Cyber Secure

Module 4

Cybersecurity Awareness

Author: George Nicholl

Student ID: 50095130

Cybersecurity awareness is a critical component in protecting both individuals and organisations from the increasing number of digital threats. While advanced technology and security tools play an important role, many cyberattacks succeed not because of technical weaknesses, but due to user error. Raising awareness about security threats and best practices empowers people to become a strong line of defence, rather than a point of vulnerability.

This document expands on the training video by offering detailed statistics, examples and best practices for improving cybersecurity awareness.

What is Cybersecurity Awareness

Cybersecurity awareness is the understanding of potential cyber threats and the behaviours necessary to avoid them. It involves recognising phishing attempts, using strong passwords, reporting suspicious activity, and following basic security protocols.

- IBM's 2023 Cost of a Data breach report revealed that 74% of data breaches involve a human element, including phishing, stolen credentials, and misconfigurations caused by users.
- Verizon's 2023 Data Breach Investigations Report identified phishing as the cause of 36% of breaches, making it the most common form of social engineering.
- According to Stanford University (2024), 88% of cyber incidents are caused by human mistakes, ranging from clicking on malicious links to mishandling sensitive data.

These statistics underscore the need for strong, consistent cybersecurity awareness initiatives.

When users are empowered with the knowledge to act responsibly, they become one of the strongest lines of defence against cybercrime.

Common Threats or Mistakes

A. Falling for Phishing or Social Engineering

- Clicking malicious links or sharing sensitive information
- Being tricked by urgent or emotional messages that bypass logic

B. Weak or Reused Passwords

- Using simple passwords or repeating them across accounts
- Enabling attackers to compromise multiple systems quickly

C. Ignoring Security Policies or Warnings

- Disabling updates, skipping MFA or dismissing alerts
- Leaving systems vulnerable to preventable exploits

D. Mishandling Sensitive Information

- Sharing credentials, sending data to the wrong recipient or storing files insecurely

Together, these habits create major entry points for cybercriminals, especially in organisations without consistent training.

Real-World Impact of Human Behaviour

- IBM (2023) – 74% of data breaches involved a human element.
- Verizon (2023) – Phishing Accounted for 36% of breaches.
- Stanford (2024) – 88% of incidents are caused by human mistakes.
- LastPass (2023) – 44% of employees admit to sharing passwords with colleagues.
- NordPass (2024) – 64% of users reuse passwords.

These statistics show that even well-secured systems can fail without strong user awareness behaviour.

Why Awareness Programs are Essential

Cybersecurity awareness is not just about recognizing threats, it's about building a culture where secure behaviour is second nature.

- Purplesec (2024) reported that 98% of cyberattacks rely on social engineering - a tactic that manipulates human trust and behaviour to gain unauthorised access.
- NordPass (2024) found that 64% of users reuse passwords across multiple accounts, making them vulnerable to credential stuffing attacks.
- A study by LastPass (2023) showed that 44% of employees have shared passwords with colleagues, which increases the risk of unauthorised access and insider threats.
- Organisations that implement formal cybersecurity awareness training report 45% fewer security incidents than those without structured programs (IBM, 2023).

Components of an Effective Awareness Program

A. Ongoing Training & Education

- Regular sessions covering phishing, password safety, and data handling
- Reinforced through newsletters, posters and reminders

B. Phishing Simulations

- Safe tests that help employees identify suspicious emails
- KnowBe4 reports up to 74% improvement in awareness through simulations

C. Clear Polices & Easy Reporting

- Users should know what's expected and how to report issues quickly
- Encouraging reporting without blame increases visibility into threats

D. Gamification & Engagement

✔ Quizzes, competitions, and recognition to drive participation

E. Leadership Support

✔ Managers modelling good behaviour promotes a security-first culture

Key Takeaway

Cybersecurity awareness is not a box to be ticked once a year. It is a continuous investment in people. Even the most secure systems can be undone by one careless click. Organisations that actively foster a culture of awareness benefit from fewer breaches, faster response times and a more resilient workforce. By educating users about potential threats and encouraging proactive security behaviour, organisations can drastically reduce human-related vulnerabilities. When people understand their role in cybersecurity, they become part of the solution - not part of the problem.

Why This Matters for You

Everyone has a role to play in cybersecurity. Whether you're in IT or another department, your everyday actions affect the safety of everyone in your organisation. Awareness helps prevent mistakes before they happen and ensures you know what to do when something feels wrong.

Quick Recap: Cybersecurity Awareness Best Practices

DO:

- ✔ Think before you click – verify links and services
- ✔ Use unique, strong passwords and enable MFA
- ✔ Report anything suspicious to your IT or security teams
- ✔ Follow company security policies and guidelines

DON'T

- X Don't reuse passwords or disable updates
- X Don't ignore alerts or keep security to "just IT"
- X Don't share passwords or sensitive data over insecure channels

References

IBM (2023) *Cost of a Data Breach Report 2023*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 2 April 2025).

Verizon (2023) *2023 Data Breach Investigations Report*. Available at: https://www.verizon.com/about/news/2023-data-breach-investigations-report (Accessed: 2 April 2025).

Hancock, J. and Tessian (2020) *Psychology of Human Error*. CISO Mag. Available at: https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/ (Accessed: 2 April 2025).

Purplesec (2024) *2024 Cybersecurity Statistics: The Ultimate List Of Stats, Data & Trends*. Available at: https://purplesec.us/resources/cybersecurity-statistics/ (Accessed: 2 April 2025).

NordPass (2024) *How many passwords does the average person have?*. Available at: https://nordpass.com/blog/how-many-passwords-does-average-person-have/ (Accessed: 2 April 2025).

LastPass (2023) *Password Sharing*. Available at: https://www.lastpass.com/features/password-sharing (Accessed: 2 April 2025).

KnowBe4 (2024) *New KnowBe4 Statistics Reveal Security Awareness Training Reduces Phishing Susceptibility by 75%*. Available at: https://www.knowbe4.com/press/security-awareness-training-reduces-phishing-susceptibility-by-75 (Accessed: 2 April 2025).

SANS Institute (2024) *2024 Security Awareness Report*. Available at: https://www.sans.org/security-awareness-training/resources/reports/sar/ (Accessed: 2 April 2025).

IBM (2023) *Cost of a Data Breach Report 2023*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 2 April 2025).

SANS Institute (2024) *2024 Security Awareness Report*. Available at: https://www.sans.org/security-awareness-training/resources/reports/sar/ (Accessed: 2 April 2025).