TOP 10 Best Practices for Effective Password Management

If users had to remember only one password, life would be simple enough. But as computing resources multiply, users are expected to remember numerous passwords that get more and more complex and have to be changed frequently to thwart hackers. No mere human can keep up with all that. But passwords aren't going away; they remain a valuable security tool. This Top 10 card lists best practices to set and enforce an effective password management policy.

1

Complexity is good: Passwords should be hard to crack. As opposed to just about everything else in IT, complexity is desirable in passwords. Strong passwords employ combinations of lower and uppercase letters, digits, punctuation and special characters (FL!8mno#). An even more secure alternative is to use a passphrase containing several words (makemoresoup), but not commonly used expressions from movies, songs or everyday vernacular.

2

Avoid easy guesses: This should be a given, but about three-quarters of attacks on corporate networks involve weak, easily cracked passwords. To avoid weak passwords, tell users to stay away from names of family members, pets, employers or favorite bands. In fact, they should shun complete words altogether, especially default passwords such as "password" and "admin."

3

Do not share: When it comes to passwords, sharing is decidedly not caring. Instruct users not to share them with anyone, including friends, family, partners and colleagues – no matter how much they trust the person. A prohibition on sharing should be part of a corporate security policy, and may even be required by applicable data-protection regulations. Remind users they are responsible for the misuse of any password they share.

4

Do not recycle: Recycling passwords for multiple websites, applications and services is a bad idea. Doing so means a hacker needs only crack one password to gain access to various accounts – including those with sensitive and confidential information. Unfortunately, studies show more than half of all users recycle one password for multiple accounts, putting themselves and their employers at risk of a security breach.

TOP 10 Best Practices for Effective Password Management

5 **Embrace change:** Updating passwords regularly helps thwart hackers because they can't use them after they expire. Require password updates periodically, say, every 45, 60 or 90 days. Tagging a number to the previous password or making some other slight variation isn't enough; the new password should be substantially different.

6 **Mind the storage:** With so many passwords to remember – as many as 20 per user – it's virtually impossible to remember them all, especially when they change periodically. Use a password management solution or, at the very least, tell users to store passwords in a safe place, such as an encrypted file. What you definitely don't want is people keeping a list of passwords next to their computers, where it is easily found.

7 **Add a step:** Even remembering one complex password can be a challenge. Multifactor – or two-factor – authentication effectively addresses this challenge. Instead of forcing users to search their memory to remember a password, multifactor authentication provides a one-time password or PIN through a smartphone, token or fob. This approach is cost-effective and strengthens your security practices

8 **Keep it central:** Anything that can be managed from a central location will always be easier, cheaper and less time-consuming. A password management system keeps things simple by automating strong password generation and update requirements, and managing user permissions. Passwords are stored and organized in secure vaults, easing the pressure on users to remember and store all their passwords.

9 **Make it a single:** Regardless of how many applications, websites and systems users access, what if they didn't have to log on to each separately? Single sign-on (SSO) makes this possible via a specially designed website that allows access to everything else. Combined with multi-factor authentication, SSO strengthens security and boosts productivity. Time wasted on resetting forgotten passwords is, instead, used to complete tasks.

10 **Manage smartly:** The better you manage your password policies, the less likely you are to suffer a breach that could ruin your reputation, incur hefty fines and invite regulatory scrutiny. A password management system helps secure your resources by safely storing, synchronizing and auditing passwords from devices on premise and in the cloud. Passwords are kept up to date and easily accessible when you need them.