



< DARE >

DARE to learn digital skills

Virtual Exchange in Higher Education and youth
101083723

*Course 1:
Online Training Course on Data Protection and
Cybersecurity*



Co-funded by
the European Union



DARE TO LEARN DIGITAL SKILLS

Introduction to the Course Syllabus:

Welcome to the Online Training Courses offered under the DARE 4.0 project.

These courses are designed to equip participants with essential skills in key areas of digital transformation, catering to both beginners and those with foundational knowledge.

Each course provides in-depth insights and practical knowledge to empower learners in today's digital landscape.

Course Descriptions:

1.Data Protection and Cybersecurity: The "Data Protection and Cybersecurity" course covers fundamental aspects critical to safeguarding data and navigating cybersecurity challenges. Participants will explore topics ranging from the basics of data protection regulations to understanding cyber threats and best practices in cybersecurity.

2.Digital Marketing and Crowdfunding: The "Digital Marketing and Crowdfunding" course delves into strategies essential for digital marketing success and effective crowdfunding campaigns. Participants will learn about content marketing, SEO techniques, social media strategies, and the dynamics of different crowdfunding models.

3.Social media and Social Media Strategies: The "Social Media and Social Media Strategies" course provides comprehensive insights into leveraging social media platforms effectively. Participants will discover how to develop impactful social media strategies, engage with influencers, harness AI tools, and manage social media platforms efficiently.

4.Social media, Cybersecurity, and Cyberbullying: The "Social Media, Cybersecurity, and Cyberbullying" course addresses the intersection of social media with cybersecurity and personal safety. Participants will learn about privacy protection, cyber threats on social media, handling cyberbullying, and maintaining a secure online presence.

5.Mobile App Development: The "Mobile App Development" course is designed to equip participants with the skills necessary to create mobile applications for various platforms. From app design principles to hands-on development using Android, iOS, and no-code platforms, participants will gain practical experience in app development.

Course Structure: Each course is structured into modules that progressively cover essential topics within the respective fields. Participants will engage in interactive learning activities, including video lectures, readings, practical assignments, and discussions. The courses are designed to foster a holistic learning experience, ensuring participants gain both theoretical knowledge and practical skills.

Learning Outcomes: Upon completion of each course, participants will:

- Gain a comprehensive understanding of the course topic.
- Acquire practical skills applicable to real-world scenarios.
- Be equipped to apply learned concepts in their professional endeavours.
- Receive a certificate of completion recognizing their achievement.

We invite you to embark on this educational journey with us and discover how these courses can empower you to thrive in the digital age.

Let's build a future where digital skills drive innovation and transformation.

All reading lists and problem sets can be found online on the platform:


<https://learning-youth-power.org/?s=DARE+4.0>





< DARE >

TABLE OF CONTENTS



Introduction to the course - Data protection and cybersecurity

Introduction to data protection and cybersecurity

Data and data theft

Cyber-threats

Personal data protection

Cybersecurity



Co-funded by
the European Union

SESSION TITLE/TOPIC:	Introduction to the course - Data protection and cybersecurity
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To introduce and get to know the participants •To present the course topic •To evaluate participants knowledge in the topic and expectations on the course
TIME:	110 + 35 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Getting to know participants (15 minutes)</u></p> <p>Name association (5 minutes) This is a good way for participants to remember each other's names. Every participant should say their name and tell one adjective starting with the first letter of their name for example. - I'm Andrew. A as Ambitious. If there are participants with the same first letter names, adjectives should not be repeated.</p> <p>One-Minute Introduction (10 minutes) Everyone - starting with the facilitator should introduce themselves in one minute. They should say more about themselves; i.e. their age, where they are from, what they like, their hobbies, interesting facts about them (for example. - I like coffee, I am a morning person...). Participants could give an interesting story that describes their interests and personality.</p> <p><u>Introducing e-learning system (10 minutes)</u></p> <p>The instructor should give the main information on how e-learning for this course works. Main topics that should be covered are: 1.How to access the course 2.How long does each course module takes to finish 3.Zoom sessions after every module 4.Where to find detailed information and instructions</p> <p><u>Introducing the course topic (35 minutes)</u></p> <p>In this part participants will be asked a few questions. In order to motivate them to actively participate, questions will be answered in different ways. After participants answer specific questions, provide them with time to discuss it. For example: I know about hacking because - I was hacked → Let the participant share his/hers story if he/she is willing to do so.</p> <p>True or false questions (10 minutes) If the answer is yes - leave the camera on, if answer is no - turn off the camera.</p> <p>Did you hear about cybersecurity? 1.I know the importance of cybersecurity. 2.I can name 3 cyber threats. 3.I know how to protect my data on the internet. 4.I cover my camera to protect my privacy.</p> <p>This or that questions (10 minutes) The participants should pick a term which is closest to their answer.</p> <p>I heard for cybersecurity terms through - school / social networks 1.I know about hacking because - I was hacked / I heard stories 2.If I want to protect my data I will - Not enter my information on the internet / Be more careful with giving my information on the internet 3.I will change my password because - I don't remember my last one / I am precautious 4.If I want to download my favourite game from the internet I will - Download the torrent / I will be worried about the viruses</p>

Course topic discussion (30 minutes + 10 minutes)

Defining the terms (15 minutes)A

Participants will be given a few terms mentioned in this course and they need to try to define them.

Data
Cyber attack
Privacy
Computer virus
Hacker
Security
Cyber crime
Encryption
Back up
Data Theft
Antivirus

Connecting cybersecurity with everyday security (15 minutes + 10 minutes)

Read an example to the group and ask them questions. This session will lead them to understand that cybersecurity is as important as real life security.

Example - A group of people walked in a bank. They explored the bank hallways and found their vault. They opened the door to the vault, and put the money in their bags. After some time they left the bank.

Questions:

Is this scenario possible in real life and why?
What security systems are stopping this from happening?
Can you connect this scenario with online money theft?
How can banks prevent this from happening online?

Possible Answers:

This scenario is not possible in real life because banks have their security systems. Robbing a bank is a possibility but you can not walk into the vault that easily and leave a bank like nothing happened.
Security guards in the bank, vault passwords and security, alarm systems etc.
There are scammers that can use multiple cyber attacks to gain access to the bank's system, their data etc., they can also use some attacks to scam employees for making transfers...
Setting a good security system, encryption for data, cybersecurity education for employees...

Let participants think of other real-life situations of a crime, security systems used to prevent them, connection between real life situations and similar cybercrime examples.

Course expectation discussion (15 minutes)

Ask participants about their expectations on the course

What are you expecting to learn?

Do you expect this course to have an impact in your daily life?

Will you pass your knowledge you gain in this course, to someone in your surroundings?

Do you expect this course to encourage you to explore more about this topic?

Begin learning (10 minutes)

Let the participants say one quote or to say something themselves to wish each other good luck in learning.

SESSION TITLE/TOPIC:	Introduction to data protection and cybersecurity
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To repeat terms included in the first module •To discuss module topic •To evaluate gained knowledge •To evaluate experiences with the module.
TIME:	100 + 20 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Module practice - Defining terms (10 minutes)</u></p> <p>Participants will be given a few terms they have learned about in this module and they need to explain them.</p> <p>List of the terms:</p> <ul style="list-style-type: none"> •Cybersecurity •Firewall •Hacker •Reconnaissance •Data masking •Phishing •Cyberbullying •Data breaches <p><u>Discussion (20 + 10 minutes)</u></p> <p>Open discussion with the participants. Now when they know more about data protection, privacy and cybersecurity, ask them about their experiences.</p> <p>List of topics for discussion:</p> <ul style="list-style-type: none"> •What had they already known; •How did they protect their data before; •Will they change their behaviour on the internet and what will they change etc. <p>Discussion should be led for topics of privacy and cybersecurity – as two discussions, each dedicated to one of the topics.</p> <p><u>Hacker VS cybersecurity (50 minutes)</u></p> <p>Separate participants into pairs so that one represents the attacker and the other one individual/company member.</p> <p>Using only knowledge, they gained in this module the attacker should create a way to collect the data, and the other one will need to think of all possible ways and solutions to stop/prevent it.</p> <p>Simple example:</p> <p>Attacker - Creating mail that represents a bank. Sending links to enter data so the bank account won't be disabled.</p> <p>Individual - After receiving an email, call a bank to check out the accuracy of an email. After being told about the scam, deletes the email and blocks the contact.</p> <p><u>Module evaluation (20 minutes + 10 minutes)</u></p> <p><u>Regular questions (10 minutes)</u></p> <p>Ask participants about their experience with this module. After a certain question you can let the participants share more information about their thinking and behaviour.</p> <p>Did this module meet your expectations?</p> <ol style="list-style-type: none"> 1.After completing this module have you explored more on yourself? 2.Did you share knowledge you gained in this module with others? 3.What would you change about this module?

True or false questions (10 minutes)

If the answer is yes - leave the camera on, if answer is no - turn off the camera. After a certain question you can let the participants share more information about their thinking and behaviour.

1. This module got me interested in this subject.
2. I am looking forward to learning more about cybersecurity and data protection.
3. I am thinking of starting a career in cybersecurity/ethical hacking.
4. After learning more about the risks I updated my passwords.
5. After learning more about the risks I installed firewalls and antivirus software.

SESSION TITLE/TOPIC:	Data and data theft
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To discuss module topic •To evaluate gained knowledge •To introduce deep web to participants •To evaluate experiences with the module
TIME:	95 + 35 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Discussion (15 + 10 minutes)</u></p> <p>Open discussion with the participants. Now when they know more about data and data theft, ask the participants about the topic. What did they already know; what surprised them the most; do they think that information they were provided will change their perspective; have they connect previous module with this one and how etc.</p> <p><u>What would I do? (20 minutes)</u></p> <p>With this game participants will be put in a few situations of data theft. Discuss with the participants how they would react and what would they do if they faced this situation.</p> <p>Situation A</p> <p>You received an email from Andrew that works for Instagram. In the email content it is stated that Instagram changed their privacy policy, and because of that every user needs to login manually on the link provided. When you open the link, it looks like a legit Instagram login page. This Instagram profile is really important to you. What would you do?</p> <p>Situation B</p> <p>Your day is busy, and suddenly you receive a phone call. On the other line is a man named Matthew. He calls from Amazon. Apparently, you ordered something worth \$2.500,00. Matthew needs you to confirm or cancel the order because it was suspicious. You do not want to be billed for something you did not order, so you say that you want to cancel the order. Matthew will guide you through the process. He will ask you for your information such as first and last name, the address, credit card number attached to the Amazon account. What would you do?</p> <p>Situation C</p> <p>You just finished downloading your favourite game from the internet. When you continued to the installation, your firewall warned you that this program can harm your PC or it may contain a suspicious program. Your friend just called to see if you are ready to play a game, you describe the problem you run into. Your friend tells you that it is okay, he downloaded multiple games from the same website and nothing has gone wrong. What would you do?</p> <p><u>Learning about deep web (45 + 15 minutes)</u></p> <p><u>Introduction (10 minutes)</u></p> <p>Ask participants a few questions to open the session topic. You can directly ask questions or using a true false model (If the answer is yes - leave the camera on, if answer is no - turn off the camera.) or using this or that model (The participants should pick a term which is closest to their answer.)</p> <p>Questions:</p> <p>Have you ever heard of the term “deep web”?</p> <ol style="list-style-type: none"> 1.How did you hear about the “deep web”? 2.Can you define what deep web is? 3.Do you know the difference between surface web and deep web? 4.If representing the web with the iceberg, the deep web is positioned where?

Presentation (25 minutes)

Using the presentation provided with session 3 outlines, participants will have a chance to learn about the deep web. Be aware that in this session we only discuss the deep web itself, so the dark web should not be included.

Q&A (10 minutes)

In this part let the participants ask the questions about the deep web, try to focus on questions so they don't include dark web topics and illegal things that can be found there.

Module evaluation (15 minutes + 10 minutes)**Regular questions (10 minutes)**

Ask participants about their experience with this module. After a certain question you can let the participants share more information about their thinking and behaviour.

Did this module meet your expectations?

After completing this module have you explored more on yourself?

Did you share knowledge you gained in this module with others?

What would you change about this module?

True or false questions (5 minutes)

If the answer is yes - leave the camera on, if answer is no - turn off the camera. After a certain question you can let the participants share more information about their thinking and behaviour.

This module got me interested in this subject.

I am looking forward to learning more about data privacy and protection.

After learning more about the risks, I changed my behaviour online

SESSION TITLE/TOPIC:	Cyber-threats
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To discuss module topic •To evaluate gained knowledge •To evaluate experiences with the module
TIME:	110 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Module practise - Defining terms (10 minutes)</u></p> <p>Participants will be given a few terms they have learned about in this module and they need to explain them.</p> <ul style="list-style-type: none"> • Malware • Trojan Horses • Worms • Spyware • Social engineering • Passphrases • Antivirus software <p><u>Discussion (20 minutes)</u></p> <p>Open discussion with the participants. Now when they know more about cyber threats, ask the participants about the topic.</p> <ul style="list-style-type: none"> • What did they already know; • What surprised them the most; • What cyberthreat sources they know about; • Have they ever been exposed to cyber-attack; • Do they think that information they were provided will change their perspective; • Have they connected the previous module with this one and how. <p><u>Prevent cyber-attacks (20 minutes)</u></p> <p>With this discussion game participants need to recognize cyber-attacks and think of a solution to prevent the attack or stop it while it is happening.</p> <p>Scenarios for the discussion game:</p> <ol style="list-style-type: none"> 1. While downloading a movie your PC is slowed down, the cursor is barely moving. 2. You opened a website and the window popped up that your phone has a virus and it offers you to download an antivirus software 3. You got an email to reset your Facebook password because someone tried to login using your login data 4. You are working for a big company. And someone is calling on the phone and introducing themselves as CEO, He wants you to send an urgent \$50.000,00 payment. <p>Participants need to discuss what the possible steps they would take would be, and further on discuss what would be the best solutions out of the steps suggested within the group. Facilitator concludes the game with conclusion on the best possible solutions and why it would that would be best solutions.</p> <p><u>Biggest cyber-attack (35 minutes)</u></p> <p><u>Watching documentary video (15 minutes)</u></p> <p>With the participants watch a video about the biggest cyber-attack in history. https://www.youtube.com/watch?v=GSNopHdNnKE</p> <p><u>Discussion (20 minutes)</u></p> <p>With the participants discuss video material. Let them share a cyber-attack story they may have heard of.</p>

Module evaluation (15 minutes + 10 minutes)**Regular questions (15 minutes)**

Ask participants about their experience with this module. After a certain question you can let the participants share more information about their thinking and behaviour.

1.

Did this module meet your expectations?

2. After completing this module have you explored more on yourself?

3. Did you share knowledge you gained in this module with others?

4. What would you change about this module?

True or false questions (10 minutes)

If the answer is yes - leave the camera on, if answer is no - turn off the camera. After a certain question you can let the participants share more information about their thinking and behaviour. Discussion should follow each of the questions – topics.

1. This module got me interested in this subject.

2. I am looking forward to learning more about this topic.

3. After learning more about the risks, I changed my behaviour online.

4. I am interested in cybersecurity/ethical hacking career.

SESSION TITLE/TOPIC:	Personal data protection
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To discuss module topic •To evaluate gained knowledge •To learn more about personal data protection •To evaluate experiences with the module
TIME:	120 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Module practise - Defining terms (10 minutes)</u></p> <p>Participants will be given a few terms they have learned about in this module and they need to explain them.</p> <p>Personal data Private information Data trading Location tracking Data Hoarding Data broker sites</p> <p><u>Discussion (20 minutes)</u></p> <p>Open discussion with the participants. Now when they know more about personal data protection, ask the participants about the topic.</p> <ul style="list-style-type: none"> •What did they already know; •Did they protect their data before; •Do they think that information they were provided will change their perspective; •Have they connected the previous module with this one and how. <p><u>Learning about IP address, proxy and VPN services (70 minutes)</u></p> <p>Introduction (20 minutes)</p> <p>Ask participants a few questions to open the session topic. You can directly ask questions or using a true false model (If the answer is yes leave the camera on, if answer is no turn off the camera.) or using this or that model (The participants should pick a term which is closest to their answer.)</p> <p>Questions:</p> <ol style="list-style-type: none"> 1. Have you ever heard of the term "IP address"? 2. What do you know about the IP address? 3. Have you ever heard of the term "proxy server"? 4. Have you ever heard about the VPN services? 5. Can you define VPN? 6. Do you use VPN? Why? <p>Presentation (40 minutes)</p> <p>Using the presentation provided with session 4 outlines, participants will have a chance to learn about the IP address, proxy servers and VPN.</p> <p>Q&A (10 minutes)</p> <p>In this part let the participants ask the questions about the IP address, proxy, VPN.</p> <p><u>Module evaluation (20 minutes)</u></p> <p>Regular questions (10 minutes)</p> <p>Ask participants about their experience with this module. After a certain question you can let the participants share more information about their thinking and behaviour.</p> <ol style="list-style-type: none"> 1. Did this module meet your expectations? 2. After completing this module have you explored more on yourself? 3. Did you share knowledge you gained in this module with others? 4. What would you change about this module?

True or false questions (10 minutes)

If the answer is yes - leave the camera on, if answer is no - turn off the camera. After each question discussion should follow the topic of the question.

- 1.This module got me interested in this subject.
- 2.I am looking forward to learning more about this topic.
- 3.After learning more about the risks, I changed my behaviour online.

SESSION TITLE/TOPIC:	Cybersecurity
SPECIFIC SESSION GOALS:	<ul style="list-style-type: none"> •To discuss module topic •To evaluate gained knowledge •To evaluate experiences with the module •To evaluate experiences with the course
TIME:	130 minutes
ACTIVITY & METHODOLOGY DESCRIPTION	<p><u>Module practise - Defining terms (15 minutes)</u></p> <p>Participants will be given a few terms they have learned about in this module and they need to explain them.</p> <ul style="list-style-type: none"> • Cybersecurity • Risk assessment • Implementation of proactive defence mechanisms • Threat intelligence • Application security • Authentication • Authorization • Encryption • Cloud security • Multitenancy • Misconfiguration <p><u>Discussion (20 minutes)</u></p> <p>Open discussion with the participants. Now when they know more about cybersecurity, ask the participants about the topic. What did they already know; do they think that information they were provided will change their perspective; have they connected the previous modules with this one and how etc.</p> <p><u>Cybersecurity never have I ever (40 minutes)</u></p> <p>Participants should have 5 fingers raised to the camera. Ask them questions below and if they have done or been in the situation, they need to put one finger down. You can ask participants to share their story after a certain question.</p> <p>Never have I ever ...</p> <ol style="list-style-type: none"> 1. Been hacked 2. Tried to log in into someone else's account 3. Shared my password 4. Changed my password in order to protect my data 5. Opened suspicious link 6. Set up two-factor authentication 7. Backed up my data 8. Stored my data to a cloud 9. Read privacy policy 10. Blocked firewall 11. Downloaded pirate games/movies/software 12. Installed antivirus 13. Give access to my files to unknown application 14. Accepted website cookies not knowing what they are 15. Used VPN to surf the internet 16. Encrypt my information 17. Ordered something online without checking web shop accuracy 18. Used false name to protect my privacy 19. Googled myself 20. Deleted my data from the google 21. Used the same password for multiple websites 22. Wondered how hackers work

Cybersecurity priorities (10 minutes)

After completing the cybersecurity and data protection course, ask participants to think and sort security methods from the highest level of importance for: individual and company separately.

Cybersecurity interesting facts (10 minutes)

First participants if they have some interesting cybersecurity facts to share. After that, discuss the facts below.

- 85% of people posting puppy photos are trying to scam you
- Every 39 seconds there is a cyber attack
- 43% of cyber-attacks target small business
- 75% of cyber-attacks start with an email
- Human error accounts for 95% of all data breaches
- The global average costs of a data breach is \$3.9 million
- On average, only 5% of companies' folders are properly protected.
- 21% of files aren't protected
- Cybercrime is quickly becoming more profitable than the illegal drug trade
- Word, Powerpoint and Excel (the Microsoft office formats) comprise the most prevalent group of malicious file extensions
- Cybercrime is set to cost \$6 trillion in 2021 - twice what it was in 2015
- The Netherlands has the lowest cybercrime rate, whilst Russia has the highest
- Ransomware is currently the leading technique used by cybercriminals
- The United States loses \$100 billion annually as a result of cybercrime, which targets over 594 million victims per year.
- As the Internet of Things (IoT) expands, cyber criminals have found new ways to target victims
- Social media users are also likely to click links posted by trusted friends, which criminals can use to their advantage.
- Links shared on Facebook and Twitter are sometimes the product of bots, which can lead to "spear phishing."

Module evaluation (15 minutes)**Regular questions (10 minutes)**

Ask participants about their experience with this module. After a certain question you can let the participants share more information about their thinking and behaviour.

Did this module meet your expectations?

1. After completing this module have you explored more on yourself?
2. Did you share knowledge you gained in this module with others?
3. What would you change about this module?

True or false questions (5 minutes)

If the answer is yes - leave the camera on, if answer is no - turn off the camera. After a certain question you can let the participants share more information about their thinking and behaviour.

1. This module got me interested in this subject.
2. I am looking forward to learning more about this topic.
3. After learning more about the risks I changed my behaviour online.
4. I am thinking of starting a career in cybersecurity/ethical hacking.

Course evaluation (20 minutes)

Ask participants about their experience with this course. After a certain question you can let the participants share more information about their thinking and behaviour.

Did this course meet your expectations?

1. Are you satisfied with the knowledge you gained in the field of cybersecurity and data protection?
2. Were online sessions useful for you?
3. What would you change in this course?



< DARE >

THE END

Thank Your For Listening

“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.”



Co-funded by
the European Union

