Today’s headlines are filled with news of public data breaches. However, even with all of this public awareness, the majority of individuals involved in a data breach are unaware their credentials might have been compromised. And, unfortunately, even when people are aware of a breach, they are slow to change the affected passwords.

Enter credential-stuffing. An attack where cybercriminals use passwords stolen from one breached website to attempt to break into other sites or networks via software and botnets.

As an employer, if even one of your company’s employee’s privileged account credentials are exposed via a public data breach, your organization is at risk.

The best way to protect your employees and your company is to detect and defend against these attacks is BreachWatch® by Keeper. It constantly scans employees’ Keeper vaults for passwords that have been exposed on the dark web from a public data breach and notifies the user to take action. It also informs the administrator whether that employee has resolved the exposed password, or ignored it.

For more information about BreachWatch or to schedule a demo, visit keepersecurity.com/breachwatch or email sales@keepersecurity.com

Sources:
1 Akami, “Credential Stuffing: Attacks and Economies”, April 2019

© 2019 Keeper Security, Inc.