

DIGITAL SAFETY

Digital safety is a branch of cybersecurity that focuses on individuals' comfort, convenience, and privacy online. It addresses the potential harms that can arise from the misuse of technology, including cyberbullying, cyberstalking, and identity theft (Matthew et al., 2021).



CAUSES OF DIGITAL SAFETY ISSUES

1 Human Error

Human error is a major cause of cybersecurity breaches. According to studies, human error is the main cause of 95% of cyber security breaches. A significant percentage of breaches, ranging from 74% to 95%, involve human error, emphasizing the need for better training and awareness (Usecure, 2023; Infosec Institute, 2023; Security Today, 2023).

2 Weak Passwords

Poor password management, including using easily guessable passwords and reusing passwords across multiple sites, makes systems vulnerable to attacks (Usecure, 2023; Haughn, 2023). The National Centre for Cyber Security's 2019 report found that 123456 remains the most popular password in the world, and 45% of people reuse the password of their main email account on other services

3 Software Vulnerabilities

Exploiting software vulnerabilities is a common method used by cybercriminals to gain access to data (SHRM, 2023; Security Today, 2023). Regular updates and patches are essential to mitigate these risks. Failure to update systems can leave them exposed to known vulnerabilities, as seen in high-profile breaches (Security Today, 2023; Haughn, 2023).

IMPACTS OF DIGITAL SAFETY BREACHES

1 Financial Losses

Breaches can result in high costs from legal fees, data recovery, and compensation. Companies may also face fines for not complying with data protection laws. For example, the Equifax breach cost over \$1 billion, and Meta was fined \$1.3 billion for GDPR violations (IMF, 2024; CSO Online, 2023). On average, a data breach costs \$4.45 million (Forbes, 2023).

2 Reputational Damage

Breaches can destroy customer trust and loyalty, leading to a loss of business. The negative impact on a company's image can last a long time, making it hard to recover (IMF, 2024; World Economic Forum, 2023).

3 Operational Disruptions

Cyberattacks can halt business operations. Ransomware attacks can lock up important data, forcing companies to pay for decryption. Such disruptions can affect supply chains and entire economies, as seen with a cyberattack on the Central Bank of Lesotho (IMF, 2024; UpGuard, 2023).

STRATEGIES FOR ENHANCING DIGITAL SAFETY

1 Education and Training

Implement consistent training on recognizing phishing attempts and handling sensitive data securely. Use practical exercises and real-life scenarios to improve learning. Conduct engaging awareness campaigns and simulations tailored to specific organizational risks. Keep staff updated on emerging threats through regular education and updates on cybersecurity trends (E-Learning Company, 2023)

2 Robust Password Policies

Enforce strong password policies and multi-factor authentication (MFA) to add an extra layer of protection. Encourage the use of password managers to create and securely store complex passwords. Require regular password changes to make unauthorized access more difficult (E-Learning Company, 2023)

3 Regular Software Updates

Regularly update and patch software to prevent exploitation of known vulnerabilities. Use automated update systems to ensure timely and consistent application of updates. Continuously monitor for vulnerabilities and address them promptly to maintain security (E-Learning Company, 2023)

References

Matthew, Tolulope Joshua Ashaolu, Abayomi Ajayi-Majebi and Musa, S.M. (2021). Digital Safety. [online] ResearchGate. Available at: https://www.researchgate.net/publication/354973536_Digital_Safety [Accessed 2 Aug. 2024].
Infosec Institute. (2023). Human error responsible for data breaches. Retrieved from <https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/>
Haughn. (2023). How does human error impact cyber attacks?. Retrieved from <https://www.haughn.com/how-does-human-error-impact-cyber-attacks/>
Security Today. (2023). Just why are so many cyber breaches due to human error?. Retrieved from <https://securitytoday.com/articles/2022/07/30/just-why-are-so-many-cyber-breaches-due-to-human-error.aspx>
SHRM. (2023). Human error cited as top cause of data breaches. Retrieved from <https://www.shrm.org/topics-tools/news/risk-management/human-error-cited-top-cause-data-breaches>
Usecure. (2023). The role of human error in successful cyber security breaches. Retrieved from <https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>
CSO Online. (2023). The biggest data breach fines, penalties, and settlements so far. Retrieved from <https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>
Forbes. (2023). Cybersecurity statistics. Retrieved from <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/>
IMF. (2024). Rising cyber threats pose serious concerns for financial stability. Retrieved from <https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability>
UpGuard. (2023). Biggest data breaches in financial services. Retrieved from <https://www.upguard.com/blog/biggest-data-breaches-financial-services>
World Economic Forum. (2023). How does your industry compare when it comes to the financial impact of cyber threats?. Retrieved from <https://www.weforum.org/agenda/2023/03/how-does-your-industry-compare-when-it-comes-to-the-financial-impact-of-cyber-threats/>
E-Learning Company. (2023). Strategies for implementing effective digital citizenship and online safety training. Retrieved from <https://elearning.company/blog/strategies-for-implementing-effective-digital-citizenship-and-online-safety-training/>
E-Learning Company. (2023). Strategies for effective digital citizenship and online safety curriculum. Retrieved from <https://elearning.company/blog/strategies-for-effective-digital-citizenship-and-online-safety-curriculum/>