CYBERYOUTH

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

Implementation of Security Solutions

Session Activity 1

Who is There?

By Eseda, Estonia

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!

►In this session, you will learn about man-in-the-middle (MITM) attack, which is a cyber attack in which a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges and use them for malicious purposes like making unauthorized purchases or hacking.

CYBERYOUTH

Co-funded by the European Union

Eavesdropping in a Coffee Shop

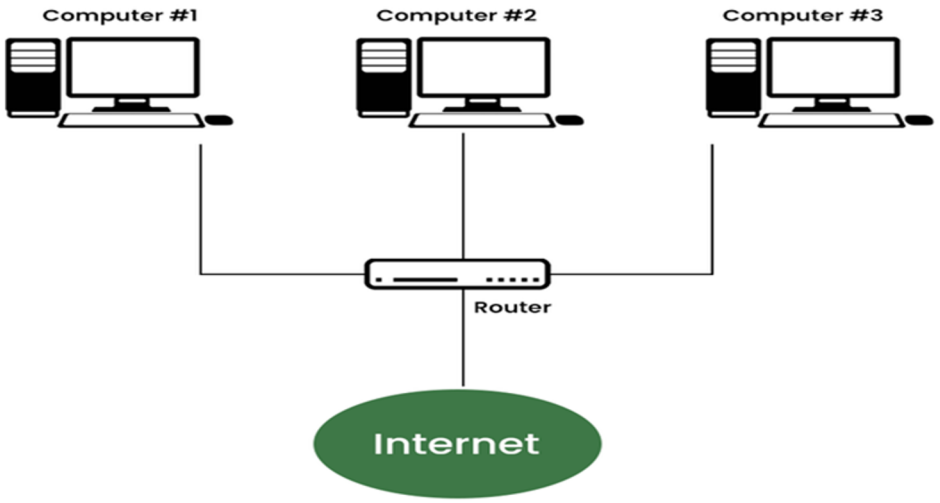
- DISCUSS:
- You meet a friend at a coffee shop to catch up. Little do you know that the person at the table next to you is listening in and recording everything you say.
- How would this make you feel?
- What could you do to ensure that no one eavesdrops on your conversation?
-
- Just like your conversations in public spaces like coffee shops are rarely private, your computing activity can be easily accessed and compromised when you use public WiFi.
- What types of information would you be scared of when an illegal hacker access? (Any idea, ex, account numbers, personal communication, passwords …)

CYBERYOUTH

Co-funded by
the European Union

Normal Internet Connection

- Normally, a user on a private network connects to the public internet through a router. The user's computer knows the router's IP address and sends its packets of information there. The router knows the computer's address so it sends it packets there. This connection is working as designed. (See the below image) (Seems pretty easy right))



CYBERYOUTH

Co-funded by
the European Union

How about if your internet connection is intercepted/watched?

- In a **Person-in-the-Middle attack, a bad actor inserts itself in between the user's computer and the router** by:
- convincing the router that it is the user's computer
- convincing the victim's computer that it is the router. (See the image)
- A man-in-the-middle (MITM) attack is a cyber attack in which a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges and use them for malicious purposes like making unauthorized purchases or hacking.

CYBERYOUTH

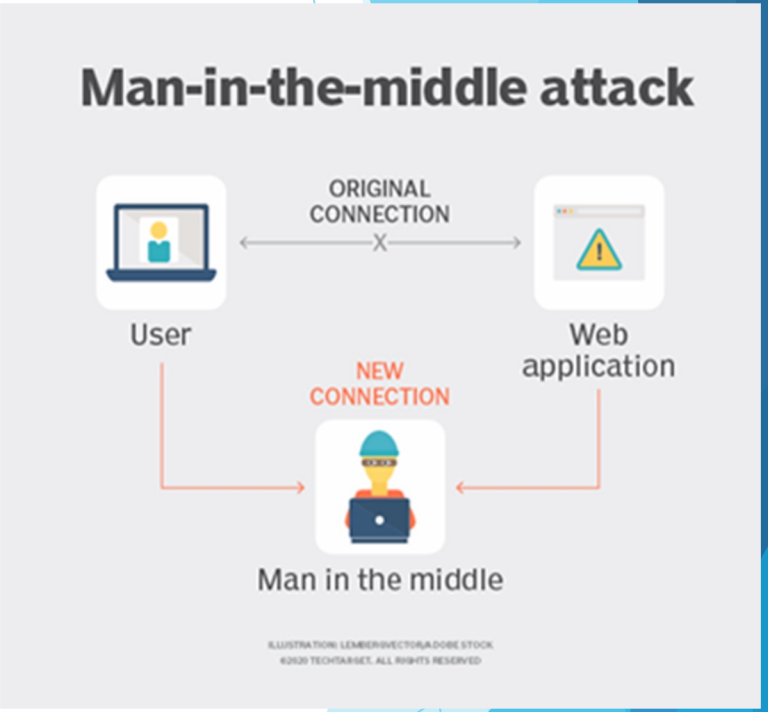
Co-funded by the European Union

How it works?

MiTM attacks are also sometimes referred to as *monster-in-the-middle*, *machine-in-the-middle*, *monkey-in-the-middle* and *man-in-the-browser* attacks. Man-in-the-browser is the most common type of MiTM attack in which the attackers focus on browser infection and inject malicious proxy malware into the victim's device. The malware is commonly introduced through phishing emails.

Once the attack is set up, the illegal hacker sees all incoming and outgoing information from the victim’s computer. This could mean seeing all the images on the victim’s computer or logging (capturing) every keyboard key the victim types. Worse, a person-in-the-middle attack actually gives the bad actor the opportunity to completely take over the computer..

MiTM cyber attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive personal information -- such as login credentials, account details or credit card numbers -- in real time.



CYBERYOUTH

Co-funded by the European Union

How it works?

►Typically, these attacks are carried out through a two-step process known as *data interception* and *decryption*. Data interception entails an attacker intercepting a data transfer between a client and a server. The attacker tricks the client and the server into believing that they are exchanging information with each other, while the attacker intercepts the data, creates a connection to the real site and acts as a proxy to read and insert false information into the communication.

►The following steps are involved in a common data interception technique:

►An attacker installs a packet sniffer to gauge any network traffic that might be insecure, such as a user accessing a Hypertext Transfer Protocol (HTTP)-based website or using a non-secure public hotspot.

►Once the user logs into the insecure website, the attacker retrieves the user's information and redirects them to a fake website.

►The fake website mimics the original website and gathers all the pertinent user data, which the attacker can then use to access all the user resources on the original website.

►The decryption phase is where the intercepted data is unencrypted. This essential step enables the attacker to finally decipher and use the data to their advantage; for example, they can carry out identity theft or cause disruptions to business operations.

CYBERYOUTH

Co-funded by the European Union

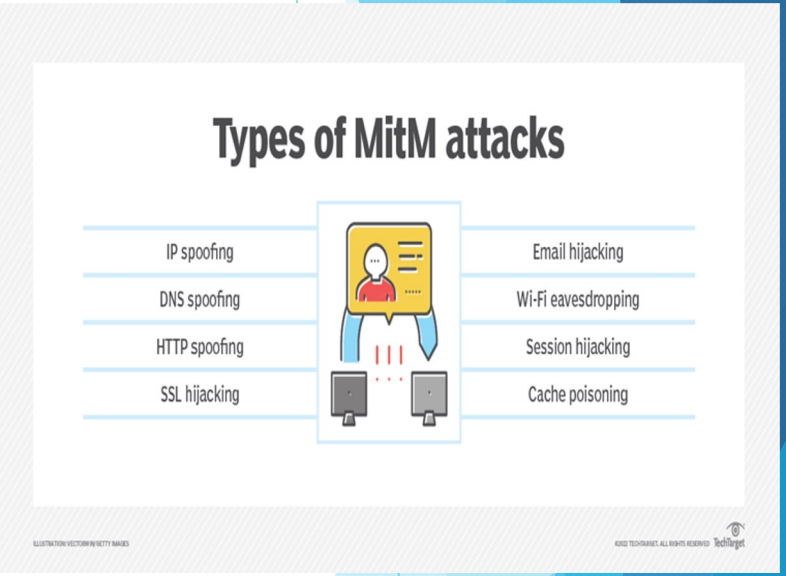
What are the types of man-in-the-middle attacks?

►To gain access to devices and sensitive information, cybercriminals use the following ways to conduct MiTM attacks:

►**Internet Protocol spoofing.** Like identity theft, IP spoofing takes place when cybercriminals alter the source IP address of a website, email address or device for the purpose of masking it. This dupes the users into believing that they are interacting with a legit source and the sensitive information they share during the transaction gets transferred to the cybercriminals instead.

►**Domain Name System spoofing.** This is a type of man-in-the-middle attack where cybercriminals alter domain names to redirect traffic to fake websites. Users might think that they are reaching a secure and trusted website, but instead, they land on a website operated by cybercriminals. The main aim behind DNS spoofing is to reroute traffic to a fake website or to capture user login credentials.

►**HTTP spoofing.** The HTTP protocol is the embodiment of secure internet communications. HTTPS indicates a safe and trusted website. During an HTTPS spoofing attack, a browser session is redirected to an unsecured or HTTP-based website without the user's knowledge or consent. Cybercriminals can monitor user interactions and steal shared personal information through this redirection.



CYBERYOUTH

Co-funded by the European Union

What are the types of man-in-the-middle attacks?

►**Secure Sockets Layer hijacking.** SSL is a protocol that establishes an encrypted connection between a browser and the web server. During SSL hijacking, a cybercriminal might use another computer and a secure server to intercept all information traveling between the server and the end user's computer.

►**Email hijacking.** This is a type of MiTM attack where cybercriminals gain control of email accounts of banks and other financial institutions to monitor any transactions that users conduct. Cybercriminals may even spoof the bank's email address and send instructions to customers that lead them to unknowingly transfer their money to the cybercriminals.

►**Wi-Fi eavesdropping.** This MiTM attack is one of the many risk factors posed by public Wi-Fi. During this attack, public Wi-Fi users get tricked into connecting to malicious Wi-Fi networks and hotspots. Cybercriminals accomplish this by setting up Wi-Fi connections with names that resemble nearby businesses.

►**Session hijacking.** Also known as stealing browser cookies, this malicious practice takes place when cybercriminals steal personal data and passwords stored inside the cookies of a user's browsing session. Sometimes, cybercriminals can gain endless access to users' saved resources. For example, they might steal users' confidential data and identities, purchase items or steal money from their bank accounts.

►**Cache poisoning.** Also known as Address Resolution Protocol, or ARP cache poisoning, this popular modern-day MiTM attack enables cybercriminals who are on the same subnet as the victims to eavesdrop on all traffic being routed between them.

CYBERYOUTH

Co-funded by the European Union

How to prevent man-in-the-middle attacks

- Mitigation is the best defense against MiTM attacks. The following highlights a few ways these attacks can be prevented:

- Secure connections. This is the first line of defense against MiTM attacks. Users should only visit websites that show "HTTPS" in the URL bar, instead of just "HTTP". Most browsers display a padlock sign before the URL, which indicates a secure website. Besides ensuring website security, it is also important to avoid using unsecured public Wi-Fi connections, as they are susceptible to attacks and interception by cybercriminals. Organizations should enforce multifactor authentication across the board, as it adds an additional layer of security to online communications.

- Avoid phishing emails. Cybercriminals purposely craft phishing emails to trick users into opening them. Users should think twice before opening emails coming from unverified or unknown sources. Phishing emails often look like they come from a legit source, such as a bank account or a financial institution. These emails might ask users to click on a link to enter their login credentials or update passwords. Clicking on these links should be avoided, as they might redirect a user to a fake website or download malicious software on their device.

Co-funded by the European Union

How to prevent man-in-the-middle attacks

- **Virtual private network encryption.** A VPN encrypts internet connections and online data transfers, such as passwords and credit card information and should be used when connecting to insecure public Wi-Fi networks and hotspots. A VPN can ambush a potential man-in-the-middle attack. Even if a cybercriminal manages to access a network, they will not be successful in deciphering the messages or accessing resources due to the encryption provided by the VPN. Organizations should also ensure their employees are logging into the company through a secure corporate VPN, especially if they are working remotely.

- **Endpoint security.** Implementing comprehensive endpoint security is paramount when trying to prevent the spread of malware and other cyber attacks. Because MiTM attacks use malware for execution, it is important to have antimalware and internet security products in place.

- Most cyber attacks are unknowingly initiated by human behavior. By educating users on the dangers of a MiTM attack and implementing mandatory proactive security awareness training for employees, organizations can preemptively safeguard their sensitive data. The training should also teach users how to spot malicious emails, and enlighten them regarding security best practices, such as implementing a VPN, avoiding public Wi-Fi networks and not clicking on suspicious email links.

CYBERYOUTH

Co-funded by the European Union

quiz

- Lets answer the quiz questions to evaluate what we have learnt.

1. **Which attack takes advantage of a trusted relationship that exists between two systems?**

A) Spoofing
B) Passwork quessing
C) Sniffing
D) Brute-force

2. **In what type of attack does an attacker resend the series of commands and codes used in a financial transaction to cause the transaction to be conducted multiple times?**

A) Spoofing
B) Man-in-the-middle
C) Replay
D) Backdoor

CYBERYOUTH

Co-funded by
the European Union

quiz

- Lets answer the quiz questions to evaluate what we have learnt.

3. The trick in both spoofing and TCP/IP hijacking is in trying to:

A) Provide the correct authentication token
B) Find two systems between which a trusted relationship exists
C) Guess a password or brute-force a password to gain initial access to the system or network
D) Maintain the correct sequence numbers for the response packets

4. The best way to minimize possible avenues of attack for your system is to:

A) Install a firewall and check the logs daily
B) Monitor your intrusion detection system for possible attacks
C) Limit the information that can be obtained on your organization and the services that are run by your Internet-visible systems
D) Ensure that all patches have been applied for the services that are offered by your system

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

Implementation of Security Solutions

Session Activity 2

Cryptography

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

You will learn

What is cryptography, its strategies and components.

CYBERYOUTH

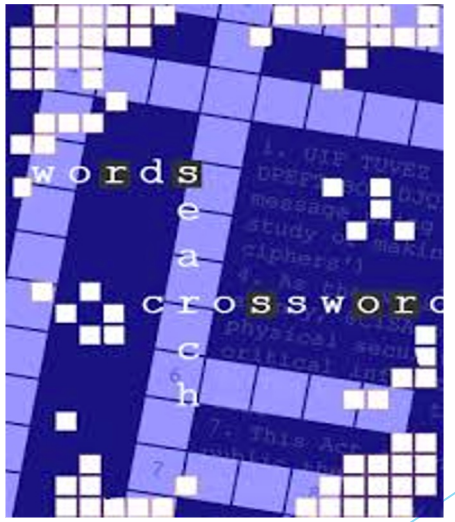
Co-funded by the European Union

Energizer

Do you like solving puzzles?

Do you like solving problems by following little hints and trying to reach to the final product?

Can you think of an example?



CYBERYOUTH

Co-funded by the European Union

Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

CYBERYOUTH

Co-funded by
the European Union

Authentication/Digital Signatures

Authentication and digital signatures are a very important application of public-key cryptography. For example, if you receive a message from me that I have encrypted with my private key and you are able to decrypt it using my public key, you should feel reasonably certain that the message did in fact come from me. If I think it necessary to keep the message secret, I may encrypt the message with my private key and then with your public key, that way only you can read the message, and you will know that the message came from me. The only requirement is that public keys are associated with their users by a trusted manner, for example a trusted directory. To address this weakness, the standards community has invented an object called a certificate. A certificate contains, the certificate issuer's name, the name of the subject for whom the certificate is being issued, the public key of the subject, and some time stamps. You know the public key is good, because the certificate issuer has a certificate too.

CYBERYOUTH

Co-funded by
the European Union

Time Stamping

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

Time stamping is very similar to sending a registered letter through the U.S. mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include patent applications, copyright archives, and contracts. Time stamping is a critical application that will help make the transition to electronic legal documents possible.

CYBERYOUTH

Co-funded by the European Union

HOW DO WE USE CRYPTOGRAPHY IN OUR DAILY LIFE?

The below are some of the examples of how we use cryptography in our everyday life.

- Cash withdrawal – Many banks have adopted an easy way to withdraw cash-using ATMs. It remains the most secure and easiest way to withdraw cash. Though you do not have to know why and how that is made possible, you should note it is all about encryption. The encryption is known as Hardware Security Module Encryption (HSM). It protects your PIN privacy and other sensitive information that is on your credit or debit card. The system also ensures cyber criminals do not access your PIN during data transactions or when using your ATM.
- HTTPS – It is the short form of Hypertext Transfer Protocol. It is an internet protocol. Information transfer is done widely across the World Wide Web, which is the Internet. The Internet has been in use since the 90s, and most of us are not aware why “HTTPS” comes before “www” in most internet addresses. The reason is it helps one to set information freely on the Internet.

  Information stored in HTTPS websites are plain texts, and you do not have to be an internet expert to know if it is relevant or not. It needs to store relevant information and other sensitive data. The information is secured with cryptographic secure socket layers.

CYBERYOUTH

Co-funded by the European Union

HOW DO WE USE CRYPTOGRAPHY IN OUR DAILY LIFE?

The below are some of the examples of how we use cryptography in our everyday life.

- Emailing – Email sites and apps like Gmail are not good at storing sensitive data or information, but it serves as a gate pass. YourYour email address has a unique piece of data cyber criminals require to infect your devices with malware or adware. Cryptography generator ensures your email has SSL encryption making it hard to receive a text in your email without encryption.

- Securing Houses -The best way to explain the importance of cryptography is how it is used in your house. Let's say you have installed security cameras around the house or you have installed the safest lock in the market, and a criminal can easily walk in without worrying about the installed security cameras. The same applies to your PC or other devices, you may have installed top-notch antivirus software, but it takes an infected USB to risk your data.

CYBERYOUTH

Co-funded by
the European Union

USEFULL RESOURCES

https://www.youtube.com/watch?v=6_Cxj5WKpIw

https://www.youtube.com/watch?v=5jpgMXt1Z9Y

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

Implementation of Security Solutions

Session Activity 3

Cloud Computing in Everyday Life

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

What we will learn

We will learn how cloud computing is being used in our everyday life with its various functions. You will be surprised with the number of everyday technology that we use are based on clou

CYBERYOUTH

Co-funded by the European Union

Energizers

Remember the early and not so fun days of video and audio streaming with a dial-up connection?

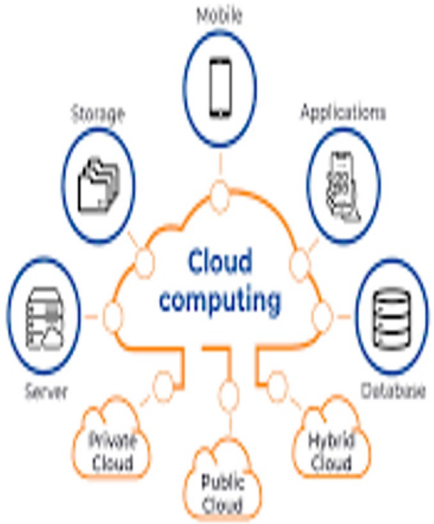
Have you ever wondered how your favourite shop knows what you recently viewed or which items to recommend to you?

CYBERYOUTH

Co-funded by
the European Union

What is cloud computing?

Cloud computing means computing on a network of servers accessible through a network connection in order to store, manage, and process data. And although we might not notice it, cloud computing has already changed our lives significantly. From how we communicate with each other to how we access information, how we travel, shop, watch our favourite shows and how business is done in general. Cloud computing affects most areas of our lives



CYBERYOUTH

Co-funded by the European Union

(1) Social media

No one can argue that social media hasn’t impacted the way everyday life is lived these days. Roughly half of the people in the world use some form of it and chances are, you are one of them. It has never been easier to keep in touch with your family and friends, network, or find people with similar interests to yours across the globe. Whichever social network you use, all of them use the cloud in one way or another - to store their users' content, for analytics, and to reduce the costs related to data backup and recovery in case a disaster occurs.

CYBERYOUTH

Co-funded by
the European Union

(2) Video and music streaming services

Remember the early and not so fun days of video and audio streaming with a dial-up connection? Both video and audio streaming has come a long way since then. And what helped it come this far were actually the advancements in the cloud computing technology. Those improvements revolutionised the way entertainment is delivered to us, bettered the performance and the viewing experience.

For example, users can now order Netflix products and services from almost anywhere in the world, using different devices in contrast to the few thousand DVD orders Netflix was able to process in the early days before migrating to the cloud.

CYBERYOUTH

Co-funded by
the European Union

(3) Online shopping

Have you ever wondered how your favourite shop knows what you recently viewed or which items to recommend to you? The answer is simple. They save all of this information to the cloud and use it whenever you sign in. Most online shops use the cloud to store the details that make completing future purchases simpler for their customers. They let you save your credit card details and mark items as favourites. Behind the curtains, cloud computing also enables them to more efficiently manage their inventory.

CYBERYOUTH

Co-funded by the European Union

(4) Wearables

Who is not counting steps these days? If you are using a fitness tracker or a smartwatch to track your activity, heart rate, or sleep, you are among the millions of adults who already use wearable technology. Wearables of all sorts are definitely in trend and due to growing awareness of the importance of healthy living, they are probably not going away any time soon. One of the key drivers behind the rapid spread of wearables is actually cloud computing. Users can simply log their activities into the cloud from multiple devices and sync those with their phones. On the other hand, the cloud gives the manufacturers an easy way to store and access customer data. By processing massive data that is at their disposal they are improving their future products and their features.

CYBERYOUTH

Co-funded by
the European Union

(5) Education

These days students, fortunately, have alternative options for pursuing and completing their degrees and are not constrained to rely on traditional methods of learning. And considering the times, it is great that they have the possibility to do that. Universities offer online courses and some degrees are available entirely through remote learning. The information and content materials utilized in courses are stored in the cloud, enabling students the access to it anytime and from anywhere. Cloud computing is improving accessibility, reducing costs and increasing collaboration in education processes and is helping educational institutions offer a more modern approach to learning.

CYBERYOUTH

Co-funded by
the European Union

(6) Storing data

Every day we create huge amounts of data. And what better way to store it than the cloud? Cloud storage is becoming increasingly popular for both personal and business use. Whether you use it for storing your family photos, for file-sharing with your team or for storing backups of your important business files, there is no denying cloud storage helps you organize your data and keep it safe. You can also easily access it anytime and anywhere, as long as you have a working internet connection.

CYBERYOUTH

Co-funded by the European Union

Useful Resources

https://www.youtube.com/watch?v=M988_fsOSWo

https://www.youtube.com/watch?v=BiPsPwcEOVE

https://www.youtube.com/watch?v=6u-tUqN9OP8

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