessed October 2019).

4 THEY'RE LONG

Longer passwords are much harder to crack than shorter ones. Pick a password that's at least eight characters—but even longer is better.

To make longer passwords easier to remember, use a passphrase made up of several words (e.g., "MyCat!Isn'tHappy8WithMe").

You can even convert passphrases into strings of randomized characters. If you use the last letters of each word, our example above becomes "YTTYHE". When you add other characters and change the capitalization, you get "Y#T!Ty8He%" —something that appears random but, because there's an underlying logic, is easy to remember.

If you have an automated tool that can create and store long passwords for you, there's no need to remember them at all!

IS THIS YOUR PASSWORD?

These 20 common passwords have been used most often by hackers in global data breaches[4]:

- ✖ *123456*
- ✖ *123456789*
- ✖ *qwerty*
- ✖ *password*
- ✖ *111111*
- ✖ *12345678*
- ✖ *abc123*
- ✖ *1234567*
- ✖ *password1*
- ✖ *12345*
- ✖ *1234567890*
- ✖ *123123*
- ✖ *000000*
- ✖ *iloveyou*
- ✖ *1234*
- ✖ *1q2w3e4r5t*
- ✖ *qwertyuiop*
- ✖ *123*
- ✖ *monkey*
- ✖ *dragon*

If you use these, or any of the UK National Cyber Security Centre's top 100,000 hacked passwords — change them ASAP!

4 "2019 State of Password and Authentication Security Behaviors Report," Ponemon Institute. https://www.yubico.com/authentication-report/ (Accessed October 2019).

PROTECTION POINT

Keep the Bad Guys Guessing

Set company-wide rules for resetting passwords. That way, even if a hacker obtains login credentials for your business, by the time they get around to using them, they're more likely to be out-of-date.

Passwords for accounts with administrative privileges and sensitive or critical systems should be changed on a regular basis—every three to six months at the very least. (Less critical systems can go longer.) Set expiry dates for passwords if you can, prompting users to change them before they can re-access a system. Make sure any new password is as strong and unique as the one being replaced. That means no updating the same password by adding a "2" at the end!

If a service you use was the target of a known or suspected data breach, change the affected password right away. That might sound obvious, but 57% of people who experienced a phishing attack didn't change their password behaviors[5]. And if you or anyone on your team shares login details with another person, change that password as soon as they're done. Even if they're well-meaning, they could have stored that password in an unsecure location or noted it in a highly visible location.

29%

of people rarely or never change their passwords[6].

5 2019 State of Password and Authentication Security Behaviors Report," Ponemon Institute. https://www.yubico.com/authentication-report/ (Accessed October 2019).

6 "Uncovering Password Habits: Are Users' Password Security Habits Improving?" Digital Guardian. https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic (Accessed October 2019).

PROTECTION POINT

Be Vigilant about Access Control

You need to give your staff access to systems and applications to do their work. But most people don't need privileges for everything. Access control is about making sure the right people have access to the right programs and accounts—and nothing more.

Set up a system for tracking who can access what, when, and how—and keep it up-to-date. Detailed logs of who accessed your systems are a must if you're in a regulated industry that has to meet stringent compliance measures for data storage and access. It also becomes important when employees leave your company. Just as you take back their keys, be sure to cancel their passwords, too. Otherwise, they could use their credentials to access data that might help their new employer lure clients away from you or steal your ideas. Somebody who left disgruntled could be even more dangerous, using leftover privileges to install malware as an act of revenge.

Even if someone would never do anything to deliberately harm you; if their computer or records were compromised, someone else could get their credentials, and that individual might not be so well-meaning.

A lot of businesses appreciate the critical importance of access control once they're made aware of it. But many have the same question: How can we do this without taking on significant extra work?

A good password management tool—one made specifically for businesses—is the answer.

89%

of ex-employees admit to retaining access to business-critical applications like Saleforce® or QuickBooks®.

7 "The Ex-Employee Menace," PR Newswire. https://www.prnewswire.com/news-releases/the-ex-employee-menace-89-retain-access-to-salesforce-quickbooks--other-sensitive-corporate-apps-270904001.html (Accessed October 2019).

PROTECTION POINT

Use a Password Management Solution

Let's be honest: creating unique passwords for every account, making sure they're updated regularly, and maintaining strict access controls seems like a lot to manage. But a full-featured password management solution is an economical and easy way to adopt good password hygiene with minimum effort.

All of us, IT professionals included, like to do things as quickly and efficiently as possible. That's often what leads to cutting corners by creating weak passwords, writing them down on sticky notes, and not staying on top of critical security details. It's human nature.

Password management software removes the burden of being diligent while keeping your business safe. These tools generate strong passwords automatically for every account and insert them as needed during the login process, so there's no memorization required—or unsecured notebooks or spreadsheets to maintain.

A good password management solution also gives you an at-a-glance view of who has access to what systems, making it a breeze to control access and revoke old credentials when employees move on. And it gives you the assurance your business is compliant with data protection laws and regulations—helping you avoid fines if you are ever breached.

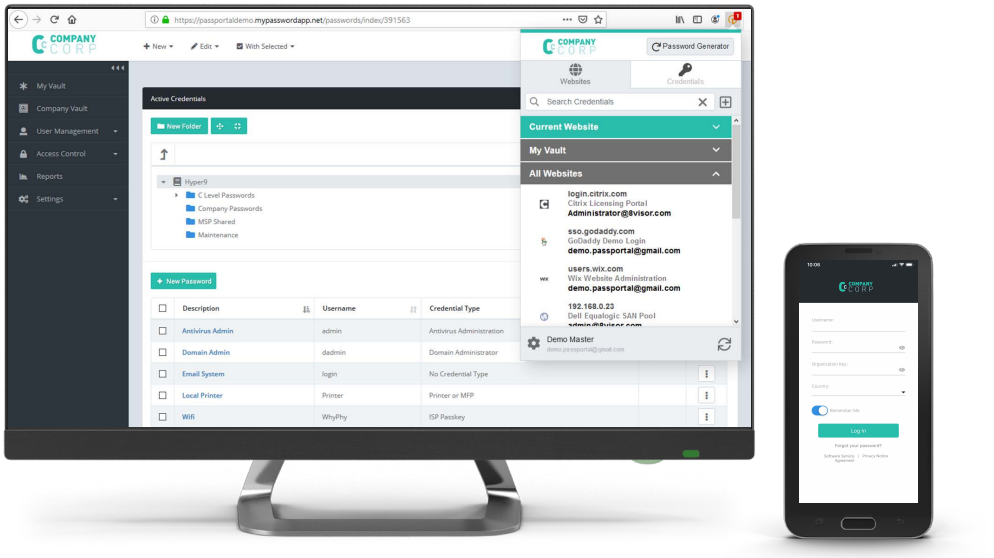
With the right password management solution, you can be a fully powered-up partner in your own security and have more control and flexibility than relying on your technicians alone.

PROTECTION POINT

Stay Protected with Smart, Simple Password Management

Cut down on risk and help your team sleep easier at night with our easy-to-use, cloud-based password management service.

Through our self-serve online portal, your employees get an at-a-glance view of only the passwords they need to perform their work. They also get access to a password generator tool, along with a browser extension that automatically completes login forms with the strong, unique passwords that have been generated—putting an end to "sticky note security."



Administrators can set password expiration warnings reminding your team to refresh their credentials on a regular basis. And if somebody leaves the company, you can revoke all their privileges in a few clicks without having to call your team for support.

With your front door secure *and* your windows sealed, you can focus on what really matters: growing your business.

Take control of your passwords and system access—and help us make your business even safer.

Want to learn more? Contact us today.

www.1computerservices.com

info@1computerservices.com

647.956.6081