

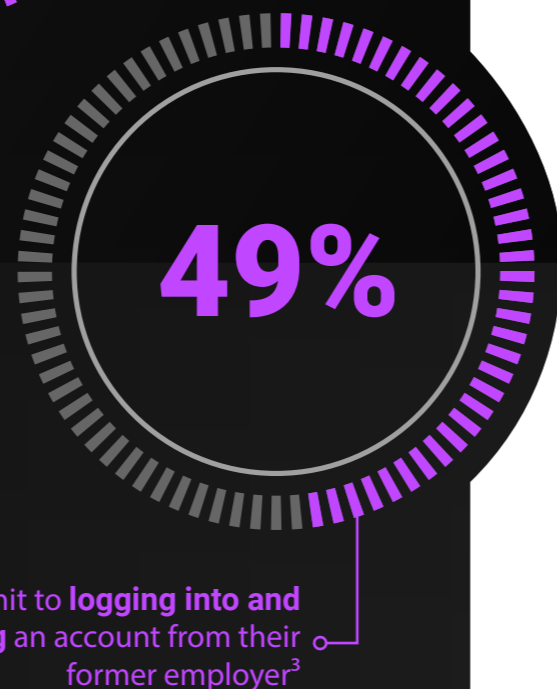
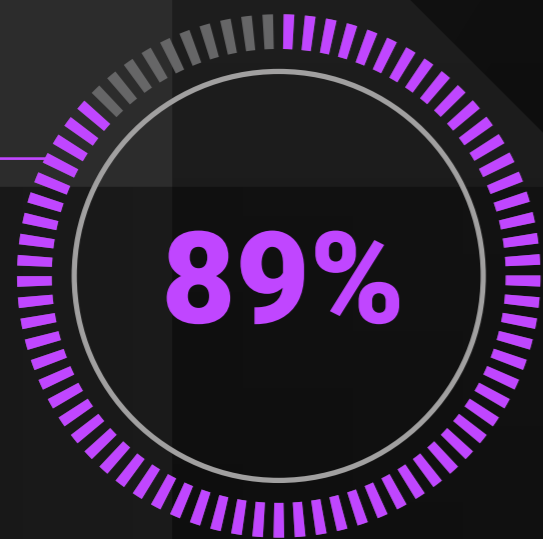
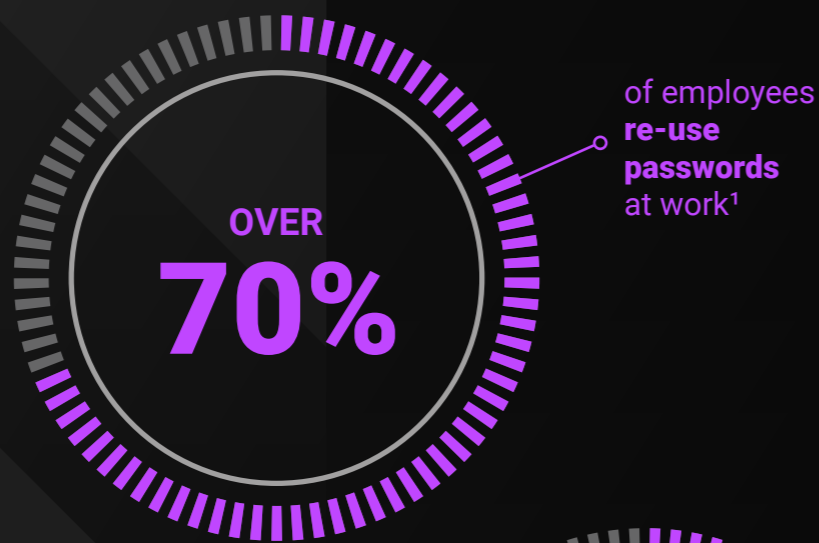


N-ABLE

5 TIPS FOR PREVENTING HARM AFTER AN EMPLOYEE LEAVES

Poor password management can open businesses to significant risk, especially when employees leave.

Consider the following:



REQUEST A DEMO

N-able™ Passportal™ + Documentation Manager lets you safeguard accounts with strong passwords, quickly revoke access when needed, and maintain documentation even after someone leaves. Request a demo today.

So how do you help ensure a smooth, safe transition following an employee departure? Follow these five tips:

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE



1

Implement a password tool with granular permissions. Make sure employees have only the level of access they absolutely need.

REVOKE ACCESS AND AUDIT CREDENTIAL USAGE FOLLOWING A DEPARTURE



3

Shut down access immediately when someone leaves, and monitor accounts for unauthorized access attempts.

AUTOMATE PASSWORD AND DOCUMENTATION MANAGEMENT



5

Password and documentation management can be a lot to handle, and it can lead to employees becoming overwhelmed and falling into bad habits.



STANDARDIZE KNOWLEDGE SHARING

2

Use centralized software to help ensure client information is properly documented, safeguarded, and accessible in the case of employee exit.



ROTATE PASSWORDS REGULARLY

4

Keep passwords fresh by rotating credentials regularly via a centralized system. This can prevent hackers from exploiting old passwords.

Password management software relieves the burden while keeping your business safe.

70%

of hacking-related breaches leveraged either stolen and/or weak passwords⁴.

Keep Your MSP safe after employee departures.