Cyber Secure

Module 8

Good Habits for staying Cyber Secure

Author: George Nicholl

Student ID: 50095130

Cybersecurity isn't just the responsibility of IT Departments, it's a shared duty that begins with individual behaviour. Developing good cyber hygiene is key to preventing breaches, reducing human error and creating a culture of security. This module builds on the final training video by outlining 10 essential habits that help individuals and organisations stay secure.

What are Good Cybersecurity Habits?

Good habits in cybersecurity are consistent behaviours that reduce risk and make it harder for attackers to succeed. Form using strong passwords to reporting suspicious activity, these everyday practices form the human firewall that comliments technical defences.

Building these habits create a "security-first" mindset, where security becomes second nature and not an afterthought.

10 Essential Habits for Staying Cyber Secure

1. **Use Strong Unique Passwords**

- Avoid common passwords or reusing across accounts
- Use long passphrases (e.g. "Summer@River_2025!").
- Consider using a **password manager** to generate and store credentials securely.

NordPass (2024) reports that 64% of users still reuse passwords, increasing the risk of breach

2. **Enable Multi-Factor Authentication (MFA)**

- Adds a second layer of protection beyond passwords
- Especially important for email, banking and cloud services

Mircrosoft (2023) states MFA can block 99.9% of account takeovers

3. **Think Before You Click**

- Be cautious of unsolicited emails or messages
- Hover over links and verify sender identities
- Report suspicious content instead of ignoring it

Verizon (2023) states that phishing accounts for 36% of breaches.

4. **Keep Software Up to Date**
- Install updates for systems, apps and browsers promptly
- Enable auto-updates to avoid delays

Unpatched vulnerabilities caused 60% of cyber compromises In 2024 (BankInfoSecurity).

5. **Lock Devices and Use Encryption**
- Lock screens when leaving devices unattended
- Use encrypted messaging and VPN's, especially on public Wi-Fi

6. **Avoid Public Wi-Fi for Sensitive Talks**
- Public networks are vulnerable to interception
- Always use a VPN when accessing sensitive data

7. **Back Up Important Data**
- Use automated cloud or offline backups
- Protects against ransomware, accidental deletion or hardware failure

8. **Be Cautious with Personal Devices (BYOD)**
- Ensure personal devices meet security standards
- Don't mix work and personal activity on the same device

9. **Stay Informed About Current Threats**
- Complete regular security training
- Follow trusted sources for updates and best practices

Trained employees are 60% less likely to be compromised (SANS Institute, 2024)

10. **Report Incidents Promptly**
- Even small mistakes like clicking a bad link should be reported
- Quick reporting enables faster containment and reduces damage

Key Takeaway

Cybersecurit habits aren't just about prevention, they are about empowerment. By mistaking secure behaviour part of your daily routine, you help to build a stronger defence for yourself, your team and your organisation

Why This Matters for You

You don’t need to be in IT to make a difference In cybersecurity. Every email you ignore, update you apply or incident that you report, contributes to the safety of your workplace.

Good habits create good defences.

Quick Recap: Cybersecurity Habits Checklist

- ✔ Use strong, unique passwords and a password manager
- ✔ Enable MFA across all accounts
- ✔ Update software and apps promptly
- ✔ Be cautious of suspicious emails and links
- ✔ Back up your data regularly
- ✔ Lock devices and use encrypted connections
- ✔ Avoid public Wi-Fi for secure tasks
- ✔ Keep personal devices secure if used for work
- ✔ Stay educated on evolving threats
- ✔ Report mistakes or incidents immediately

References

Microsoft (2023) *Why MFA Matters*. Available at : https://www.microsoft.com/security

NordPass (2024) *Password Reuse Report*. Available at: https://nordpass.com/blog/stop-reusing-passwords/

Verizon (2023) *Data Breach Investigation Report*. Available at: https://www.verizon.com/business/resources/Te46/reports/2023-dbir-public-sector-snapshot.pdf

BankInfoSecurity (2024) *Impact of Unpatched Vulnerabilities*. Available at: https://www.bankinfosecurity.com/

SANS Institute (2024) *Security Awareness Training Report*. Available at: https://www.sans.org/security-awareness-training