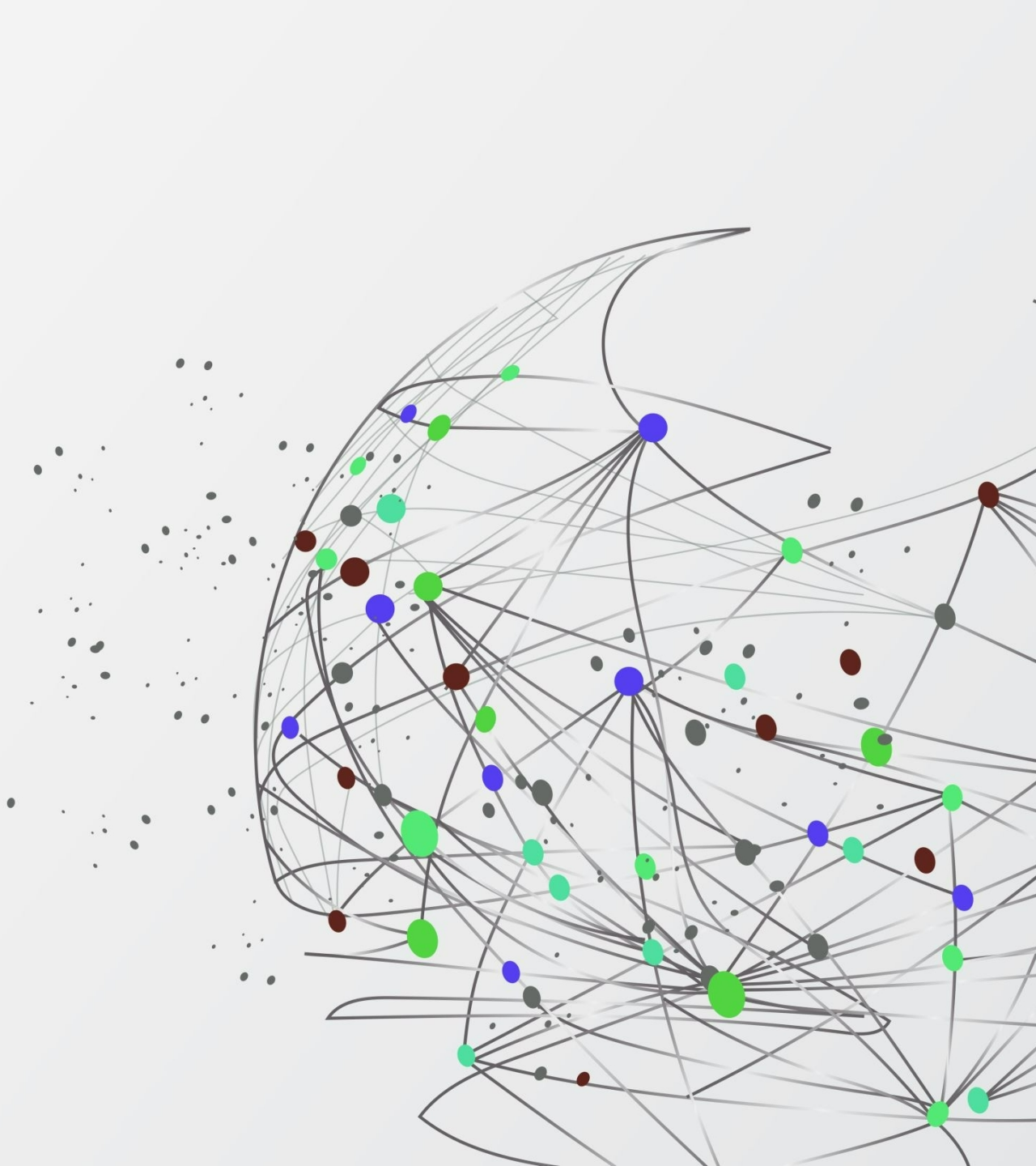
Cybersecurity Awareness in the Digital Age



By Bryce Baxter

CYSE 201S

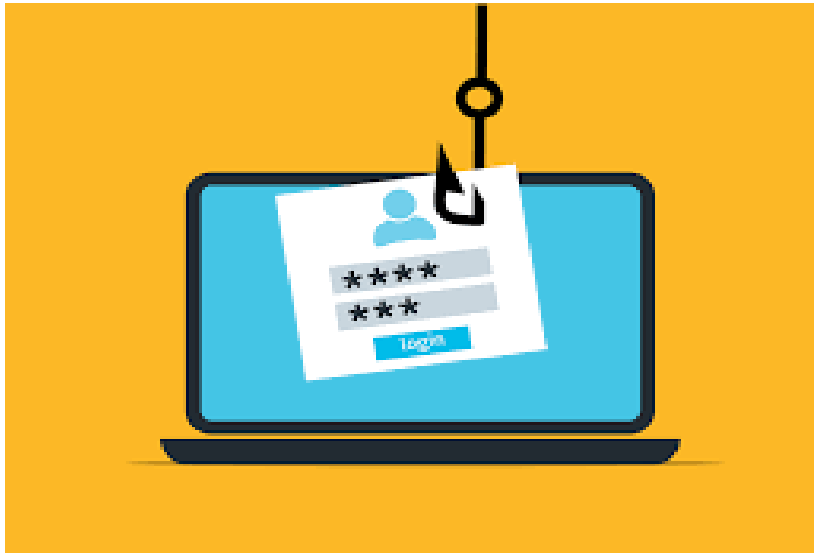
11/12/25

Why is Cybersecurity Awareness Important?

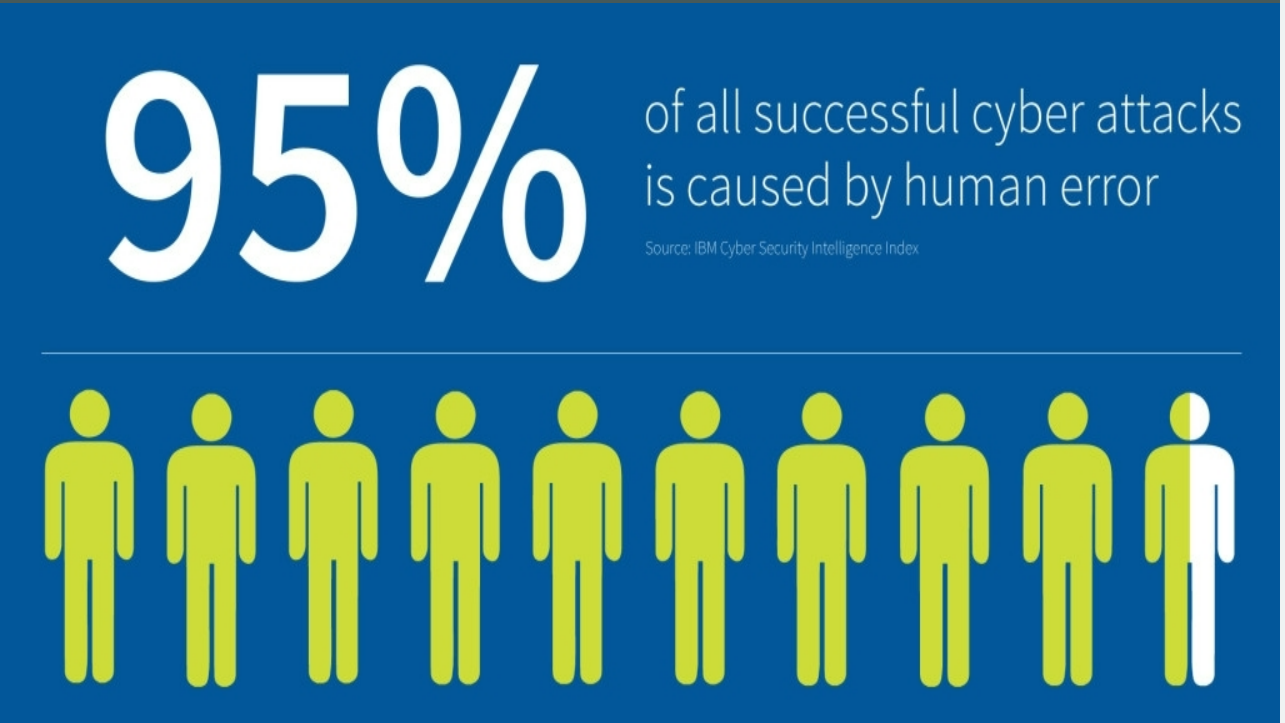
- Cybersecurity Awareness safeguards sensitive information, intellectual property, and personal data from theft, damage, or misuse.
- Since many breaches start with human error, trained employees can identify threats like phishing emails and social engineering attempts, acting as a human firewall.
- Protecting customer data and systems builds maintain customer confidence and a positive brand reputation.
- Many industries and governments require security awareness training to comply with regulations, such as GDPR (General Data Protection Regulation).

What are the most common causes of breaches?

- Phishing attacks are the most common type of data breach where the hacker tricks the victim into revealing personal and sensitive information through emails and text messages
- Weak and Stolen passwords are also incredibly common in terms of data breaches because people typically use the same password for multiple websites making it easy to access
- Malware and Ransomware is also common where suspicious software infiltrates system data to steal data, and encrypt files



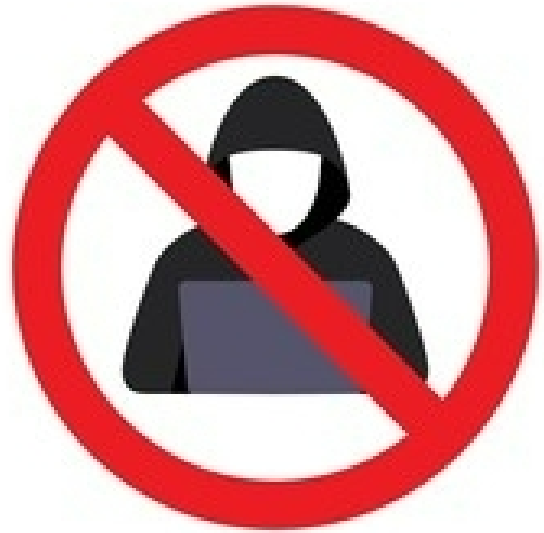
Human Error in Cybersecurity



- According to this article made in 2020, 95% of all data breaches are successful because of human error. Even with the large number of human errors, these errors are extremely easy to prevent.
- Phishing is the most common form of human error in cybersecurity but there are also factors such as social media, insecure Wi-Fi, and use of personal devices.
- Security Awareness training is so important and helpful for employees and the general public because it informs individuals on how to manage cyberattacks and data breaches.

How can these data breaches be prevented?

- Phishing attacks can be prevented by training employees to catch the signs of suspicious emails, text messages, and links.
- Weak passwords can be prevented by requiring more complex and unique password combinations as well as multi-factor authentication for all users.
- Malware and Ransomware can be prevented by regularly updating antivirus software backing up a system regularly.



Conclusion

- Cybersecurity Awareness is extremely important because all organizations and individuals should be aware of cyberattacks and how to prevent them from happening.
- Understanding the signs of cyberattacks is also just as important. Signs in a phishing email include misspellings in the text and a email that you might not recognize. Signs that a system may need to be updated are lagging and struggling to work with newer systems and the system warning you that the antivirus software is out of date.
- Strategies such as employee training, and multi-factor authentication are important to make sure that everybody is prepared for upcoming cyberattacks and how to prevent them from happening.

References

- Cyber Security Awareness - What Is It and Why Is It Important? www.dataguard.com/cyber-security/awareness.
- Adhikary, Raja. “Top 10 Most Common Causes of Data Breaches.” CloudEagle.ai, 3 Oct. 2025, www.cloudeagle.ai/blogs/causes-of-data-breaches.
- “Protecting Sensitive and Personal Information From Ransomware-Caused Data Breaches.” CISA | DEFEND TODAY, SECURE TOMORROW, 2021, www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf.