Keeper Security Report Finds People Are Overwhelmed by Too Many Passwords

Research finds 62% of people globally feel overwhelmed managing passwords, yet many exhibit overconfidence in their cybersecurity practices.

LONDON, UNITED KINGDOM, July 30, 2024 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, today released Fortifying Cyber Resilience: Insights Into Global Cybersecurity Practices. The survey of more than 6,000 respondents globally finds that 62% of people are worried about managing too many passwords, accounts and logins. This statistic underscores a growing concern among users about the complexity of password management. The report reveals critical insights into current security practices, highlighting both strengths and gaps that need to be addressed.

Overconfidence in Cybersecurity Habits

Many individuals exhibit overconfidence in their cybersecurity practices – particularly regarding password management. The survey shows that while 85% of respondents believe their passwords are secure, over half admit to sharing their passwords. Additionally, 64% of people feel confident in their cybersecurity knowledge despite 2 in 5 admitting to password reuse and 24%

"

The data reveals a cybersecurity paradox where people feel confident in their cybersecurity knowledge, yet are frequently targeted by cyber attacks and scams."
Darren Guccione, CEO and Co-Founder of Keeper Security

writing down their passwords.

Popular Password Management Practices

Risky password management practices further emphasise the disconnect between widespread cybersecurity confidence and the actual state of global cyber hygiene. Keeper's research finds

the most common methods for managing passwords include:

- Relying on memory (26%)
- Writing them down (24%)
- Storing them in a browser or phone notes app (19%)

While many people think their passwords are secure, their behaviours indicate a critical need for advanced tools and comprehensive education. Adopting a password manager, creating strong and unique passwords for every account, and enabling Multi-Factor Authentication (MFA) everywhere it's available, can significantly enhance an individual's personal cybersecurity.

Password Sharing Still Prevalent

Despite crackdowns by streaming services, over a third of respondents (34%) admit to sharing passwords for streaming sites. The other most commonly shared passwords include:

- Shopping accounts (22%)
- Personal emails (20%)
- Social media (16%)
- Work/school emails (16%)
- Bank account passwords/pins (15%)
- Work productivity platforms (13%)

Work To Be Done

The widespread challenges in bolstering global cyber hygiene demonstrate the need for education on the risks of insecure password sharing and management, as well as the adoption of solutions that will bolster cyber resilience. Despite leading industry experts and government cybersecurity agencies recommending the use of a secure password manager to store, generate and securely share passwords, Keeper's research shows that only 12% of respondents are doing so. These tools are crucial for managing online accounts and identities safely.

"The data reveals a cybersecurity paradox where people feel confident in their cybersecurity knowledge, yet are frequently targeted by cyber attacks and scams," said Darren Guccione, CEO and Co-Founder of Keeper Security. "This disparity emphasises that knowledge alone cannot mitigate cyber risks; using tools like password managers and following best practices are vital for reducing cyber risks."

Keeper's Fortifying Cyber Resilience: Insights Into Global Cybersecurity Practices report underscores the ongoing challenges that security practitioners face in guiding people to take timely actions to protect themselves online. Empowering individuals through education and technology is critical to safeguarding sensitive data and defending against today's sophisticated cyber attacks and online scams. By staying informed and adopting best practices, individuals can

proactively defend themselves against the most prevalent cyber threats.

Download the [full report](#) to learn more.

\###

About Keeper Security
Keeper Security is transforming cybersecurity for people and organisations around the world. Keeper's affordable and easy-to-use solutions are built on a foundation of end-to-end encryption, zero-trust and zero-knowledge security to protect every user on every device. Our zero-trust privileged access management solution deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging.

Charley Nash
Eskenzi PR
charley@eskenzipr.com