# Cybersecurity Awareness in the Digital Age

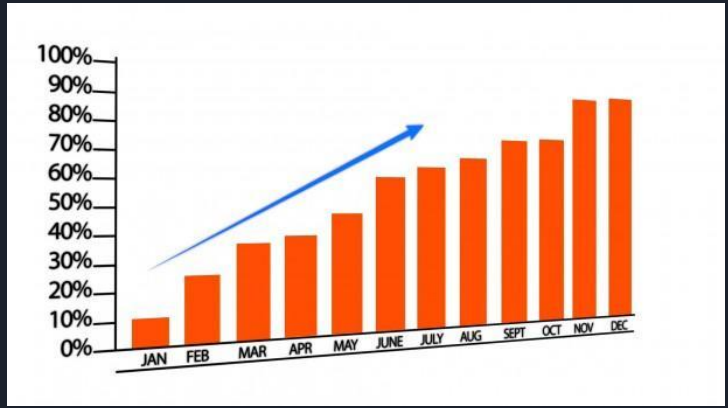
By Justin White

CYSE 201S

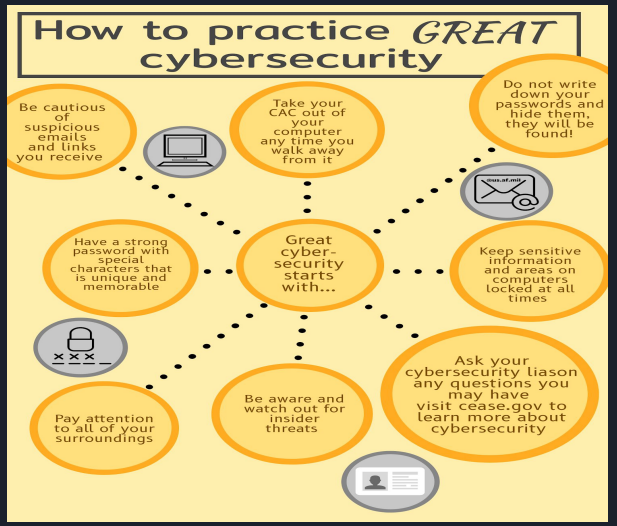
April 16th, 2025

# Why Cybersecurity Awareness Matters

- **Human Error causing breaches:** The vast majority of data breaches are the result of human error. According to studies, human errors account for between 88% to 95% of data breaches.
- **Psychological Stressors leading to mistakes:** According to research, stress, exhaustion, and distractions might increase the likelihood of clicking on unsafe links, forgetting passwords, or ignoring warnings.
- **Why It Matters:** In the digital world, mistakes can lead to severe repercussions such as stolen data, financial losses, and reputational damage.

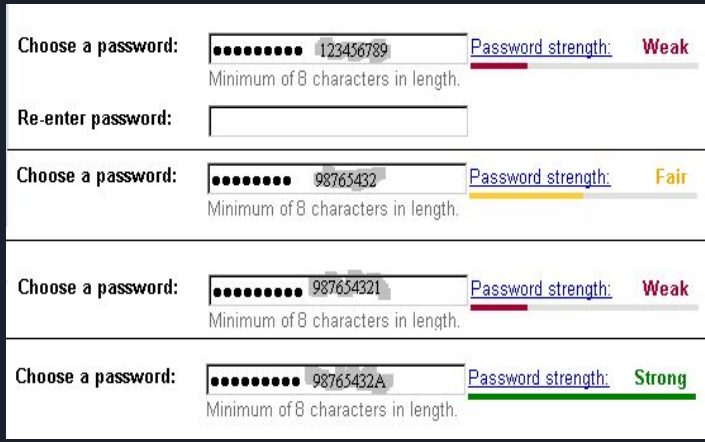
# How Social Science Helps Us Build Cyber Awareness




- Social Sciences helps us understand why and what causes people to ignore cyber security advices
- Helps design programs that show the power of good habits and routines for defending against attacks
- Gives knowledge on why and how individuals commit attacks and ways to identify them

# Common Threats due to Lack of Awareness

1. Phishing
2. Oversharing on Social Media
3. Weak passwords (Ex. 12345)
4. DDoS
5. Malware
6. Virus
7. Scams

# Ways to improve Awareness

- Provide straightforward and entertaining training that discusses major cyber dangers such as phishing, malware, and scams, using real-life examples to make it stick.
- Teach users to notice warning indicators, such as dubious links, urgent messages, or unusual login requests.
- Encourage the usage of strong passwords and password managers to prevent easy-to-guess logins.
- Encourage multi-factor authentication (MFA) or two-factor authentication (2FA) as an additional layer of safety.
- Use simulations and hands-on activities to reinforce healthy behaviors (for example, mock phishing emails or gamified learning).

# Example

Ex.1) "A company lost more than $40,000 after an employee received a forged email that appeared to be from their CEO. It requested them to wire money immediately. They sent the money because the email appeared to be legitimate and the employee failed to verify it.

**What went wrong:** No knowledge of phishing tactics, Trust in authority is used against them, No two-factor authentication or confirmation method is in place.

**Solutions:** Train employees to identify phony emails, Always verify urgent requests over the phone or in person, Use a two-step approval for money transactions.

# Takeaway

Cybersecurity is more than simply technology; it's about people. We make mistakes. But if we understand why we do it and teach it in an understandable way, we can make the digital world a safer place for everyone.

# Work Cited


Medlock, B. (2025, March 18). 2025-02-19-10 common cybersecurity threats and attacks: 2025 update. *ConnectWise*. https://www.connectwise.com/blog/cybersecurity/common-threats-and-attacks

Russo, A., Vojković, L., Bojic, F., & Mulić, R. (2022). The conditional probability for human error caused by fatigue, stress and anxiety in seafaring. *Journal of Marine Science and Engineering*, *10*(11), 1576. https://doi.org/10.3390/jmse10111576

Vojkovic, L. (2022, October 25). *The conditional probability for human error caused by fatigue, stress and anxiety in seafaring*. https://www.academia.edu/109348556/The_Conditional_Probability_for_Human_Error_Caused_by_Fatigue_Stress_and_Anxiety_in_Seafaring