CYBERYOUTH

Non-formal education for cyber-security training & resilience of youth organisations and young people

Vulnerabilities, Attack, Techniques, and Threats

Session Activity 1

A Day in the Life of an Employee

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

Welcome to our session on threat scenarios and threat prevention. Today, we will be discussing how to understand potential threat scenarios in the workplace. Let's get started!

CYBERYOUTH

Co-funded by the European Union

Workplace Security Risks

Threat scenarios can be any situations or actions that pose a risk to the security of the workplace. It is important to identify these scenarios and take necessary measures to prevent them. Understanding the types of threats that can occur is the first step towards improving workplace security.

CYBERYOUTH

Co-funded by
the European Union

Common Risky Behaviors

Common risky behaviors that can lead to workplace security breaches include leaving computers unlocked, clicking on suspicious links or attachments, and mishandling confidential information. It is important to identify these behaviors and take steps to prevent them in order to minimize the risk of a security breach.

CYBERYOUTH

Co-funded by the European Union

Threat Prevention Strategies

Best practices for preventing workplace security breaches include implementing strong password policies, using encryption for sensitive data, restricting access to confidential information, and regularly updating security software. These strategies can help to prevent security breaches and protect the workplace from potential threats.

CYBERYOUTH

Co-funded by the European Union

Personal Responsibility for Workplace Security

Maintaining workplace security is not just the responsibility of the IT department or security personnel. Every employee has a role to play in keeping the workplace secure. By following best practices and being vigilant for potential threats, employees can help to prevent security breaches and maintain a secure workplace environment.

CYBERYOUTH

Co-funded by the European Union

Listen and Analyse

Now, buckle up and listen carefully the story I will share with you. Take notes and try to spot as many unsecure actions that this employee partook in.

Let 's get going!

CYBERYOUTH

Co-funded by the European Union

THANK YOU!

CYBERYOUTH

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by the European Union

CYBERYOUTH
Non-formal education for cyber-security training & resilience of youth organisations and young people

Vulnerabilities, Attack, Techniques, and Threats

Session Activity 2

Spot the Security Threats

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

Welcome to our session on Security Awareness. Today, we will be discussing how in today's increasingly digital world, it's more important than ever to be aware of the security threats that can impact us both personally and professionally. Let's get started!

CYBERYOUTH

Co-funded by the European Union

What is security awareness?

Security awareness is the knowledge and understanding of potential security risks and threats, and the actions we can take to prevent them. It's about being proactive and taking steps to protect ourselves and our organizations from cyber attacks.

CYBERYOUTH

Co-funded by the European Union

Why is security awareness important?

A lack of security awareness can lead to serious consequences, such as data breaches, identity theft, and financial loss. By being aware of potential threats and taking steps to prevent them, we can reduce the likelihood of these negative outcomes and better protect ourselves and our organizations.

CYBERYOUTH

Co-funded by the European Union

Best practices for security awareness

To improve our security awareness, we can take a number of proactive steps, such as using strong and unique passwords, regularly updating software and applications, being cautious with email and attachments, and reporting any suspicious activity to IT or security personnel.

CYBERYOUTH

Co-funded by the European Union

Detect Threats Quickly

Now it's time to test your quick security threats spotting ability. You don't have much time to analyse the following scenarios, so focus and have fun!

Let 's get going!

CYBERYOUTH

Co-funded by the European Union

THANK YOU!

CYBERYOUTH

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by the European Union

CYBERYOUTH

Non-formal education for cyber-security training & resilience of youth organisations and young people

Vulnerabilities, Attack, Techniques, and Threats

Session Activity 3

Spot the Phish

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

Welcome to our session on email phishing. Today, we will be discussing the basics of email phishing and how to protect yourself against this common cyber attack. Let's get started!

CYBERYOUTH

Co-funded by the European Union

What is Phishing?

Phishing is a type of social engineering attack that aims to trick people into revealing sensitive information.

It typically comes in the form of an email, text message, or phone call that appears to be from a legitimate organisation.

In this session we will focus on email Phishing.

CYBERYOUTH

Co-funded by the European Union

Email Phishing

Email phishing is a common cyber attack where the attacker sends an email that appears to be from a legitimate organization in order to trick the victim into disclosing sensitive information such as passwords or credit card numbers.

To prevent falling victim to email phishing, it's important to be cautious when opening emails, check sender information, and avoid clicking on links or downloading attachments from unknown sources.

CYBERYOUTH

Co-funded by
the European Union

Phishing through Impersonation and Hoaxes

What is **Impersonation**?

Impersonation is a technique used in cyberattacks to deceive and manipulate victims.

In the case of email phishing the impersonation technique used is called **Email Spoofing**, where attackers send emails that appear to be from a trusted source but are actually fake.

CYBERYOUTH

Co-funded by the European Union

Phishing through Impersonation and Hoaxes

What is a **Hoax**?

Hoaxes are a type of social engineering attack in which an attacker uses deception to trick people into believing false information.

The different types of hoaxes that can be encountered include false warnings about non-existent computer viruses known as **virus hoaxes**, emails that ask you to forward the message to others known as email **chain letters**, false warnings about natural disasters or terrorist attacks known as **disaster hoaxes**, false claims about medical treatments or diseases known as **health hoaxes**, and false investment opportunities or lottery scams known as **financial hoaxes**.

CYBERYOUTH

Co-funded by the European Union

Examples

We will look at some examples of **email phishing** during the activity, and after that we will discuss the types of phishing attempts that you encountered and the strategies you used to identify them.

Let 's get going!

CYBERYOUTH

Co-funded by
the European Union

THANK YOU!

CYBERYOUTH

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by the European Union