KEEPER®

Fortifying Cyber Resilience

Insights Into Global Cybersecurity Practices

Overview

Digital services permeate every area of our lives, in all corners of the world – making cybersecurity a global concern. Keeper Security's report, *Fortifying Cyber Resilience: Insights Into Global Cybersecurity Practices*, explores universal trends in cybersecurity to help stakeholders, including governments, businesses and cybersecurity professionals, develop effective strategies to address global cybersecurity threats.

Keeper surveyed 6,000 individuals in Australia, New Zealand, Singapore, Indonesia, Japan, France, the UK, US and DACH regions to gain insights into the efficacy of current cybersecurity awareness programs and educational initiatives. Despite extensive efforts to educate the public on best practices, the success of cyber attacks and online scams indicates potential gaps in both knowledge and implementation. By assessing the security behaviors and practices of a diverse audience, we can pinpoint areas where public understanding is lacking. This information is vital for designing more effective awareness campaigns and training programs to bridge these gaps and empower individuals to protect themselves online.

Understanding the public's cybersecurity behaviors aids in the development and refinement of technology solutions and policies to build resilience. For instance, the survey reveals a significant number of people do not update their devices due to inconvenience or fear of performance issues. This data can guide tech companies in creating more seamless and user-friendly processes to enhance security. Similarly, given that many users rely on memory and physical notes for password management, there is a clear need to promote and simplify the adoption of password managers. Policymakers can leverage this data to draft regulations and guidelines that encourage safer online behaviors and protect consumers from cyber threats.

The global survey on cybersecurity practices also fosters international collaboration and knowledge sharing. As cyber threats transcend borders, countries can benefit immensely from learning about effective strategies and policies implemented elsewhere. By sharing survey results and collaborating on solutions, nations can build a more resilient global cybersecurity infrastructure. This collective effort not only enhances individual security but also contributes to the overall stability and security of the broader digital ecosystem.

Key Findings

Survey data indicates cybersecurity remains a critical issue globally, with a significant percentage of individuals falling victim to online scams and cyber attacks. It also sheds light on the disparity between user behaviors and user perceptions regarding cybersecurity, as well as insight into the effectiveness of current security practices and where security gaps must be addressed.

Prevalence of Cyber Threats

More than half of global respondents reported experiencing an online scam or cyber attack in the past year.

Notably, over a quarter (26%) of individuals were targeted by fake ads or online giveaways. The global economic downturn is likely contributing to the rise in this attack vector, as financially strained individuals may be more susceptible to online scams promising financial relief or rewards. This trend highlights the urgent need for heightened awareness and education about the common tactics employed by cybercriminals and the red flags to watch out for.

26%

Were targeted by fake ads or online giveaways

The most common incidents

Fake ads or online giveaways

Phishing

Smishing (phishing by text)

Vishing (phishing by phone)

Device Update Practices

Encouragingly, a majority of users are proactive about updating their devices, with 37% installing updates as soon as they are available and 35% having automatic updates enabled.

It is encouraging that many users diligently update their devices. Nonetheless, the barriers faced by those who do not update promptly – such as lack of knowledge, perceived inconvenience and fears about performance – highlight areas where enhanced user education and more user-friendly update mechanisms could make a significant impact.

Primary reasons 25%+ of people delay updates

- Lack of knowledge on how to update
- Inconvenience
- Concerns about performance impacts
- The perception that updates are unimportant
- Insufficient device storage

KEEPER

Password Creation and Management

Strength is a key consideration for 44% of users when creating passwords. Other influential factors include having a personal system (32%) and ease of remembrance, which is paramount for nearly one-third of global users (31%). However, only 8% of respondents rely on browser-recommended passwords, and a mere 12% use password managers to generate their passwords.

Alarmingly, 41% of people admit to reusing passwords across multiple accounts, despite widespread advice against this dangerous practice.

Regarding password changing habits, 30% of people regularly update their passwords. Nearly the same proportion (29%) change passwords when mandated by websites, 28% do so when they forget them and 8% wait until after a data breach.

Password practices continue to be a critical weak point in cybersecurity. The prevalent reuse of passwords and reliance on memory or physical notes for password management exposes users to significant security risks. Although many individuals believe in the security and management of their passwords, their actual practices reveal a pressing need for better tools and education. Promoting the use of password managers, the creation of strong, unique passwords for every account, and the use of Multi-Factor Authentication (MFA) whenever it's available, could substantially mitigate these risks.

41%

Admit to reusing passwords across multiple accounts

Most Popular Password Mgmt Practices

26%

Relying on memory

24%

Writing them down

19%

Storing them in a browser or phone notes app

Password Sharing

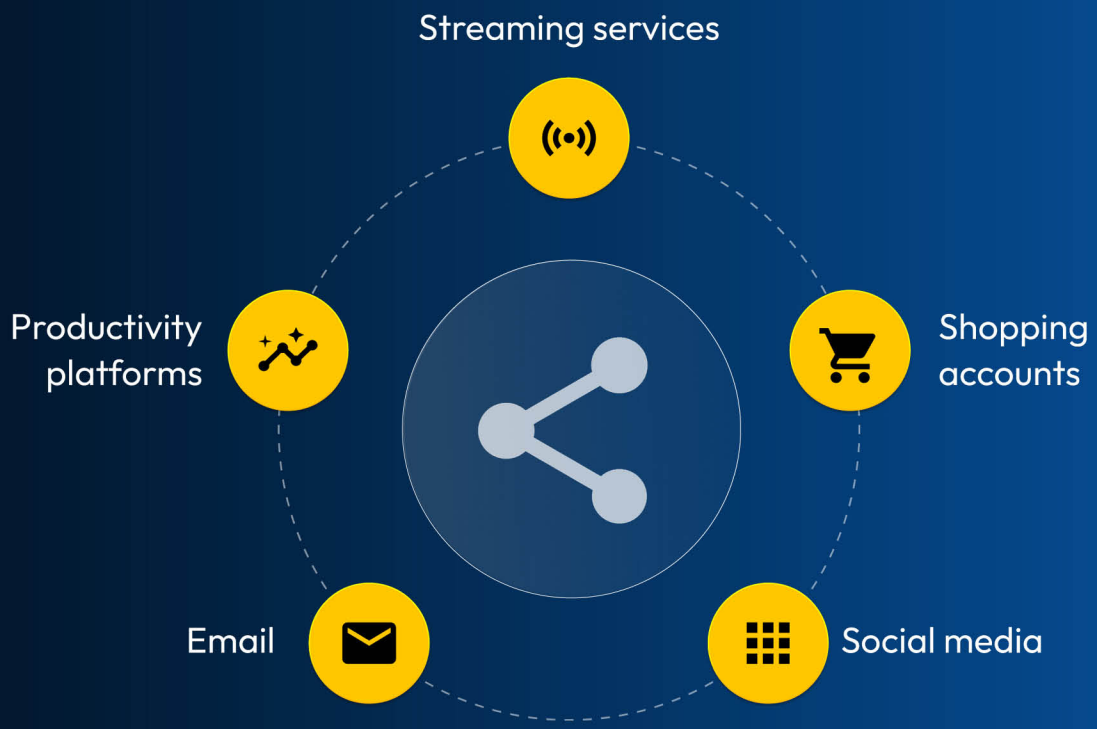
Global respondents provided feedback on password sharing, with over half (61%) admitting to having shared passwords using methods such as:

01 Verbally or over the phone

02 A text message or messaging app

03 Written down

Top 5 types of passwords people share



An astounding 15% of people admitted to sharing passwords for their bank accounts or credit cards.

The prevalence of password sharing, especially for streaming services, is particularly relevant in light of recent industry efforts to crack down on this practice. While sharing passwords is common, it poses substantial security risks when done insecurely, especially when the shared passwords are reused across multiple accounts. With only 7% of global respondents using a password manager to share passwords in a secure manner, there is a clear need for improvement and education on best practices for password sharing.

Cybersecurity Confidence

85%

Believe their passwords are secure

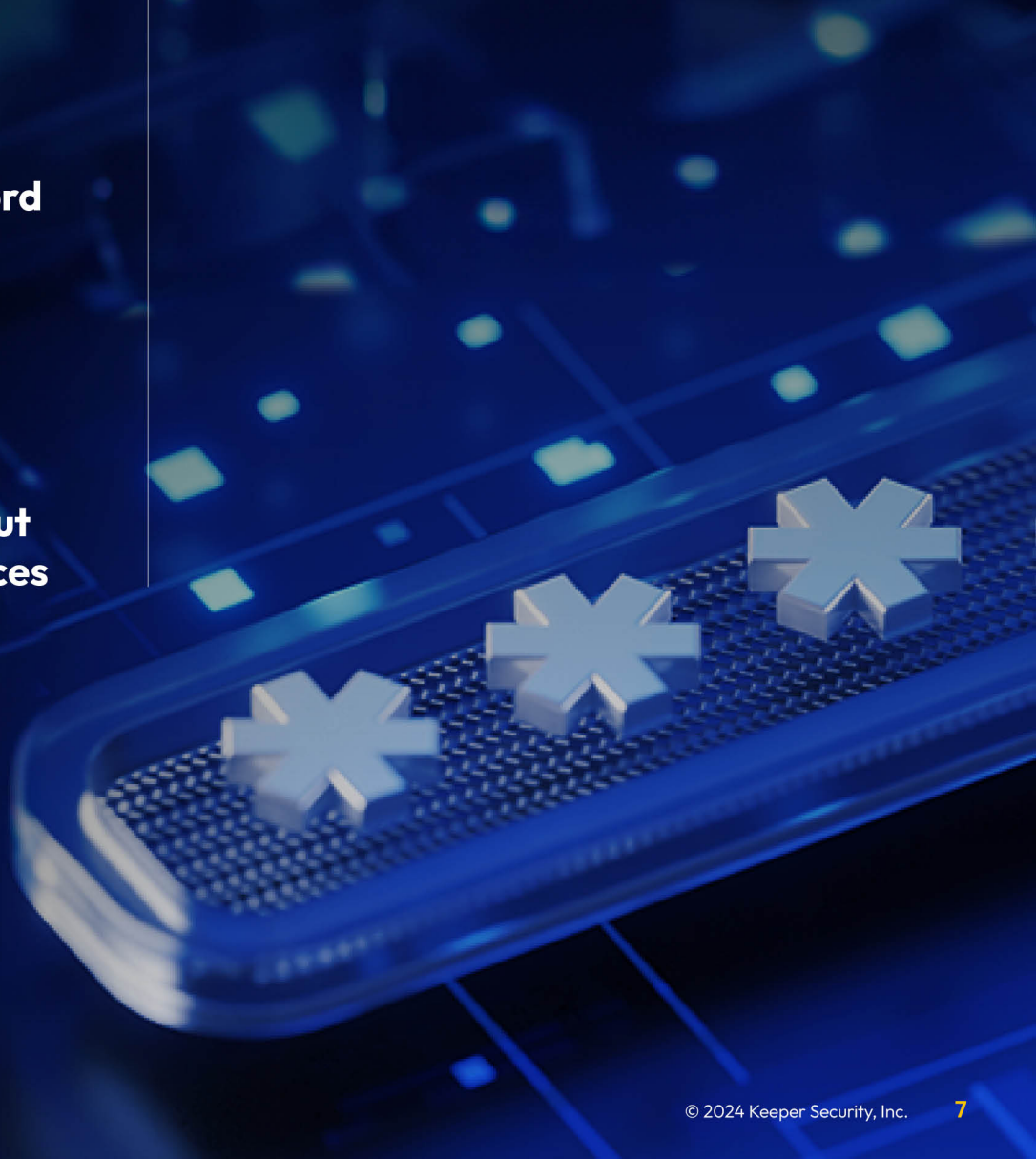
26%

Describe their password habits as cautious

13%

Are embarrassed about their password practices

Many individuals exhibit a striking overconfidence in their cybersecurity practices, particularly when it comes to password management. Despite diverse and often inconsistent approaches to cybersecurity, 85% of survey respondents believe their passwords are secure, and 83% feel they manage them well. Furthermore, a significant majority (64%) express confidence in their understanding of cybersecurity best practices. Additionally, 26% describe their password habits as cautious, while 13% worldwide admit to being careless or embarrassed about their password practices. Notably, 62% of users worry about managing the sheer volume of passwords, accounts and logins they have.



Conclusion

The data reveals a paradox in cybersecurity: while a substantial portion of the population feels confident in their cybersecurity knowledge and practices, people continue to fall victim to cyber attacks and scams. This discrepancy highlights that knowledge alone is insufficient to mitigate cyber risks; practical application and strict adherence to security best practices are equally essential.

The study underscores the urgent need to intensify efforts to educate the public about the risks associated with online scams, phishing and fake ads, especially targeting demographics more vulnerable due to the economic downturn. Equally important is simplifying adherence to security advice, such as developing and promoting more user-friendly methods for updating devices to overcome barriers like inconvenience and lack of knowledge.

Promoting the use of password managers is crucial to alleviating the prevalent concern about managing too many passwords and accounts. These tools facilitate the creation of strong, unique passwords for every account and facilitate the use of MFA, preventing the dangers of password reuse and providing secure password storage.

Moreover, users worldwide should also be equipped with clear guidelines on the risks of insecure password sharing and offered safer alternatives. Emphasizing the importance of password security is vital to enhancing overall cybersecurity resilience.

Keeper's **Fortifying Cyber Resilience: Insights Into Global Cybersecurity Practices** report underscores the challenges faced by security practitioners in guiding people to take appropriate actions at critical times, both online and in the workplace. While users exhibit a commendable level of confidence and awareness, it is crucial to consistently reinforce practical security behaviors. By addressing gaps in user behavior and advancing education and technological solutions, we can collectively bolster protection against the escalating threats of cyber attacks and online scams.

Methodology

This online survey of 6,000 respondents in Australia, New Zealand, Singapore, Indonesia, Japan, France, the UK, US and DACH was conducted by market research company OnePoll, in accordance with the Market Research Society's code of conduct. This survey was overseen and edited by the OnePoll research team. OnePoll are MRS Company Partners, corporate membership of ESOMAR, and Members of the British Polling Council.