Devolutions

The Importance of Using a Password Manager

IT'S A "BAD NEWS, GOOD NEWS" KIND OF STORY

Recently, Devolutions surveyed decision-makers in SMBs worldwide on a variety of key cybersecurity practices and trends. Answers to each question are presented in this report and highlighted in this infographic.

One key takeaway from the survey is how some **SMBs are — and some aren't — using a password manager.** So it's a **"bad news, good news"** kind of story. Let's start with the former:

The Bad:

- **47% of SMBs still allow end users to re-use passwords across personal and professional accounts** — despite the fact that this is a major security risk.
- **29% of SMBs rely on human memory for storing passwords — which is a "worst practice"** instead of a best one, since the average business user must keep track of a whopping 191 passwords, requiring them to input credentials for various websites and apps 154 times per month. It's just too much for human memory.
- **15% of SMBs do not use ANY tools to protect or manage passwords.**

The Good:

- **81% of SMBs store credentials in a personal password manager to protect their personal data.**
- **88% of SMBs provide some form of cybersecurity education to their end users** (even though this really should be 100%, it's a sign that things are headed in the right direction!).
- **76% of SMBs believe that password managers are best suited for validating and monitoring good password practices.**

The Solution

There are three things that all SMBs should be doing to keep their data, customers, and reputations safe: **use a password manager, implement best practices, and educate end users.**

1. Use a Password Manager

The first (and most obvious) thing is to use a password manager — **a corporate version for the organization**, and **a personal version for each end user to store their non-business credentials and other sensitive information.** Research has shown that 81% of data breaches are caused by compromised, weak, and re-used passwords, while 29% of all breaches (regardless of attack type) involve the use of stolen credentials.

At Devolutions, we offer **Password Hub Business for organizations**, and **Password Hub Personal for end users:**

- Password Hub Business is a secure and cloud-based password manager for teams. It empowers organizations to easily and securely vault and manage business-user passwords, along with other sensitive information, through a user-friendly web interface that can be quickly, easily, and securely accessed via any browser. Click here to learn more.
- Password Hub Personal is our safe, easy-to-use, and free password manager for individual users who want to store personal passwords in a secure vault, and it is only accessible to them. Users can easily create and access their own Password Hub Personal from their Devolutions Account. Click here to learn more.

2. Implement Password Management Best Practices

Here are some of the **password management best practices that SMBs should implement right now:**

- **Use MFA**
- **Use complex passphrases**
- **Change passwords when there is evidence of a compromise**
- **Compare passwords against a list of known weak and compromised passwords**
- **Enforce just-in-time access for privileged accounts**
- **Enforce a password history policy**
- **Eliminate password re-use**

3. Educate End Users

An **effective and affordable way to help end users** be part of the solution — instead of unintentionally contributing to the problem — is through a **cybersecurity training platform**. This is a portal that provides end users with **self-paced, hands-on, skills-based threat detection and mitigation training in a live and dynamic simulated environment.** Threats can include ransomware, phishing, DDoS, and so on, and the training program can be customized to cover specific topics, such as social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, etc. Plus, supervisors and managers can track each end user's progress and development, and provide additional coaching or resources as required.

Read the Report

We invite you to **download the State of Cybersecurity in SMBs in 2020 report here**, and **view the accompanying infographic that highlights our key findings.**