KEEPER® | PRESS RELEASE

New Survey Finds Enterprise Password Security is as Flimsy as a Sticky Note

Keeper Security study uncovers U.S. employees' bad habits when saving and sharing work-related passwords, presenting an unprecedented cybersecurity risk for their organizations.

CHICAGO, IL, April 6, 2021 – A majority of Americans are using sticky notes to store their work-related passwords, and most of them admit to having lost these notes, according to Keeper Security's new **Workplace Password Malpractice Report**. The report surveyed 1,000 U.S. employees to better understand current password management practices and how these habits have evolved over the past year.

A Sticky Situation with Password Management

According to the report, more than half of American employees (57%) are currently writing down work-related passwords on sticky notes, indicating large-scale carelessness when it comes to password management and potentially leading to significant cybersecurity risk. Additionally, two-thirds (66%) have lost these sticky notes in the past, making it difficult to know who ultimately has access to sensitive company information.

A majority of respondents (62%) said they have a notebook or journal where they store logins and passwords, and 81% of those say they keep these notebooks next to or close to their work devices, where they can be easily accessed by any passerby. This trend has increased in the remote work era, as most workers (66%) report they're more likely to write down work-related passwords while working from home than they are in the office.

Sharing Is Caring? Employees Seem to Think So

Perhaps more concerning, a majority of U.S. employees (62%) say that they've shared a work-related password over text message or an email, where the password could be intercepted in transit by cybercriminals. Nearly half (46%) report that their company directs employees to share passwords for accounts that are used by multiple people. Additionally, one-third (34%) of respondents have shared their work-related passwords with colleagues on the same team, and 31% have shared this information with their managers. A small but significant percentage of respondents, 14%, have shared work-related passwords with a significant other.

Best security practices dictate that an employee's accounts should be disabled as soon as the individual leaves the company, but nearly a third of respondents (32%) admit to having logged onto an online account that belongs to a former employer.

Personal Details Remain a Popular Pick For Employee Passwords

Employees are incorporating personal details into their work-related passwords, even though social media makes it easy for cybercriminals to find and exploit this information. Over a third of employees (36%) have used their company's name when creating a new password for a work-related account, another third (34%) have used their significant other's name or birthday, and 31.4% have used their child's name or birthday while creating a work-related password.

"The transition to a remote working environment has led to even more reckless password management practices, which is very worrying," said Darren Guccione, CEO and Co-Founder of Keeper Security. "As most employees work from the comfort of their homes, they have become too comfortable with how they create, store and then share these passwords with family and colleagues. The lack of cybersecurity hygiene not only puts the individual at risk, but can also present a wide range of negative consequences for their organization. It's important to remember that following proper security guidelines in a work-from-home environment is just as critical as in an office environment."

Additional Notable Findings:

- A majority of employees (53%) keep password-protected personal accounts on their work devices.
- 43% reveal they currently use the same password for both personal and work-related accounts.
- Nearly half of employees (49%) are currently saving work-related passwords in a document in the cloud.
- 50% say they currently save passwords in a document on their desktop.
- More than half (54%) currently save work-related passwords on their phone.

Join Keeper CEO and Co-Founder Darren Guccione and world-renowned author and cybersecurity expert Dr. Eric Cole, as they do a deep dive into the findings of the Workplace Password Malpractice Report and discuss the findings and how to safeguard your organization **Tuesday, April 13th at 1 PM CST**.

To download a copy of the Workplace Password Malpractice Report, infographic and more, visit our dedicated **resources hub**. For more information on Keeper Security, or how to defend your organization from password-related data breaches, go to **keepersecurity.com**.

Methodology

Keeper Security contracted with Pollfish to conduct this survey of 1,000 full time employees in the United States. Only individuals who use passwords to log into work-related online accounts were included. The survey was completed in February 2021.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. In 2020, Keeper was named PCMag's Best Password Manager of the Year & Editors' Choice for the third time. Keeper has also been named PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).