



The State of Password Security in 2020 for SMBs: The Good, the Bad & the Ugly



The GOOD, the BAD & the UGLY

Devolutions surveyed Information Technology decision-makers in small and mid-sized businesses (SMBs) across the world in order to understand the state of password security in 2020 and moving forward.



DID YOU KNOW

Global cybercrime revenues have reached a staggering **\$1.5 trillion** per year

and the average price tag of a data breach is now **\$3.9 million** per incident.

THE GOOD



88% of SMBs provide some form of cybersecurity education to their end users.

81%

of SMBs store credentials in a personal password manager to protect personal data.

77%

of SMBs have a minimum password length and complexity policy.



76% of SMBs believe that password managers are best suited for validating and monitoring good password practices.

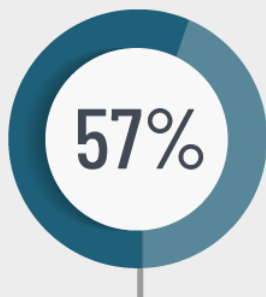
4,752 SMBs do not allow password re-use across any accounts.

THE BAD

88% of SMBs are more concerned with the privacy and security of their online data now than they were five years ago.



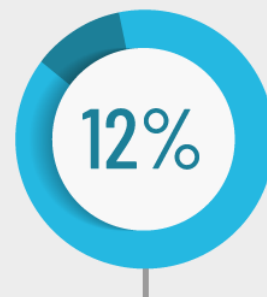
72% of SMBs believe that cloud security will become a bigger concern in the next three years.



of SMBs say they have experienced a phishing attack in the last three years.



of SMBs believe that IoT threats will get worse in the coming years.




of SMBs do not know if they have faced a cyber attack in the last year.


THE UGLY



97%

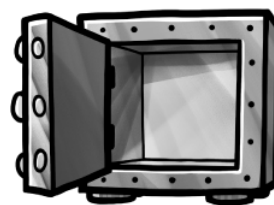
of SMBs believe that end users are at least somewhat responsible in the event of a data breach.

78%  of SMBs consider a PAM solution at least somewhat important to their organization's cybersecurity program

76%  of SMBs do not have a fully deployed PAM solution in place.

62% of SMBs do not conduct a security audit at least once a year, and **14%** of SMBs never conduct security audits at all.

47%



of SMBs allow end users to re-use passwords across personal and professional accounts.

15% of SMBs do not use any tools to protect or manage passwords.



HOW TO STAY SAFE

When it comes to cybersecurity awareness and protection, SMBs are generally trending in the right direction. However, there are still some worrisome — and in some cases alarming — vulnerabilities that, if exploited by hackers, could lead to costly and potentially catastrophic consequences. In addition, there are the ever-present threats posed by negligent end users who accidentally trigger data leaks. To protect their data, customers, reputation, and organization, SMBs should implement the following five recommendations:

RECOMMENDATIONS

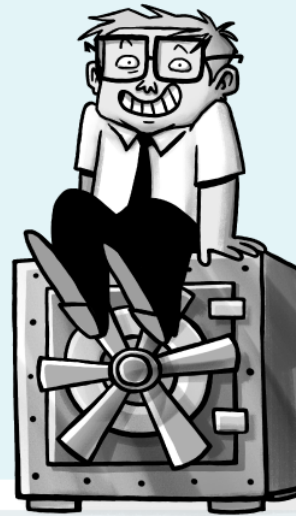
1 - Implement a Privileged Access Management (PAM) Solution

External hackers and internal rogue users have upped their game, and SMBs must do the same by implementing a PAM solution that delivers seven must-have characteristics and features like **Secure Password Vault, Account Brokering, as well as Role-Based Access Control.**

2 - Enforce Strong Password Management Policies

SMBs are urged to adopt and enforce the following password management policies, which are based on advice from various reputable sources, such as NIST and the Center for Internet Security:

- Use 2FA
- Use a Password Manager
- Use Passphrases
- Change Passwords After 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 - Implement the Principle of Least Privilege (POLP)

POLP is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more and nothing less. There are a number of POLP best practices that SMBs are strongly encouraged to adopt: **Evaluate Access Levels, Deploy One-Time-Use Credentials, Enforce Account Separation, and Continuously Monitor and Regularly Audit.**

4 - Implement Segregation of Duties (SoD)

In recent years, the concept of SoD has expanded into the cybersecurity space to prevent conflicts of interest, wrongful acts, fraud, abuse, and the building of secretive “silos” around activities. SMBs are urged to adopt different SoD best practices like **Analyze Access Levels, Align Tasks with Roles, as well as Train End Users.**

5 - Provide End Users with Cybersecurity Training

While there are several ways to deliver cybersecurity training, among the most effective for SMBs is enrolling their team in an online cybersecurity 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. Key topics that can be covered include **Social engineering, Email security, Mobile device security, Safe web browsing, and Safe social networking.**

Source

<https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually>
<https://www.ibm.com/security/data-breach>

**CONTROL
THE IT
CHAOS**