5 Dangers of Leaving Password Management to Employees

Devolutions

OVERSIGHTS AND MISTAKES IN THIS AREA ARE POTENTIALLY JUST TOO CATASTROPHIC

Employees who can "manage themselves" are highly valued. After all, nobody wants to (or should want to) micro-manage every little thing an employee does. Micro-managing is not only tedious for everyone involved, but it's inefficient and costly. And frankly, for many SMBs that have limited staff, it's not even an option. Everyone needs to manage themselves to an extent or the business will fold.

However, there are a few functions that shouldn't be assigned to employees regardless of how competent and reliable they are, and at the top of the list is password management. Oversights and mistakes in this area are potentially just too catastrophic.

Here are 5 dangers of leaving password management to employees:

1. They Choose Weak Passwords

Largely due to security fatigue, many employees choose weak, easy-to-remember passwords. Unfortunately, this isn't just convenient for employees; it's also convenient for hackers. The 2019 Verizon Data Breach Investigation Report (DBIR) found that 80% of hacking-related breaches involved compromised and weak credentials.

2. They Use the Same Passwords

Another consequence of security fatigue is that employees too often use the same password across multiple accounts. Even if this password is suitably complex, it is nevertheless extremely risky since it potentially provides hackers with a master key. A survey by LogMeIn found that 59% of people use the same password for multiple accounts, and most of them use the same password for as long as possible.

3. They Store Passwords Insecurely

Employees who manage their own passwords are prone to storing them insecurely — not necessarily because they're being reckless (although some are), but because they want easy, convenient access. A survey by Digital Guardian found that 39% of people write their passwords down on a piece of paper, and 10% keep their passwords in a file on their computer.

4. They Share Passwords Insecurely

Like the rest of the general population, most employees safeguard their personal information, such as their credit card number, social security number, and so on. However, many employees are far less stringent when it comes to sharing passwords with colleagues. Research by SurveyMonkey has found that despite the risks, 34% of employees admit to sharing passwords at work.

5. They Use Their Own Password Management Tool

The good news is that some employees who manage their own passwords use their own password management tool. This is certainly better than storing passwords on spreadsheets or choosing

"password1234" for their accounts. But the bad news is that these employees do not have secure access to group passwords, and the standards and rules they set (or which are set by their tool) may fall short of company protocol —and this creates a vulnerability that hackers can exploit. Also, something even worst than group passwords is that employees maintain control over the passwords even after employment termination. Past employees having access and control over related systems can be dangerous for the whole organization.

Solving the Problem

Enabling or obligating employees to manage their own passwords may seem cost-effective and efficient, but the risks far outweigh the rewards. This is especially true for small businesses, since 60% of them disappear within six months of a major cyber attack.

The way to solve this problem is clear: don't let employees manage passwords! Instead, centralize this critical function within IT, and at the same time provide employees with education and coaching — perhaps through a cybersecurity training platform — so they can be part of the security solution, instead of unintentionally part of the problem. After all, the job that could be lost in the aftermath of a costly breach or hack might be their own.

How Devolutions Can Help

Devolutions offers two solutions to help businesses of all sizes centralize and control password management without slowing down administrators or employees: Devolutions Password Server and Devolutions Password Hub.

Devolutions Password Server enables businesses to control access to privileged accounts and manage remote sessions through a secure solution, which can be deployed on-premises. When used in combination with Remote Desktop Manager, Devolutions Password Server functions as a single pane that integrates password and credential vaulting with a robust, efficient remote connection management solution. Request a 30-day trial.

Devolutions Password Hub is a secure and cloud-based password manager for teams that is controlled by IT pros. It allows businesses to securely vault and manage passwords and other sensitive information through a user-friendly web interface that can be quickly, easily and securely accessed via any browser. Request a free 30-day trial.