By Khamari Scott

CYSE201S

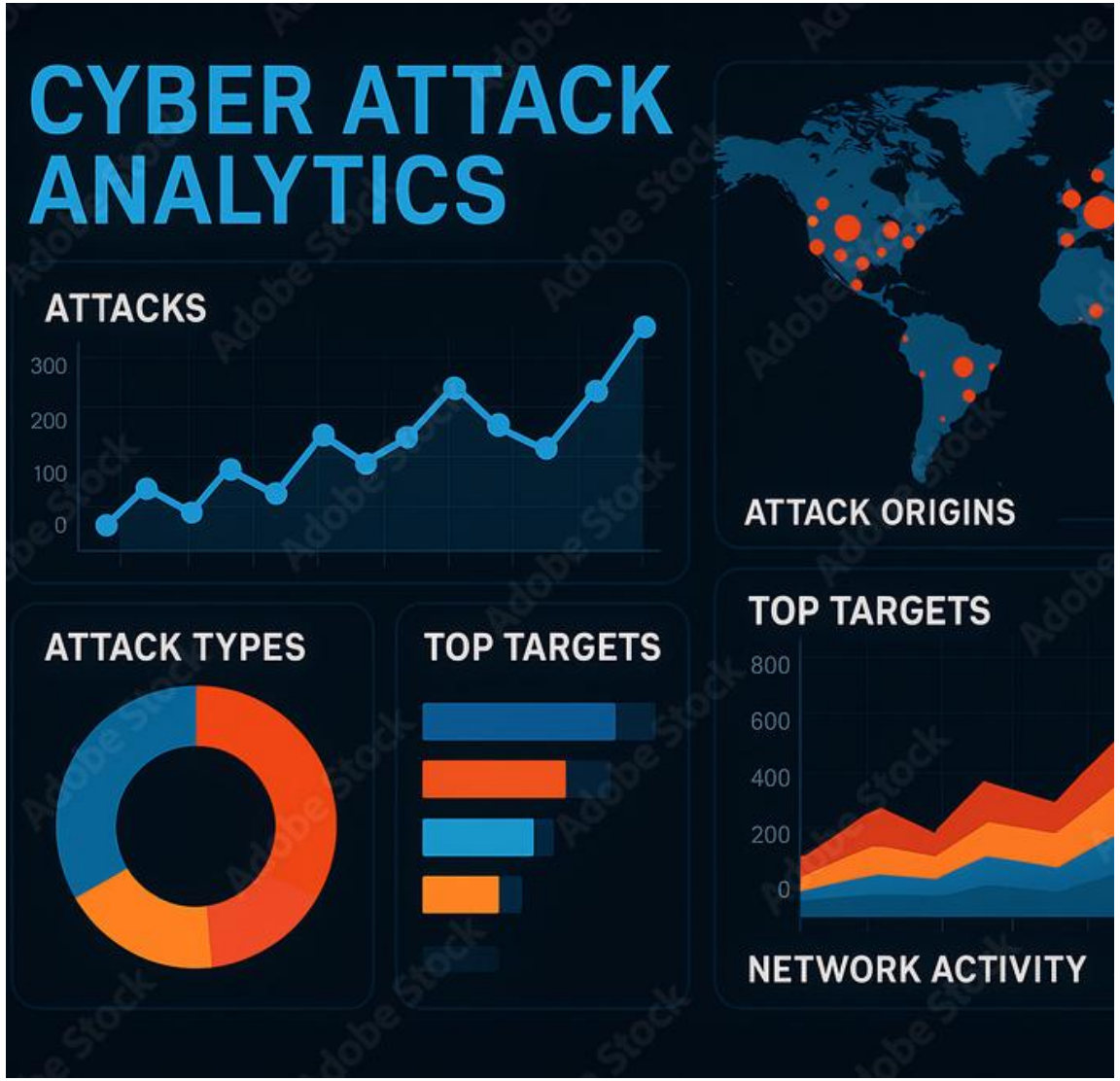
Cybersecurity Awareness and Society

What is cybersecurity awareness?

- Cybersecurity is defined as protecting both systems/networks/data from unauthorized access. Awareness refers to knowing about risks and behaviors that are considered secure while on-line.
- Most attacks against computer systems or networks are targeted toward humans rather than computers/technology.
- Social Science Connection:
  Psychology explains the reasoning behind a person falling victim to an attack.
  Sociology describes the social influences on a group's behavior.

Why it matters to society

- Data breaches can be very costly when they occur, with tens of thousands of individuals affected at times. Identity theft and potential financial losses are common problems associated with large-scale data breaches. The emotional impact may include feeling stressed, fearful, embarrassed etc. Large-scale data breaches negatively affect all types of business (healthcare/government) in addition to others.
- Weaknesses in awareness = greater risk of attacks for everyone.



Human Behavior and Cyber Threats

- Social Engineering is used through phishing, scams, etc., where they exploit trust, urgency and/or fear.
  Many times, when people are asked to create strong passwords for accounts they use frequently, they will often either use the same password across multiple platforms or completely disregard updating their existing passwords.
- Example:
- A romance scam uses manipulative tactics to play with the victims' emotions to get money from them.
- Social Science Insight:
- Cognitive Biases → We make fast decisions without thinking about all aspects.
  Social Pressure → We tend to follow the crowd.

Improving Digital Literacy

- Provide education on recognizing scams
  Create and use unique passwords
  Turn on Two-Factor Authentication (2FA)
  Keep your operating system and applications updated
- Problem:
  Individuals do not take time to learn from trainings; individuals find training confusing.
- Solutions:
  Provide users with easy-to-understand and enjoyable training.

Solutions(Tech + Social Science)

- The combination of technology with an understanding of how humans behave is one way to increase user-friendliness in security systems.
- Barrier:

People either do not follow through on their training or cannot understand the information that has been provided.

- Solution:

Training can be made simpler, more engaging, and relevant.

Why this matters(Reflection)

- The combination of technology with an understanding of how humans behave is one way to increase user-friendliness in security systems.
- Barrier:
  People either do not follow through on their training or cannot understand the information that has been provided.
- Solution:
  Training can be made simpler, more engaging, and relevant.

References

- Federal Trade Commission. (2023). *How to recognize and avoid phishing scams*. How To Recognize and Avoid Phishing Scams | Consumer Advice
- National Institute of Standards and Technology. (2023). *Cybersecurity framework (CSF) 2.0*. The NIST Cybersecurity Framework (CSF) 2.0
- Adobe. (n.d.). *How to increase your digital literacy*. How to improve digital literacy skills | Adobe Acrobat
- Bright Defense. (n.d.). *Recent data breaches: Biggest data breaches of all time*. List of Recent Data Breaches in 2026