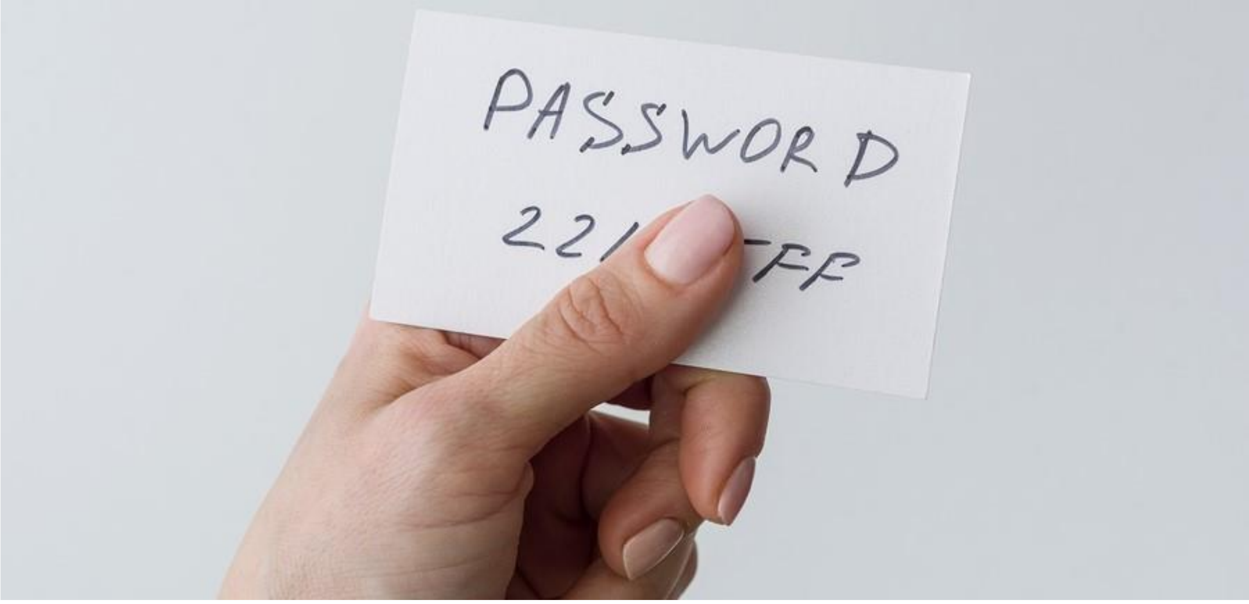
Close the Door to Hackers by Purging Weak Passwords



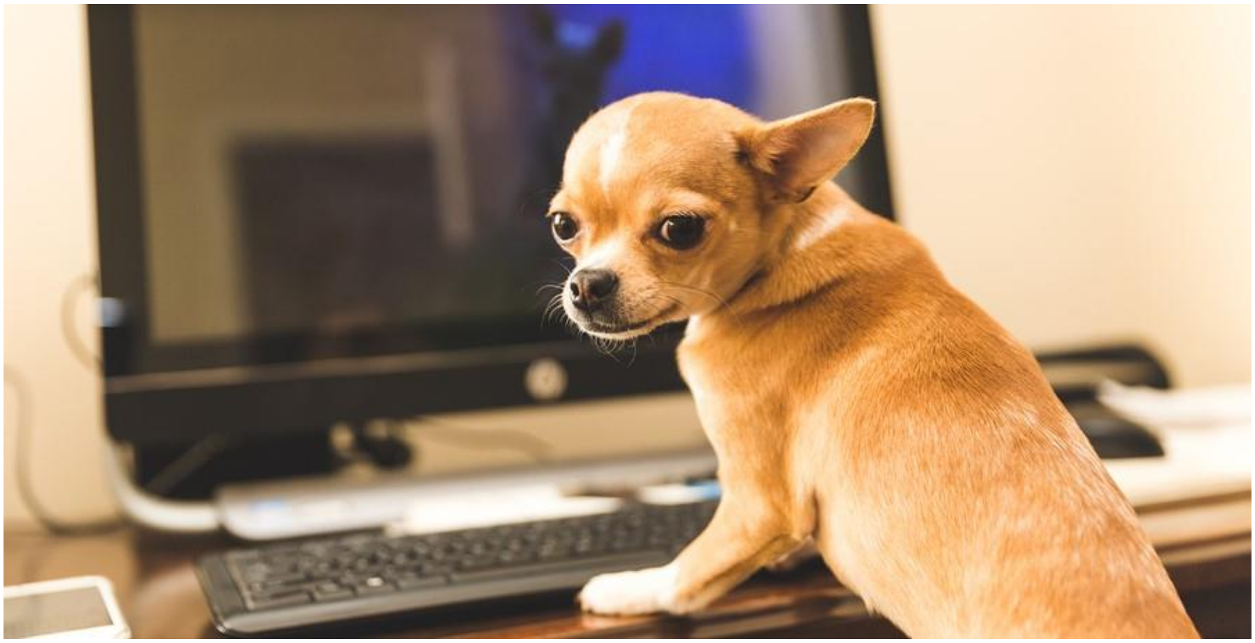
Marriott, Target, Home Depot and others have made headlines in recent years for data breaches that affected millions of customers. But did you know that 43 percent of breaches hit small businesses? Limited resources and lack of expertise often leave security gaps in smaller organizations, compounded by weak passwords and other risky practices.

For instance, in the Target attack, hackers stole credentials from a much smaller company in the retailer's supply chain. They then used the stolen credentials to access Target's network. Sadly, similar scenarios play out over and over again. And users make the job much easier for criminals by opting for convenience over security.

Common Password Mistakes

No business wants hackers in their system. But unfortunately, by continuing to allow weak passwords, they leave the welcome mat out and the door unlocked. Consider whether you have seen any of these common password mistakes in your business.

For instance, do multiple techs share passwords for privileged accounts or keep a list of passwords stored in a spreadsheet? Perhaps you or other employees re-use passwords to avoid trying to remember dozens of different credentials. These password practices may save some time in the short term, but they leave your business vulnerable to attack.



Hackers Love Weak Passwords

According to the most recent Verizon Data Breach Investigations Report (DBIR), compromised credentials play a factor in 80 percent of hacking-related data breaches. Cyber criminals exploit weak passwords in several different ways. Some of the most common include:

1) **Credential stuffing** – Hackers purchase lists of credentials stolen from sites with poor security. They then test these credentials against other websites. Statistically, they have a good chance of finding that users have re-used passwords on multiple sites.

2) **Social engineering** – Phishing plays a factor in the majority of cyber crimes. Criminals pose as legitimate businesses or other trusted source, tricking their victims to reveal credentials.

3) **Password spraying** – Hackers test a list of common passwords to gain access to an account. For instance, recent reports indicate that over 23 million accounts still use "123456" as a password.

4) **Keylogging** – Using a publicly-available tool, bad actors record keystrokes to capture passwords. The keylogger begins running when the computer starts up and then sends a log of keystrokes to the hacker. Some of these tools can be configured not to display in the Windows Task Manager, making them difficult to detect.

5) **Dictionary attacks** – Using password-cracking tools, criminals can test thousands of passwords in a matter of minutes. In a dictionary attack, they actually try every word in the dictionary as a possible password.

In addition, leaving passwords on sticky notes or in publicly available files leaves users and businesses open for more targeted attacks. Consider the password posted next to a server or PC. Anyone with physical access to the computer can then gain access to the network.

How to Protect Your Business

The Ponemon Institute reports that the average cost of a data breach has risen to $3.92 million. Add to that the inevitable damage to business reputation, and the loss can prove catastrophic for a small business.

Businesses that take steps to ensure against weak passwords significantly strengthen their defense against cyber attack. The Verizon report urges the use of multi-factor authentication and password managers. In addition, password policies should emphasize and enforce good password hygiene, particularly for privileged accounts.

The data security experts at eMazzanti have helped hundreds of small businesses implement comprehensive cyber security. We keep up-to-date on the latest developments in business security so that we can customize a solution build for your needs.