Password Management Tools

Strong and secure passwords are a must-have IT investment for businesses

White Paper

CRA™
Transform IT
Computer Resources of America

Computer Resources of America

https://www.consultcra.com/

Password management tools-A must-have IT investment for businesses

As a business owner, you know how important it is to keep your business data safe and secure. Perhaps you have already even invested in cybersecurity solutions such as antivirus platforms and firewalls. But, do you have a password management system? A lot of companies spend sizable amounts fortifying their IT infrastructure, but end up ignoring this one basic element--passwords. In reality, password security should be a bedrock of any cybersecurity planning they undertake. Research points out that more than 80% of data breaches happen due to password hacking, meaning that poor password hygiene is responsible for a majority of cybercrimes that follow data breaches. To make sense of this statistic better, let's first look at what constitutes poor password hygiene.

Using simple passwords

Often passwords that are easy-to-remember are easy-to-hack. Do you use passwords such as password, password1234, delta123, etc.,? If yes, then you should be changing them at the earliest to something less obvious.

Repeating passwords across platforms

As another solution for remembering passwords, people tend to use one, single password universally. This dilutes the password even if it is a strong one. Plus, there's always the risk of the password being hacked at one place and putting the data stored at all other places also at risk.

Unauthorized password sharing

Unauthorized password sharing for the sake of getting things done faster is a very real problem. For example, someone is on leave and someone else needs access to a particular file from their computer. The employee who is on leave shares the password and that can result in a security compromise.

Writing down passwords

This the most obvious, yet oft-made password mistake. Just so they don't forget the passwords, people tend to write them down on a piece of paper, a diary or sometimes, store it on their phone. You know what can follow if the piece of paper or diary or the phone is stolen. Same goes for storing passwords on email and if the email server is compromised.

Not revoking access on time

Cases where ex-employees log-in credentials were used to hijack company data are not unusual. When companies forget to revoke the access of employees as they move out of the department or organization, they are leaving a gaping cybersecurity hole open which is easy to take advantage of.

Not updating passwords

Using the same password for years or even months can be risky. Passwords should be changed every 3 months and perhaps even sooner for critical applications.

Single factor authentication

For the more critical areas, multi-factor authentication must be deployed. Relying on password alone is a huge cybersecurity risk. Multi-factor authentication includes tokens, biometric authentication, OTPs, etc., which make it very difficult to hack into the application.

In summary, these are some of the basic password mistakes that almost everyone is guilty of at some point. You can prevent these from happening in your organization by educating your staff about them and training them to cultivate good password hygiene. However, as we all know, there's always a degree of uncertainty present where human behavior is involved. This is where password management tools come into play.

Password management tools are software programs that put up enough security and safety mechanisms in place to ensure there's no password breach.

All passwords are encrypted and stored privately, so no one, other than the authorized user has access to their passwords.

It takes care of timely password update reminders and password reset, so you don't have to worry about them.

Password management tools make it easy for you to enforce role-based access permissions. For example, a data entry executive may be able to enter data into the sheet only once, and may need authentication from the manager to edit the data, or only someone at the managerial level may be allowed to make edits to the data.

Some password management tools support multi-factor authentication, thus helping you make this important security feature a part of your data security process.

Password management tools also offer administrators and managers a full view of the log-ins and also generate detailed access reports. You will know which user logged in, at what time, using which device. Some password management tools can send alerts when there's a log-in from devices, networks or locations that are unusual.

There are a variety of password management tools available on the market. While their basic function is the same–keeping your passwords secure–password management tools can offer you a lot more in terms of data security. Consult with an MSP who deals with cybersecurity as they can help you pick the password management tool that's right for your business. But, remember, at the end of the day, there's no substitute for good password hygiene, so no matter what tool you deploy, you still need to educate and train your employees to follow good cybersecurity practices.

For more information please contact,
Kristel Broward | Computer Resources of America
Phone: 2123764040 | Email: kristelb@consultcra.com