Co-funded by the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL

CHAPTER VII

Security Best Practices and Policies

Contents

- ✓ **Security Awareness Training and Education**
  - Key Components of Security Awareness Program
  - Measuring Training Effectiveness
  - Demonstrating the impact of security Education
- ✓ **Password Management and Authentication Mechanisms**
  - Best Practices for creating strong password
  - Password Storage and Protection
  - Password Policies and Management Tools
  - Future Trends in Authentication
- ✓ **Security Policies and Procedure for organization**
  - Developing Security Policies
  - Creating Effective Security Procedures, monitoring and Compliance
  - Best Practices

Co-funded by the European Union

Introduction

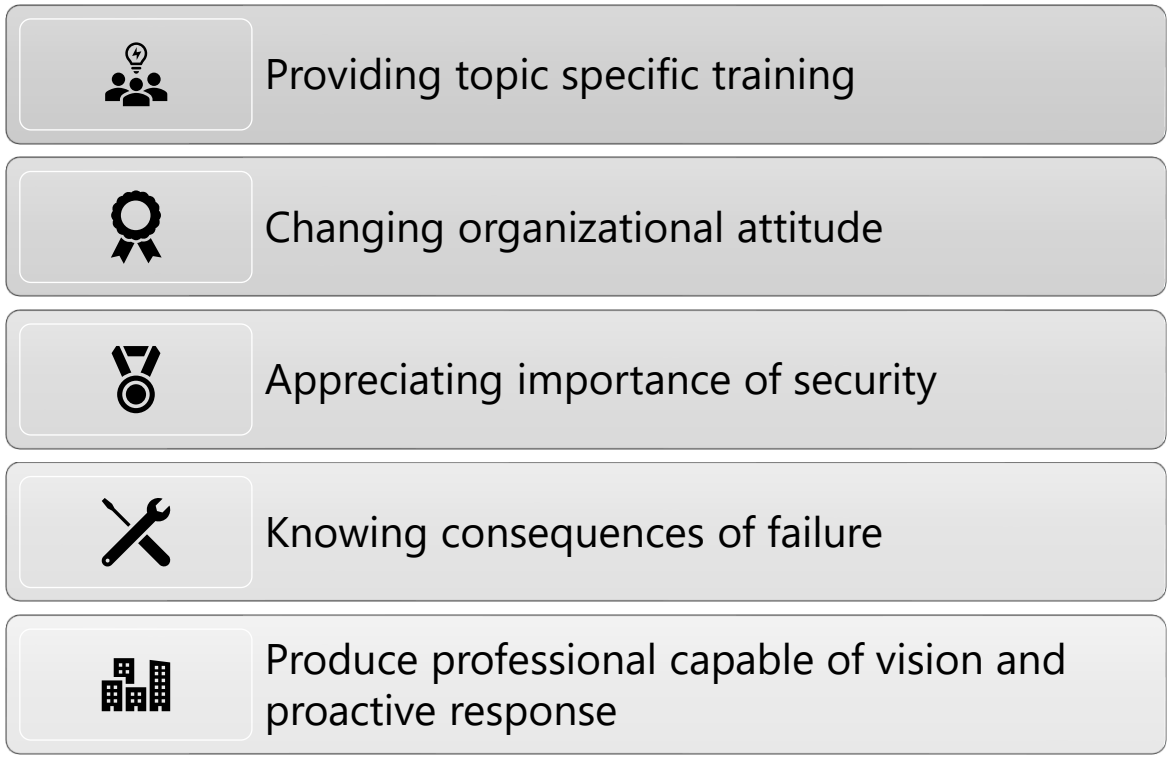
Co-funded by the European Union

Security Awareness Training and Education

- Security awareness training emphasises information security, and especially cybersecurity.
- The training encompasses a broad range of topics essential for maintaining cybersecurity hygiene, including but not limited to recognising phishing attempts, understanding the importance of strong password practices, identifying malware, and adhering to company security policies and procedures

Security Awareness Training and Education

- Key Components of Security Awareness Program
- Measuring Training Effectiveness
- Demonstrating the Impact of Security Education



Security awareness program

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Key Components of Security Awareness Program

- Employee Training
- Policy Development
- Phishing and Social Engineering
- Technical Measures
- Incident Response

Co-funded by the European Union

✓ Employee Training

- Employee training is the foundation of any cyber security awareness program.
- It is important to educate employees on the risks they face, how to identify potential threats, and the steps they need to take to protect themselves and the organization.
- Training should be ongoing, and should include regular updates on the latest threats and best practices.

Co-funded by the European Union

✓ Policy Development

- Developing and enforcing policies and procedures is another key component of a cyber security awareness program.
- These policies should cover all aspects of cybersecurity, including access control, incident response, and data protection
- They should be regularly reviewed and updated to keep up with the latest threats and industry best practices.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

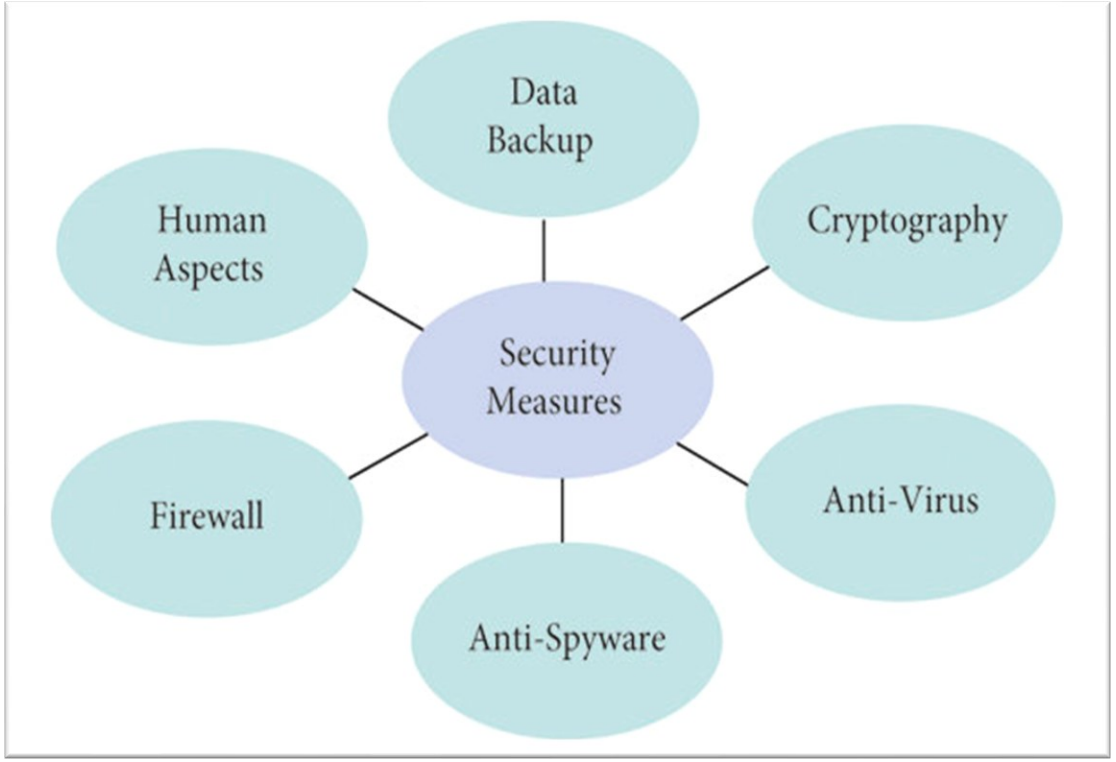
✓ Phishing and Social Engineering

- Phishing and social engineering are two of the most common ways that hackers gain access to sensitive information.
- It is important to educate employees on how to identify and avoid these types of attacks, and to provide them with the tools they need to report suspicious activity

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

✓ Technical Measures

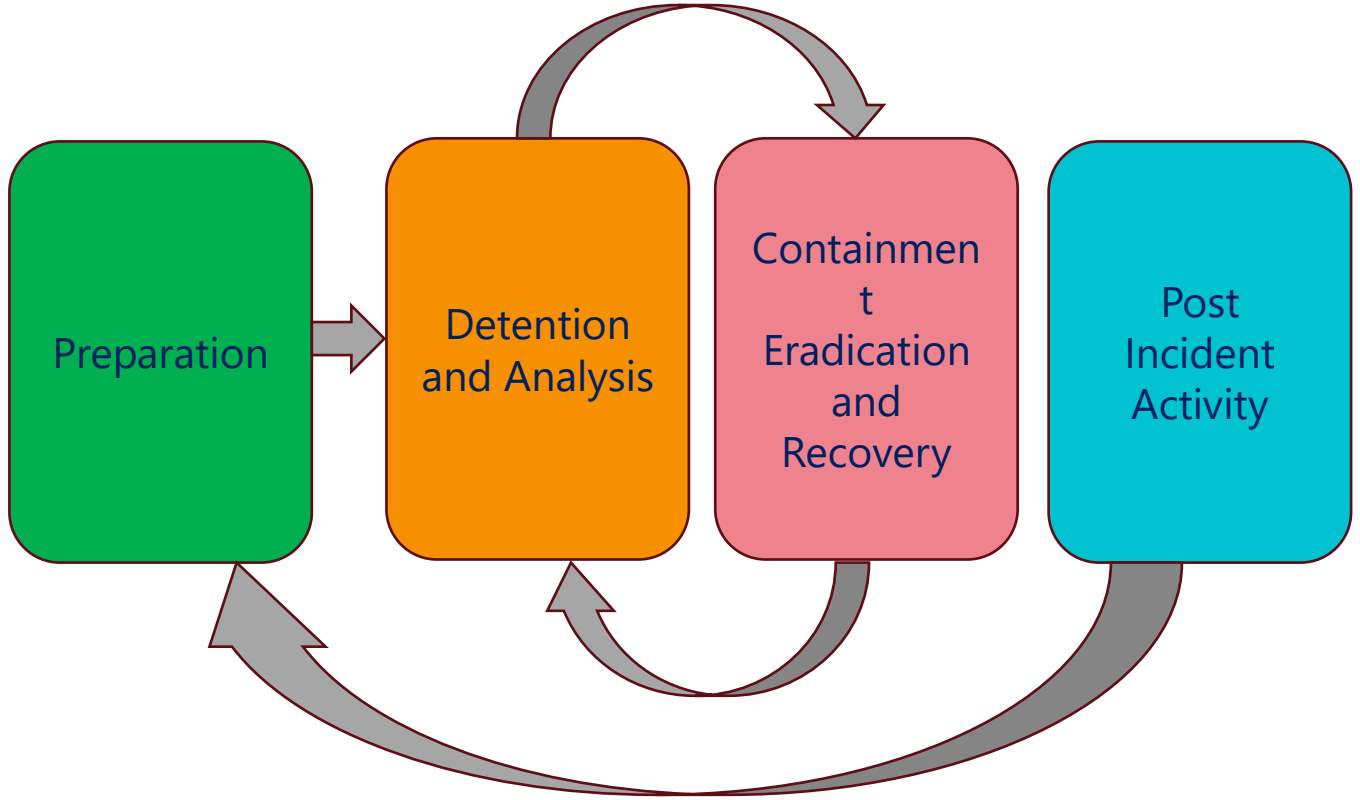
- Technical measures such as firewalls, intrusion detection and prevention systems, and encryption are essential for protecting your organization's systems and data.
- It is important to ensure that these measures are properly configured and regularly updated to keep up with the latest threats.



Co-funded by the European Union

✓ Incident Response

- Having a plan in place for responding to a cyber-attack is critical.
- This plan should include clear roles and responsibilities, a process for reporting incidents for containing and mitigating the impact of an attack.
- It is important to regularly test and update the incident response plan to ensure that it is effective in the event of a real attack.



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Measuring Training Effectiveness

01 Identify skills gaps

02 Test your employees

03 Up your reporting game

04 Check your culture

Co-funded by
the European Union

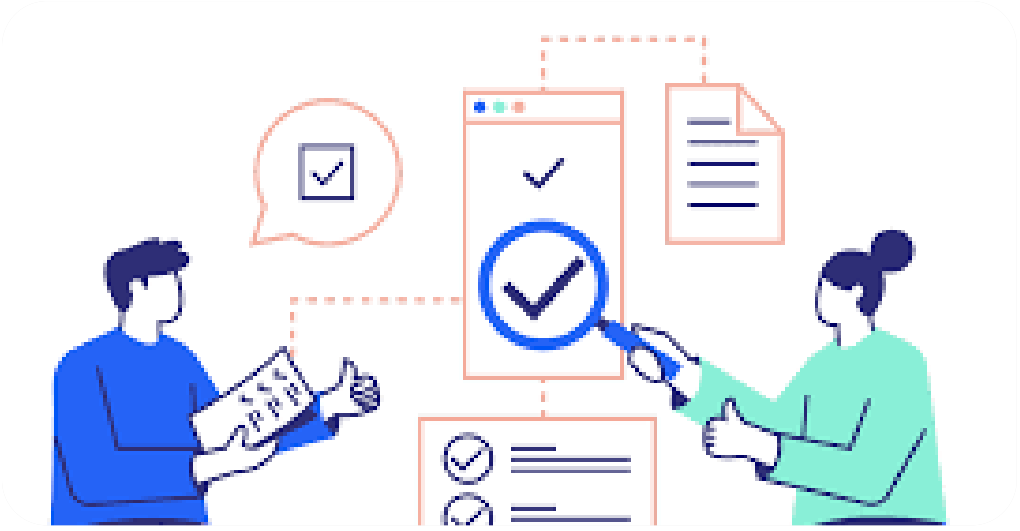
Identify skills gaps

- Skills gaps are deficiencies in performance caused by lack of skills for, or knowledge about, the workplace(for instance, keeping business information secure).

Co-funded by
the European Union

Test your employees

- Test your employees by integrating tools like phishing simulators in to a Learning Management System (such as the one your eLearning is hosted on)



Co-funded by
the European Union

Up your reporting game

- Build a real picture about the effectiveness of your chosen training solution and, when used alongside an intelligent learning platform, can be used to create targeted learning journeys designed to fill any gaps in knowledge and increase the training's potency.

Co-funded by the European Union

Check your culture

- Admittedly, measuring a compliance culture seems rather difficult, but that's not to say it's impossible! Businesses might use anonymous surveys.

Co-funded by
the European Union

Demonstrating the Impact of Security Education

01 ▪ Recognizing Cyber Threats

02 ▪ Empowering Employees

03 ▪ Reporting Security Incidents

04 ▪ Cost Savings

05 ▪ Preventing Security Breaches

06 ▪ Improved Incident Response

07 ▪ Customer Trust and Retainment

08 ▪ Compliance Adherence

09 ▪ Advantage Over Competitors

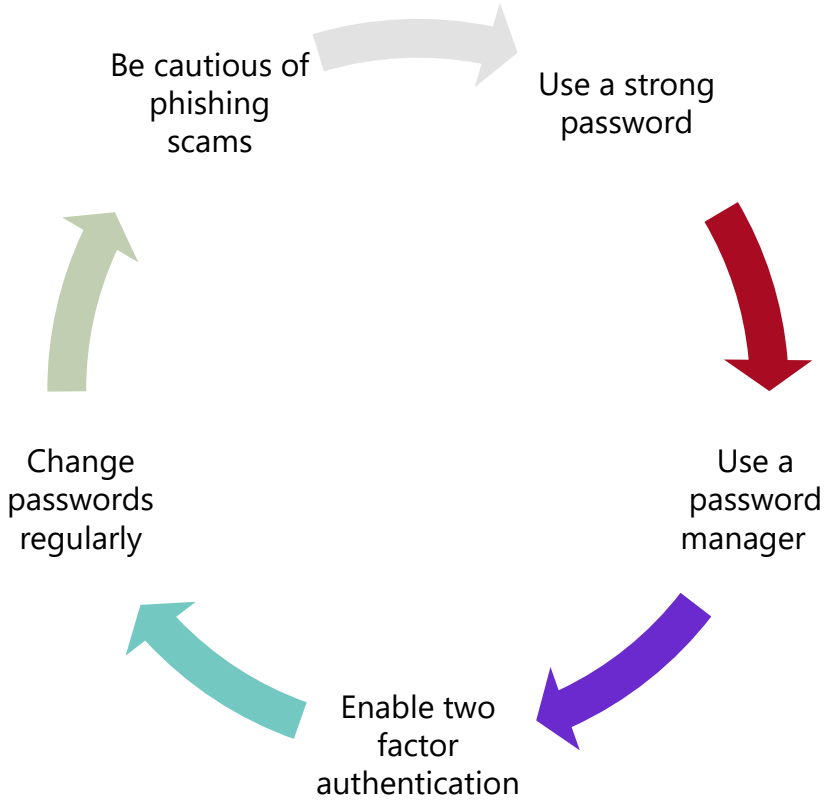
10 ▪ Adaptation to Emerging Threats

Co-funded by the European Union

❖ Password Management and Authentication Mechanisms

Key Points

- Best Practices for Creating Strong Passwords
- Passwords Storage and Protection
- Passwords Policies and Management Tools
- Future Trends in Authentication



Best practices for password management

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

❖ Best Practices for Creating Strong Passwords

- Create A Strong, Long Passphrase
- Add Advanced Authentication Methods
- Apply Password Encryption
- Test Your Password
- Implement Two-Factor Authentication
- Don’t Use Dictionary Words

Co-funded by
the European Union

❖ Best Practices for Creating Strong Passwords

- Use Different Passwords for Every Account
- Change Passwords When an Employee Leaves Your Business
- Secure Your Mobile Phone
- Protect Accounts of Privileged Users
- Avoid Periodic Changes of Personal Passwords
- Keep Your Business Offline

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

❖ Best Practices for Creating Strong Passwor

- Avoid Storing Passwords
- Be Vigilant About Safety
- Use Password Managers

Co-funded by
the European Union

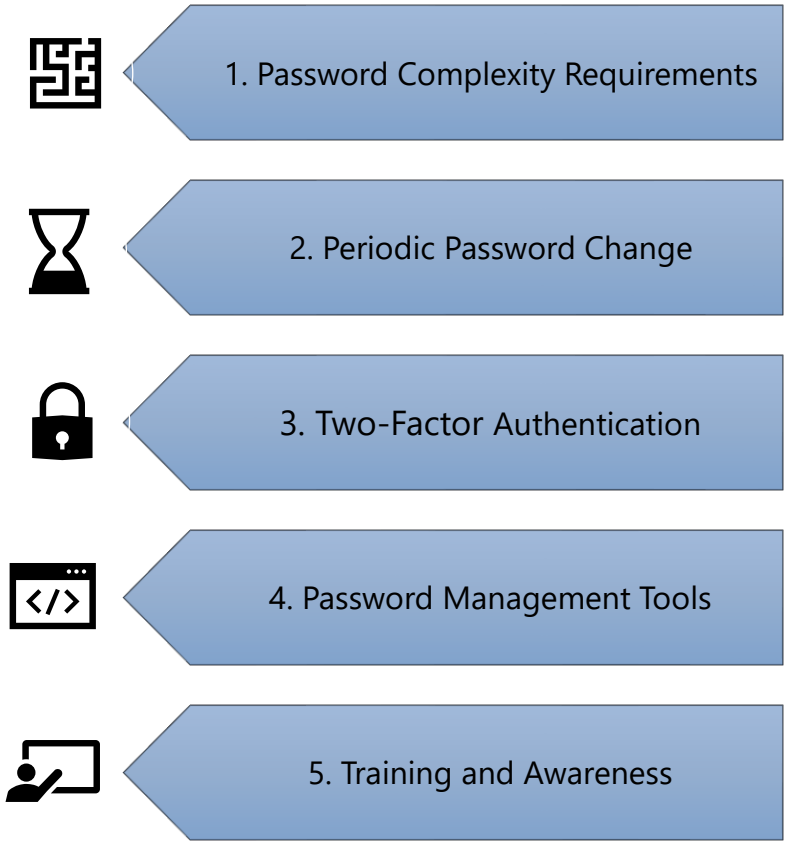
Passwords Storage and Protection

- ✓ A password manager is a technology tool that helps internet users create, save, manage and use passwords across different online services.
- ✓ Password protection is one of the most common data security tools available to users but they are easily bypassed if not created with hackers in mind.
- ✓ Strong passwords help protect data from bad actors and malicious software.

Co-funded by the European Union

Passwords Policies and Management Tools

- ✓ A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
- ✓ It provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.
- ✓ PM tools can also synchronize passwords for users across multiple systems, allowing users to access multiple applications with the same password.
- ✓ Password Management tools are applications or services that help us create, securely store, and quickly autofill passwords when necessary.
- ✓ The purpose of a password manager is to help us control our passwords and keep secure credentials everywhere we sign up



The Importance of Strong Password Policies

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Future Trends in Authentication

- Biometric authentication, such as fingerprints or facial recognition, to verify a user's identity.
- Multi-factor authentication (MFA), which requires users to provide multiple forms of authentication to access their accounts
- Private key offers a unique approach to authentication that simplifies the process while maintaining strong security.

Co-funded by the European Union

Security Policies and Procedure for Organizations

Key Points

- ✓ Developing Security Policies
- ✓ Creating Effective Security Procedures, Monitoring and Compliance
- ✓ Best Practices

Co-funded by the European Union

I. Developing Security Policies

01 Determine The Security Policy Principles

01 Verify The Security Policy

01 Review & Modify The Security Policy

01 Approve The Security Policy

Co-funded by the European Union

II. Creating Effective Security Procedures, Monitoring and Compliance

- ✓ **Create a plan**
- ✓ **Use technology**
- ✓ **Conduct surprise audits**
- ✓ **Encourage employee involvement**
- ✓ **Celebrate successes**

Co-funded by the European Union

III. Best Practices

- Focus On What To Do, Not How
- Make Policies Practical
- Right-Size Policy Length
- Keep Policies Distinct
- Make Policies Verifiable

Co-funded by
the European Union

Conclusion

Implementing robust security best practices and policies is essential for safeguarding organizational assets, data, and reputation. By fostering a culture of security awareness, regularly updating protocols, and investing in the right technologies, organizations can significantly reduce vulnerabilities. Continuous training and incident response planning ensure preparedness against emerging threats. Ultimately, a proactive and comprehensive approach to security not only protects against risks but also builds trust with stakeholders, ensuring long-term success in an increasingly digital landscape.

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

Resources

List the resources you used for your research:

Reference Books:

- Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
- B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
- Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
- Introduction to Cyber Security,Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

- https://www.researchgate.net/publication/339154293_Best_Practices_and_Recommendations_for_Cybersecurity_Service_Providers
- https://www.researchgate.net/publication/237848742_A_security_standards'_framework_to_facilitate_best_practices'_awareness_and_conformity
- https://www.sciencedirect.com/science/article/pii/S0167404823001189

Co-funded by the European Union