CYBERYOUTH

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

Core Cybersecurity Principles

Session Activity 1

Bugs and shortcuts (and cybersecurity quiz)

Co-funded by the European Union

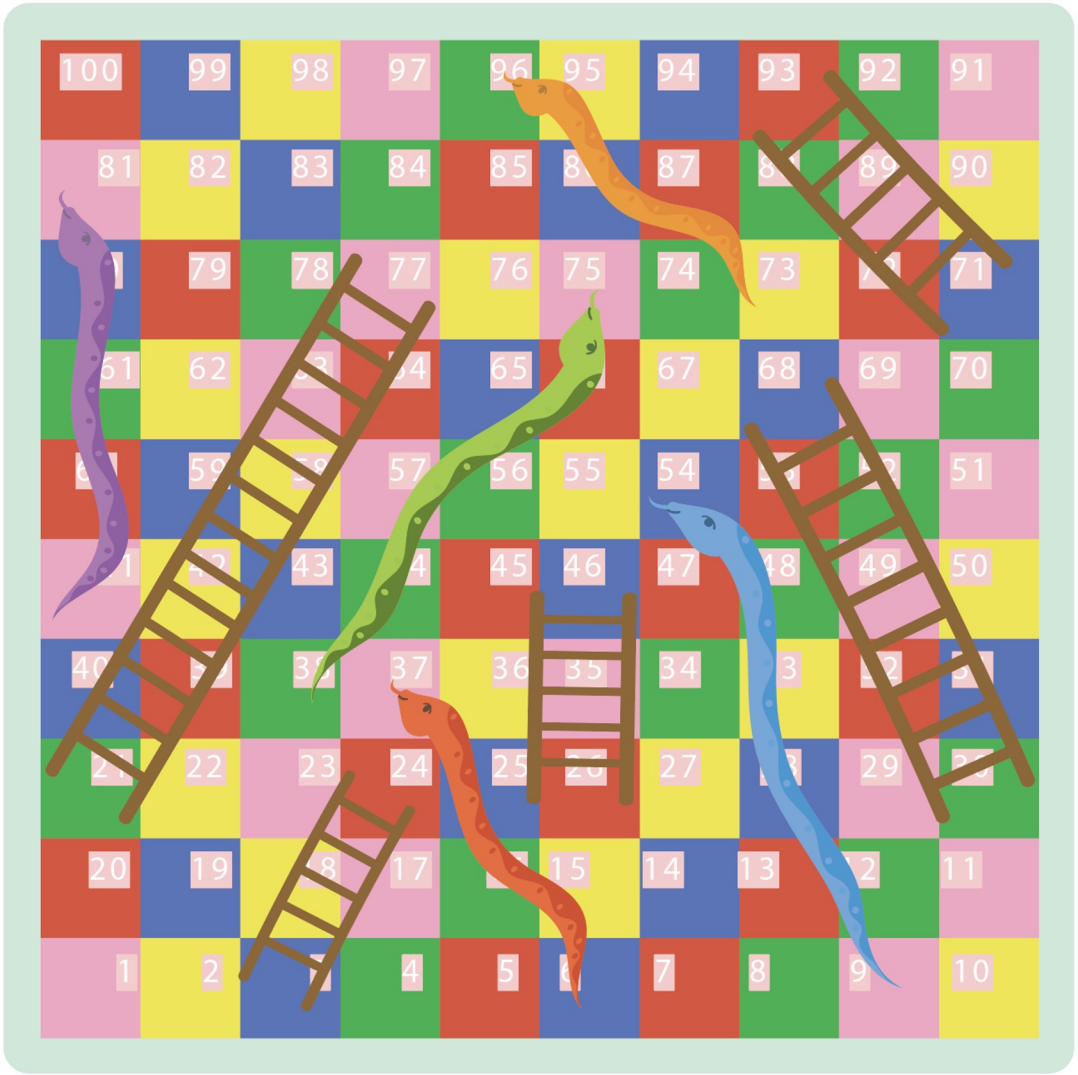
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Let’s play a game!

bugs and shortcuts

.. or also known as snakes and ladders



CYBERYOUTH

Co-funded by the European Union

What is the goal of the game

- Each team moves through the board and answers questions.
- There are two ways to win
  - answer correctly to one question from each of the colors (collect six colors)
  - or win by reaching the end of the board first

CYBERYOUTH

Co-funded by the European Union

Process

All participants randomly divide into 5 teams

Each team is assigned a token

Teams take turns rolling the dice. Tokens are moved on the board based on the number rolled. If you land on blue spot, you answer a question from the blue pile etc. There are six colors of questions for the different topics.

If you land on a bug (snake) or a shortcut (ladder) you move to the designated spot and then answer a question.

Teams work together on answering the questions.

CYBERYOUTH

Co-funded by the European Union

Don’t forget to have fun and work together!

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

Core Cybersecurity Principles

Session Activity 2

Secure or Vulnerable?

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!

You will be introduced to different scenarios. Your job is to discuss and vote whether they are secure or vulnerable.

Let’s go!

CYBERYOUTH

Co-funded by
the European Union

Sharing a password with a friend

CYBERYOUTH

Co-funded by
the European Union

Using a VPN

CYBERYOUTH

Co-funded by
the European Union

Writing your passwords in a notebook

CYBERYOUTH

Co-funded by
the European Union

Avoiding to install updates on different software

CYBERYOUTH

Co-funded by
the European Union

Connecting to public Wi-Fi

CYBERYOUTH

Co-funded by
the European Union

All of these unsecure scenarios have secure solutions. What could they be in your opinion?

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

Core Cybersecurity Principles

Session Activity 3

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!

Did you know that programmers, hackers and other people in the IT field have a special jargon and even humour that they use?

In today's game we will see who knows the most jargon words (if any) :)

CYBERYOUTH

Co-funded by the European Union

What we will learn together…

- You have 5 minutes to write at least 3 words that are hacker jargon
- No internet connection is allowed
- After the 5 minutes everyone reads their words/phrases to the group and explains their meaning
- the words are then checked with the Jargon file

CYBERYOUTH

Co-funded by the European Union

Did you get any right?

Here are some words that are from the jargon file but are heard in the mainstream occasionally.

CYBERYOUTH

Co-funded by
the European Union

Cookie

A handle, transaction ID, or other token of agreement between cooperating programs. “I give him a packet, he gives me back a cookie.” The claim check you get from a dry-cleaning shop is a perfect mundane example of a cookie; the only thing it's useful for is to relate a later transaction to this one (so you get the same clothes back). Now mainstream in the specific sense of web-browser cookies.

CYBERYOUTH

Co-funded by the European Union

Black hat / White hat / Gray hat

1. [common among security specialists] A cracker, someone bent on breaking into the system you are protecting. Oppose the less comon white hat for an ally or friendly security specialist; the term gray hat is in occasional use for people with cracker skills operating within the law, e.g. in doing security evaluations. All three terms derive from the dress code of formulaic Westerns, in which bad guys wore black hats and good guys white ones.

2. [spamfighters] ‘Black hat’, ‘white hat’, and ‘gray hat’ are also used to denote the spam-friendliness of ISPs: a black hat ISP harbors spammers and doesn't terminate them; a white hat ISP terminates upon the first LART; and gray hat ISPs terminate only reluctantly and/or slowly. This has led to the concept of a hat check: someone considering a potential business relationship with an ISP or other provider will post a query to a NANA group, asking about the provider's hat color. The term albedo has also been used to describe a provider's spam-friendliness.

CYBERYOUTH

Co-funded by
the European Union

Samurai:

A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith. In 1991, mainstream media reported the existence of a loose-knit culture of samurai that meets electronically on BBS systems, mostly bright teenagers with personal micros; they have modeled themselves explicitly on the historical samurai of Japan and on the “net cowboys” of William Gibson's cyberpunk novels. Those interviewed claim to adhere to a rigid ethic of loyalty to their employers and to disdain the vandalism and theft practiced by criminal crackers as beneath them and contrary to the hacker ethic; some quote Miyamoto Musashi's Book of Five Rings, a classic of historical samurai doctrine, in support of these principles.

CYBERYOUTH

Co-funded by
the European Union

Wetware:

[prob.: from the novels of Rudy Rucker]

1. The human nervous system, as opposed to computer hardware or software. “Wetware has 7 plus or minus 2 temporary registers.”

2. Human beings (programmers, operators, administrators) attached to a computer system, as opposed to the system's hardware or software.

CYBERYOUTH

Co-funded by
the European Union

Social engineering:

Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem. See also the tiger team story in the patch entry, and rubber-hose cryptanalysis.

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