thinkCSC's

Guide to Password Security

think CSC | Your Chief Technology Office

THE PROBLEM WITH PASSWORDS

Usernames and passwords are the go-to security solution for so many networks, services, and social media sites, but they are the weakest link in your security efforts, particularly when taking into consideration the risk of human error. Usernames and passwords are often the only layer of security that stands between your employees and your business network. While best practices demand that we should use different passwords for every service (do you?), the reality is that most of us repeatedly reuse passwords. That is a huge problem. The password that may have just been stolen from your employee during the latest breach may be the same one they use to connect to your network, your financial system, or their work email.

COMPROMISED PASSWORDS ARE RESPONSIBLE FOR 81% OF HACKING-RELATED BREACHES.

Verizon Data Breach Report

PASSWORD REUSE IS A HUGE PROBLEM

When passwords are shared among different services, it can have a devastating impact, yet it is one of the most common causes of security breach. When one service is compromised, ***every subsequent use of that credential is at risk***.

- Malicious actors inject themselves into the middle of an email conversation regarding an invoice or other financial transaction and intercept data (e.g. provide the other party with different bank routing info).
- Cyber criminals create rules to forward, delete, or hide messages so that their activity is undetected.
- Information is gathered for later use for other nefarious purposes.

It all starts with a password that someone used in more than one place and found its way into the hands of the criminal element on the Dark Web.

THE DARK WEB WANTS YOUR CREDENTIALS

Your usernames and passwords are your portkeys to the business applications that are the lifeblood of your organization. Those credentials are also one of the hottest commodities on the Dark Web.

WHAT IS THE DARK WEB?

The Dark Web is an untraceable, undetectable area of the web that can be accessed only by using special software. Originally created to provide an environment of free speech and anonymity, the nature of the Dark Web has allowed online criminal activity to flourish. And while some usage of the Dark Web is benign and can actually provide a voice for those in oppressed countries, nearly half of all activity on the Dark Web is criminal. From the sale of illicit drugs to far more nefarious activities, the Dark Web can be a dangerous environment. One of the most common crimes taking place is the disclosure and sale of business credentials and personal information. The criminals who obtain these credentials are patient and sophisticated – and are willing to wait, sometimes years, for the opportunity to use the information to harm your business for financial gain.

YOUR BUSINESS IS VULNERABLE

Usernames and passwords are often the only layer of security that stands between your employees and your business network. While best practices demand that we should use different passwords for every service (do you?), the reality is that most of us repeatedly reuse passwords. Credentials to things your employees might consider unimportant, such as a pizza delivery service, can give second-rate cyber thieves the extra boost they need to compromise your entire network.

If “Joe’s Pizza” happens to have a loyalty program and has collected that data (most restaurants do). They might even pick up the answer to a generic security question or two. This information can potentially give them the advantage they need to leapfrog into something more important, such as the security question on your email password reset or key details for a credit application.Identifying compromises and taking actions to contain those breaches are critical to your overall personal and professional security posture.

PASSWORDS ALONE WILL NOT PROTECT YOU

While reusing passwords, using passwords that are not strong enough, or using the same password for multiple applications will inevitably result in your organization and executives within your organization being compromised. But **password strength alone is not enough** to protect your organization from sophisticated and persistent hacking attempts.

SECURITY HYGIENE

Security hygiene practices are the essential best practices that ensure the security of personal identity. These practices include:

- Timely security patch installation
- Multi-factor authentication
- Threat detection solutions
- Multi-layer browser and email security
- Advanced monitoring
- Employee training
- Strict policies regarding public Wi-Fi use
- Comprehensive mobile device management

Security hygiene best practices also calls for the use of unique, strong, regularly changed, complex passwords. But more than stringent password management, we believe it is absolutely critical to employ the use of a **password manager** like Myki.

THERE IS MORE THAN A 25% CHANCE YOUR BUSINESS WILL EXPERIENCE A DATA BREACH BECAUSE OF POOR SECURITY HYGIENE.

Infosec

PASSWORD SECURITY GUIDANCE

Many organizations, especially small businesses, rely on username and password protocol as their primary cybersecurity protection method. They assume that requiring employees to use strong passwords, and then requiring regular changes to those passwords, is an adequate approach to cyberattack prevention. On the contrary: Relying primarily on passwords puts you at grave risk.

81% OF HACKING-RELATED BREACHES (50% OF ALL BREACHES) LEVERAGED WEAK OR STOLEN PASSWORDS

Verizon Data Breach Report

IMPROVE PASSWORDS

Require employees to use a different password for each access point they encounter and provide ongoing security training. Passwords should be randomly generated. Length matters more than complexity, but passwords should be required to include a variety of characters..

USE PUSH NOTIFICATIONS

Do not rely on passwords alone; insist on multi-factor authentication that includes a push notification that is delivered to the individual user's device and ensure that push notifications expire quickly - within 30-60 seconds.

USE A PASSWORD MANAGER

To prevent your employees from becoming complacent about using unique, complex passwords at every access point, employ the use of a password manager so that your employee must only remember one password.

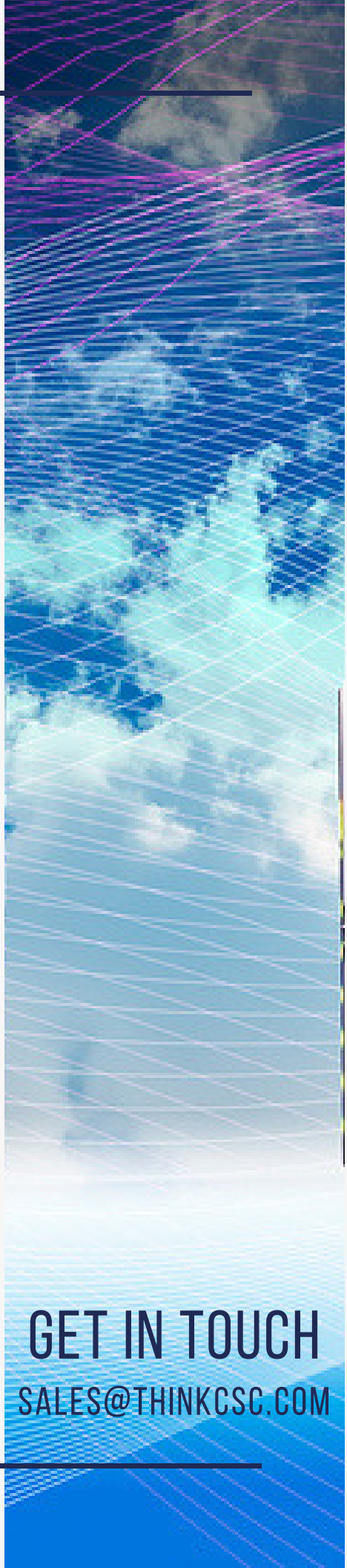
There is no single solution that will protect you from every possible attack. It's all about risk identification and management. Two areas at risk for causing the most damage – credentials that are up for grabs on the Dark Web and human error – can be minimized with the proper tools, training, and support.

Creating a cybersecure team isn't difficult but it is critical. Given the rise in cyberattacks over the last decade and, especially, the recent, coordinated, worldwide ransomware attack, providing cybersecurity training to employees is essential for every organization. Your organization needs to operate in a culture of zero trust – a belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

PARTNERING WITH THINKCSC

thinkCSC has more than 20 years of experience helping clients exceed their goals. We understand that business and technology are so intertwined that you can't be strategic about one without the other. We offer customized and bundled outsourced IT services you need to achieve your objectives; increase efficiency, productivity, and agility; cut down on IT costs; and ensure you have a competitive edge. Whether you want to outsource most or all of your infrastructure management, or if you simply want to optimize the systems already in place, thinkCSC provides personalized IT expertise that saves money and provides the manpower that ensures your infrastructure is always an asset – never a liability.

At thinkCSC, we believe that in order to achieve maximum success, regardless of the size or type of your organization, you must make IT an integral part of your overall business strategy and partner with IT professionals who not only understand how to leverage technology to their advantage but who are also committed to understanding your business goals and aligning your IT strategy to theirs. We pride ourselves on having the best business-savvy technical experts in the industry. If you would like to learn how to create an IT security strategy aligned with your organizational goals, contact thinkCSC for more information.



GET IN TOUCH

SALES@THINKCSC.COM