

Table of contents

01

Title

02

Why Cybersecurity Awareness Matters

03

Social Science Connection

04

Common Cyber Risks

05

Why Awareness Is Low

06

Improving Cyber Awareness

07

Building Digital Literacy

08

Conclusion



Cybersecurity Awareness In The Digital Age

Jimmy Hernandez

CYSE 201S - Cybersecurity and the Social Sciences

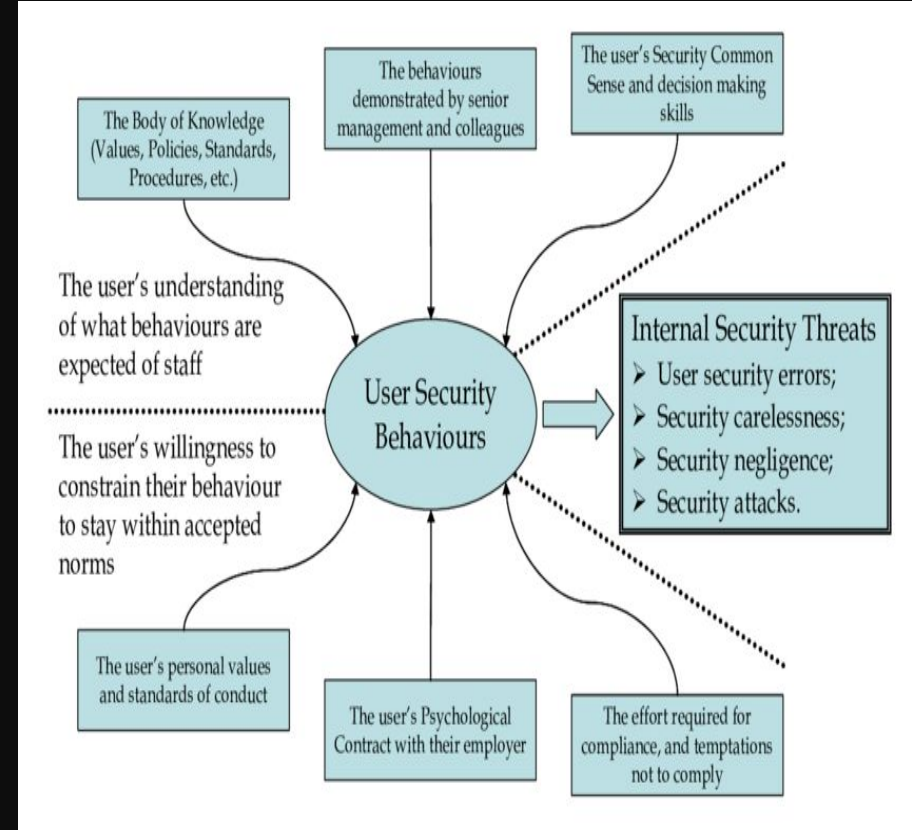
Why Cybersecurity Awareness Matters

- Growing number of cyber threats targeting everyday users
- Human behavior is the weakest link
- Social engineering exploits trust, emotions, and habits



Social Science Connection

- Online behavior shaped by culture, habits, and social norms
- Risk perception influences online safety decisions
- Digital inequalities make some people more vulnerable



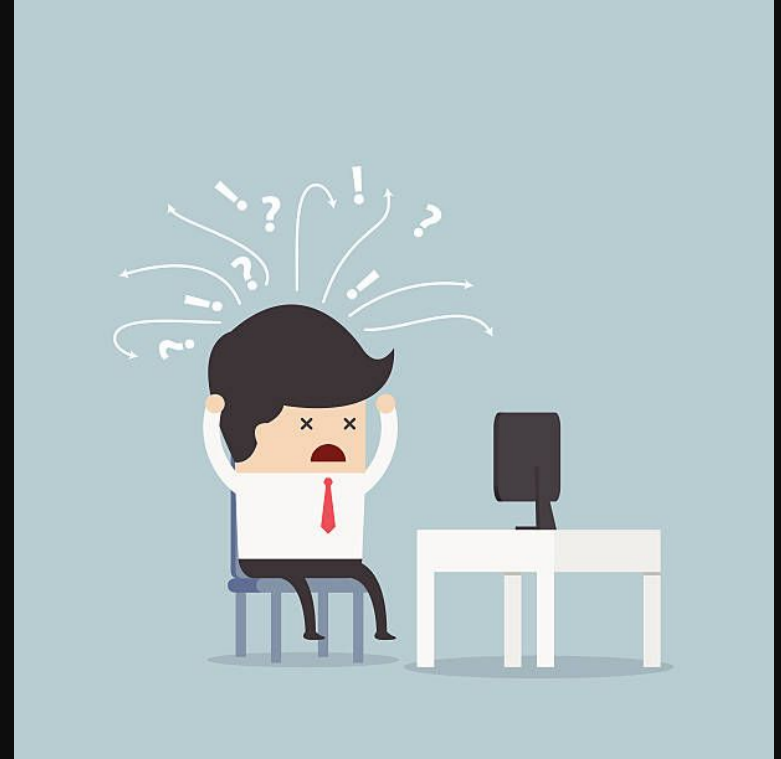
Common Cyber Risks

- Phishing & scams
- Weak passwords
- Oversharing on social media
- Malware from unsafe links
- Public Wi-Fi risks



Why Awareness Is Low

- Lack of digital literacy
- “It won’t happen to me” mindset
- Rapidly changing technology
- Misunderstanding of privacy risks



Improving Cyber Awareness

- Teach basic digital hygiene: strong passwords, updates, MFA
- Use real-life examples of attacks
- Community workshops & school programs
- Normalize secure habits



Building Digital Literacy

- Think critically about online information
- Recognize social engineering tactics
- Learn privacy settings
- Know how to report suspicious activity



Conclusion

- Cybersecurity is a social, not just technical, issue
- Awareness empowers safer online behavior
- Digital literacy reduces cyber risks for society



References

- CISA. (2023). Cybersecurity awareness resources. Cybersecurity & Infrastructure Security Agency. <https://www.cisa.gov/cybersecurity-awareness>
- Hadnagy, C. (2021). Social engineering: The science of human hacking (3rd ed.). Wiley.
- NIST. (2022). Cybersecurity and digital literacy guidelines. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>