

Acronis

Cyber Foundation
Program

#CyberFit

Cyber safety basics

Level 2



Internet.

Good or bad?

Opportunities:

- Search for information
- Education
- Entertainment
(movies, music, games, books, etc.)
- Work
- Arts
- Travelling
- Maps and directions
- Chatting with friends
- Etc.



Internet.

Good or bad?

Threats:

- Scams
- Hacking
- Bullying
- Other types of cybercrimes



Digital era requires digital literacy

Internet is a common place and is not regulated by any authorities or police.

Best way to deal with negative experiences on the internet is to avoid them.



Stay alert and apply general logic rules:

- If someone asks you for money, your logins and passwords or personal data, it is most likely to be a scammer.
- Any trustworthy organization never asks for such details in emails or messages.
- If someone offers you money or a prize on the internet, it is most likely to be a scam.



Hackers and scammers



Hackers are often involved in cybercrimes. Being super professional technical experts, they can break into your computer system and steal all the data they want.

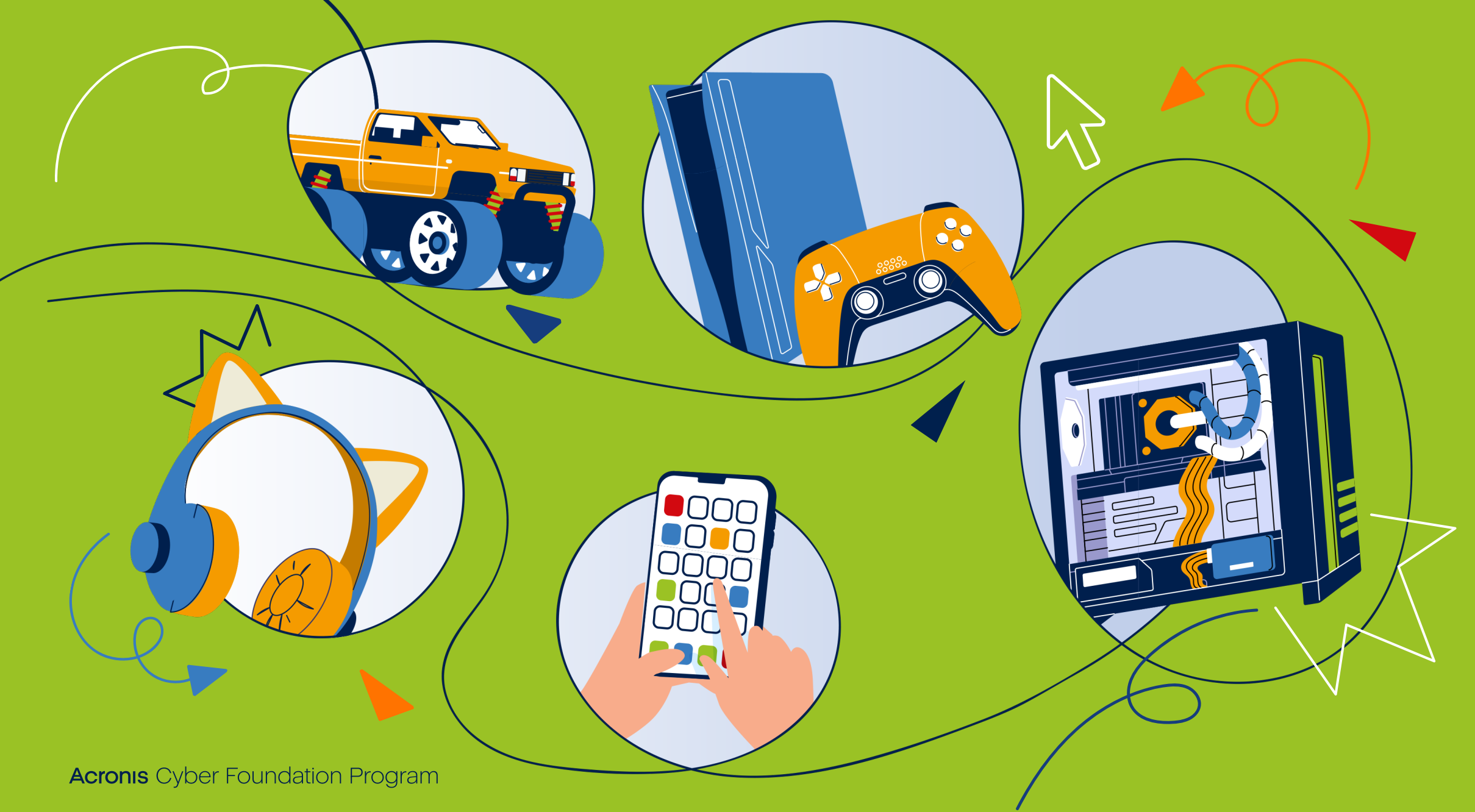
Scammers are people who commit or participate in a fraudulent scheme or operation.



Private and personal information

**What's something you own that others might be tempted to steal?
Why? What would they do with it?**





Acronis Cyber Foundation Program



**The most valuable thing you have and which is most likely to get stolen is not a toy or gadget.
It is your identity.**



What do you think that means?



How and why can it be stolen?

Identity theft is a type of cybercrime in which your private information is stolen and used for criminal activity against you.

Private information is the type of information that can be used to identify you because it is unique to you (i.e., your full name, address, contact data, birthdate, etc.)



Private information





Information that can be used to identify you because it is unique to you (i.e., your full name, address, contact data, birthdate, etc.)

Personal information



Information about you that cannot be used to identify you because it is also true for many other people (i.e., your eyes color, your favorite movie, a city where you spent your last vacation in, etc.)





Private information is the most risky to share because it can be used to identify you individually.

Private information

home address
a photo of yourself with your home address behind you
email address
date of birth
favorite song
how many brothers and sisters you have
your geo location
phone number
credit card information
your favorite food
your full name
name of your pet
name of your school
a picture of your pet
your mother's maiden name
your favorite color
your favorite sport
social security number

Personal information

You cannot record calls, videos and other type of content involving other people **except you without their consent.**



What can criminals do with **stolen identities**?

- Apply for bank loans
- Purchase things from your credit cards or withdraw all the money from your bank account/
account of your parents
- Blackmail you to expose or misuse stolen personal data unless a ransom is paid
- Create your fake accounts to spread illegal information or carry out scams on your behalf or
simply behave like a fool publicly online
- Personal data, particularly healthcare information, can be used for medical identity theft, where
the thief gets medical treatment under your name
- Spy on you and your online activities
- Cyberbully someone while pretending to be you
- Create various false documents, i.e., a driving license under your name

How to stay safe?



- When surfing internet, apply general logic rules. If something seems too good to be true, it is most likely to be a scam.
- Never share your personal data in the internet.
- Beware of strangers: don't click any links or attachments coming from unknown resources.
- Download games, apps and files only through Play Market, Appstore or only from known and trustworthy resources like your school's digital library.
- Use strong passwords or passphrases to defend your devices and accounts.
- Don't share your passwords with anyone except parents and keep them in places which can't be accessed by other people.

How to create a **strong** password?



- **Don't use easy-to-guess passwords:** never use your name, surname, date of birth, telephone number, or simple numbers or words like **123456**, **password**, **Minecraft**, etc.
- A password should be at least **14 characters long**.
- A password should contain **different types of characters:** capital and lowercase letters, digits, special symbols.
- It can be easier to **use a passphrase (i.e., MinecraftIsCool246\$ or WhoRulesTheWorld?5)** or take out the first letters of each word from your phrase and add number and special symbols to create a password, **i.e. McKdlW!23 (My cat Kitty doesn't like Whiskas !23) or P&Mm@8ntc (Paul and Mary meet at 8 near the cinema).**

Kahoot time!

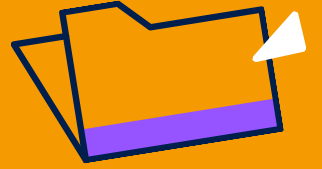




Quiz time!



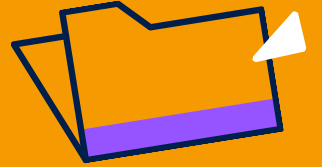
Question 1



You are having trouble accessing a task which a teacher assigned to you on the school website. Your friend Bob offers to help and asks for your password. Would you share it with him?

1. Yes.
2. No.
3. Yes, but will ask him to share his password as a guarantor of security.
4. None of the answers is correct.

Question 1



You are having trouble accessing a task which a teacher assigned to you on the school website. Your friend Bob offers to help and asks for your password. Would you share it with him?

1. Yes.

3. Yes, but will ask him to share his password as a guarantor of security.

2. No.

4. None of the answers is correct.

Question 2



You have downloaded a new app for sharing posts. All the posts there are public, not just shared with “friends”. What kind of information would be not safe to share?

1. Photos of you and your classmates in the school uniform in the school’s hall.
2. A cute video of your parrot.
3. News about your favorite movie.
4. All of the above.

Question 2



You have downloaded a new app for sharing posts. All the posts there are public, not just shared with “friends”. What kind of information would be not safe to share?

1. Photos of you and your classmates in the school uniform in the school’s hall.

3. News about your favorite movie.

2. A cute video of your parrot.

4. All of the above.

Question 3



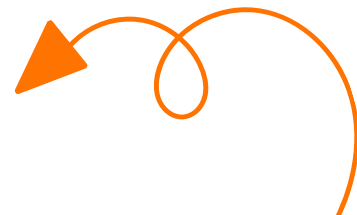
When you are setting up this new app for sharing posts, a message pops up and asks for permission to share your location. What geo location sharing option will you choose:

1. Always.

3. Only when using the app.

2. Never.

4. I will delete the app.



Question 3

When you are setting up this new app for sharing posts, a message pops up and asks for permission to share your location. What geo location sharing option will you choose:

1. Always.

3. Only when using the app.

2. Never.

4. I will delete the app.



Online threats

Phishing

Phishing is a common, effective and damaging type of cybercrime. In a phishing scam, cybercriminals will pose as legitimate representatives from banks and other agencies to try to obtain your valuable personal data via emails, text messages or telephone. They target to get your sensitive information like logins, password, banking and credit card details which will lead to your financial loss or identity theft.



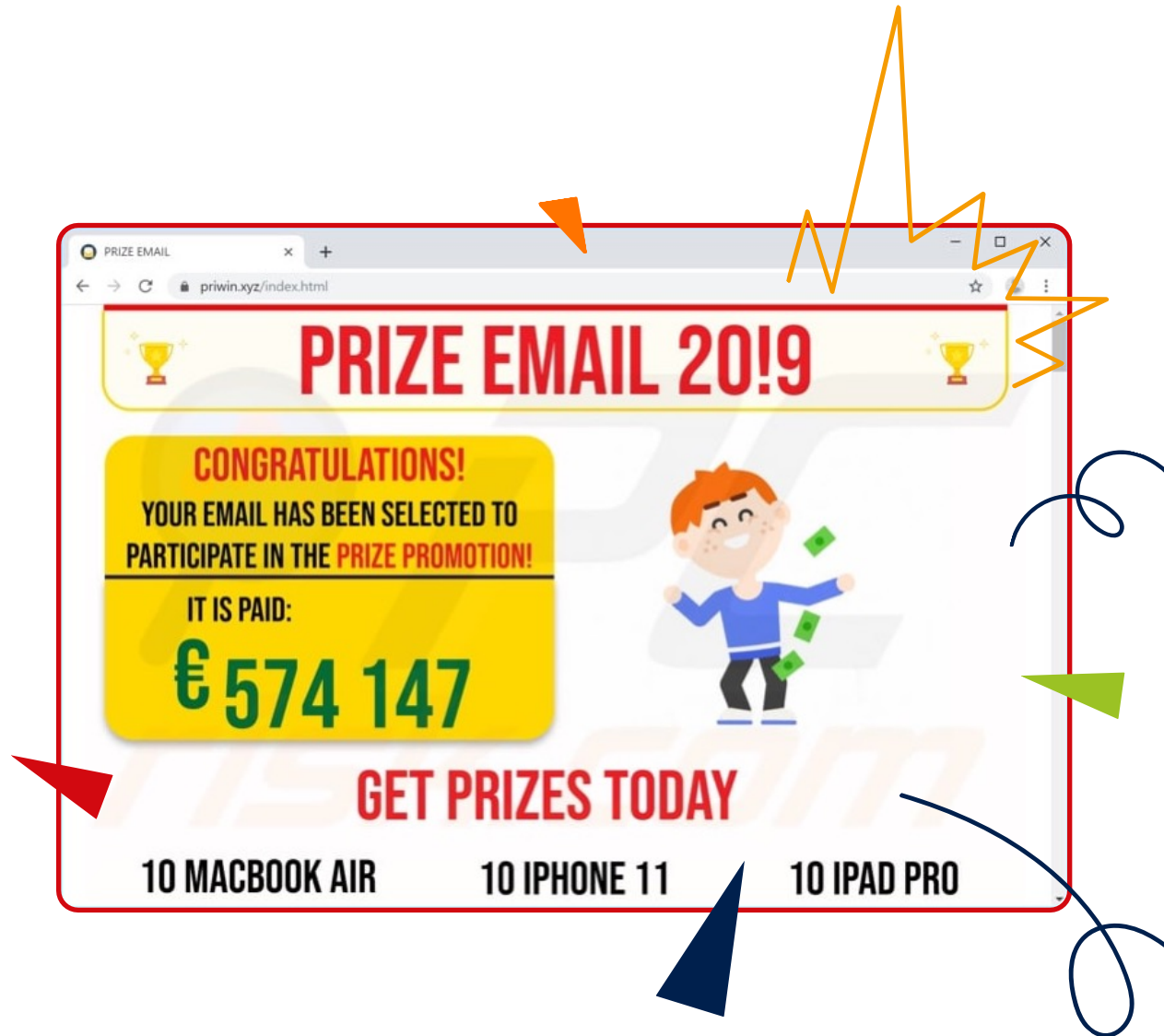
“Phishing” got its name from **“fishing”** which means that internet users can be like fish taking the bait and getting on a hook.



How do I recognize that I am being phished?

1. The received message tells you about some **prize** – you’ve won a lottery, your previously-unknown uncle from New Zealand has left you a fortune, or you’ve won an iPhone.

Don't click such links and emails, they are most likely to be a fraud!



How do I recognize that I am being phished?

2. Scammers would ask you to click a link or a button **urgently** because their offer is for a limited time or you should change your password urgently for your account not to get suspended unless you update your details immediately. Reliable organizations always provide a reasonable amount of time.

Text Message
Today 7:48 AM

Urgent notice for your USPS delivery 7H5S5 from 10/18/2023. Proceed to l8smk.info/GpFVv69nKV

Text Message
Today 1:07 PM

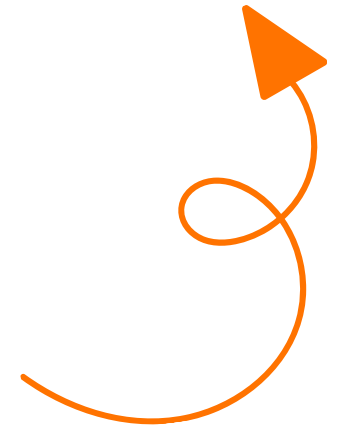
URGENT Your grandson was arrested last night in Mexico. Need bail money immediately Western Union Wire \$9500 <http://goo.gl/ndf4g5>

How do I recognize that I am being phished?



3. Watch for **misprints** or **similar-looking** to real companies' websites. For example, to dazzle a phishing website as a normal one, scammers can have a website having identically the same name as your bank but with a misprint.

Instead of going to **www.yourbank.com**, you can click on **www.youbank.com** and get defrauded there. Or it can be **www.bankofarnerica.com** instead of **www.bankofamerica.com**, which looks very identically.



How do I recognize that I am being phished?

4. Links and hyperlinks can be not what they seem to be. To be on the safe side, copy and paste it into your browser's address bar and then compare it to the real address of the company.

The same refers to shortened links (web addresses that have been condensed). Such a website may install malware on your device, steal your information, and charge you money.

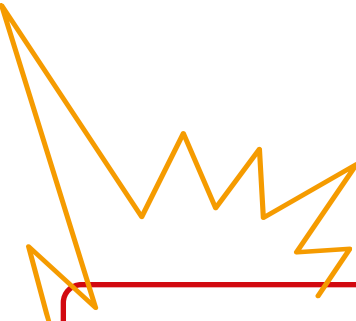




Urgent notice for your USPS
delivery 7H5S5 from 10/18/2023.
Proceed to l8smk.info/GpFVv69nKV

Hi John! Did you know that
we've made new, exciting
game. You'll find it here:
<http://cut.li/AoY8>

Thank you for your order!
Please confirm it with Chase
<https://chase.lc/3TjL7qn>



RT: @ [REDACTED]: Seems like Twitter is using
Google App Engine. Full site and all profiles
here: <http://bit.ly/d32mfH> [via @ [REDACTED]]

Soon will lose your membership

Hi,

We could not authorize your payment for the next
billing cycle of your subscription therefore we've
suspended your membership. But your current
subscription is active until it expires.

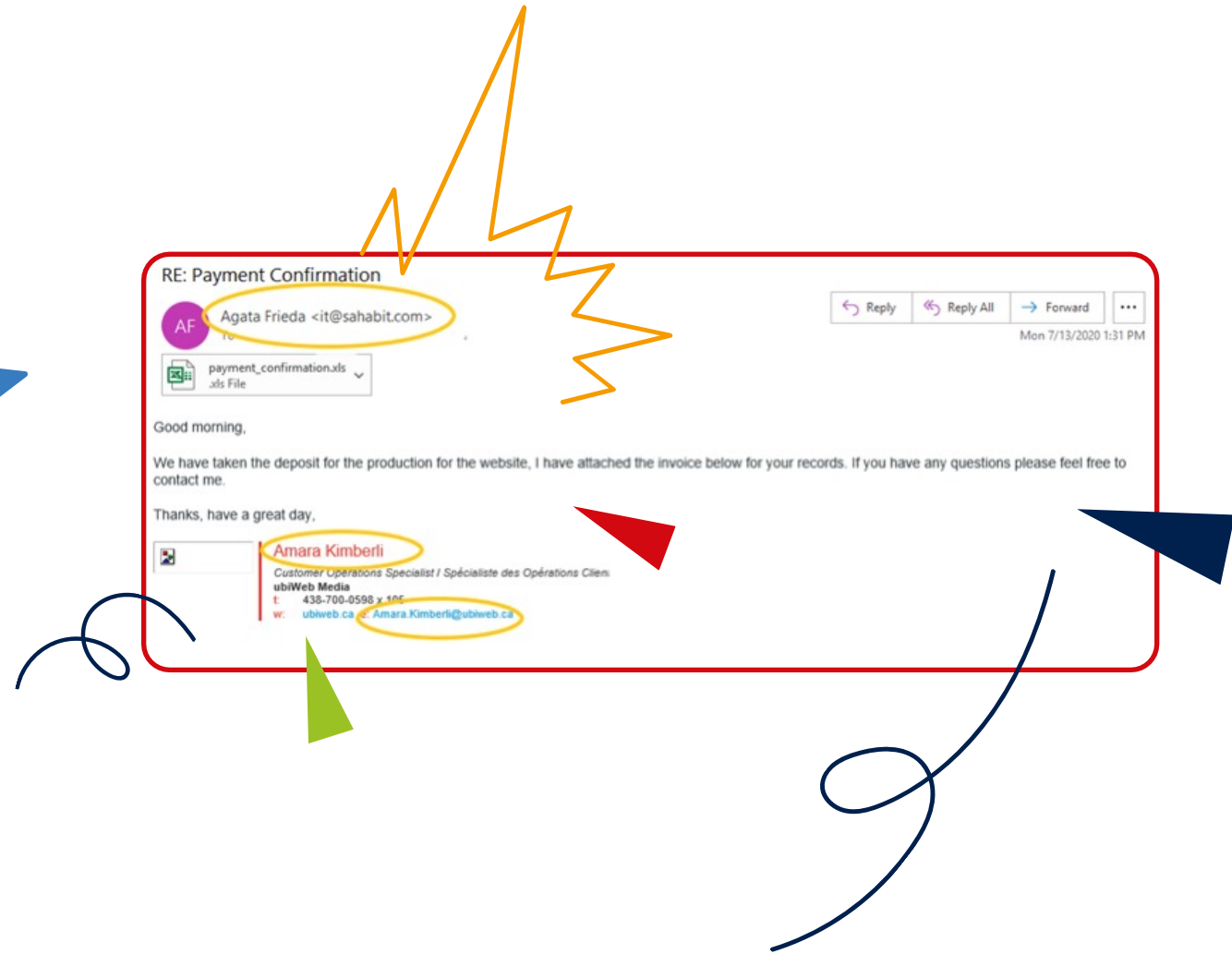
You can [restart your membership](#) at any time to
continue watching your favorite TV shows and
movies without interruption.

<https://cutt.ly/ajkq2we>
click or tap to follow link.

RESTART MEMBERSHIP

How do I recognize that I am being phished?

5. Many phishing emails contain an **attachment**. If you were not expecting such an email or it doesn't make sense, do not open the attachment!



How do I recognize that I am being phished?

6. If the email or SMS came from an **unusual or unknown sender**, or if anything seems weird and doesn't make sense, do not open it.



How do I recognize that I am being phished?

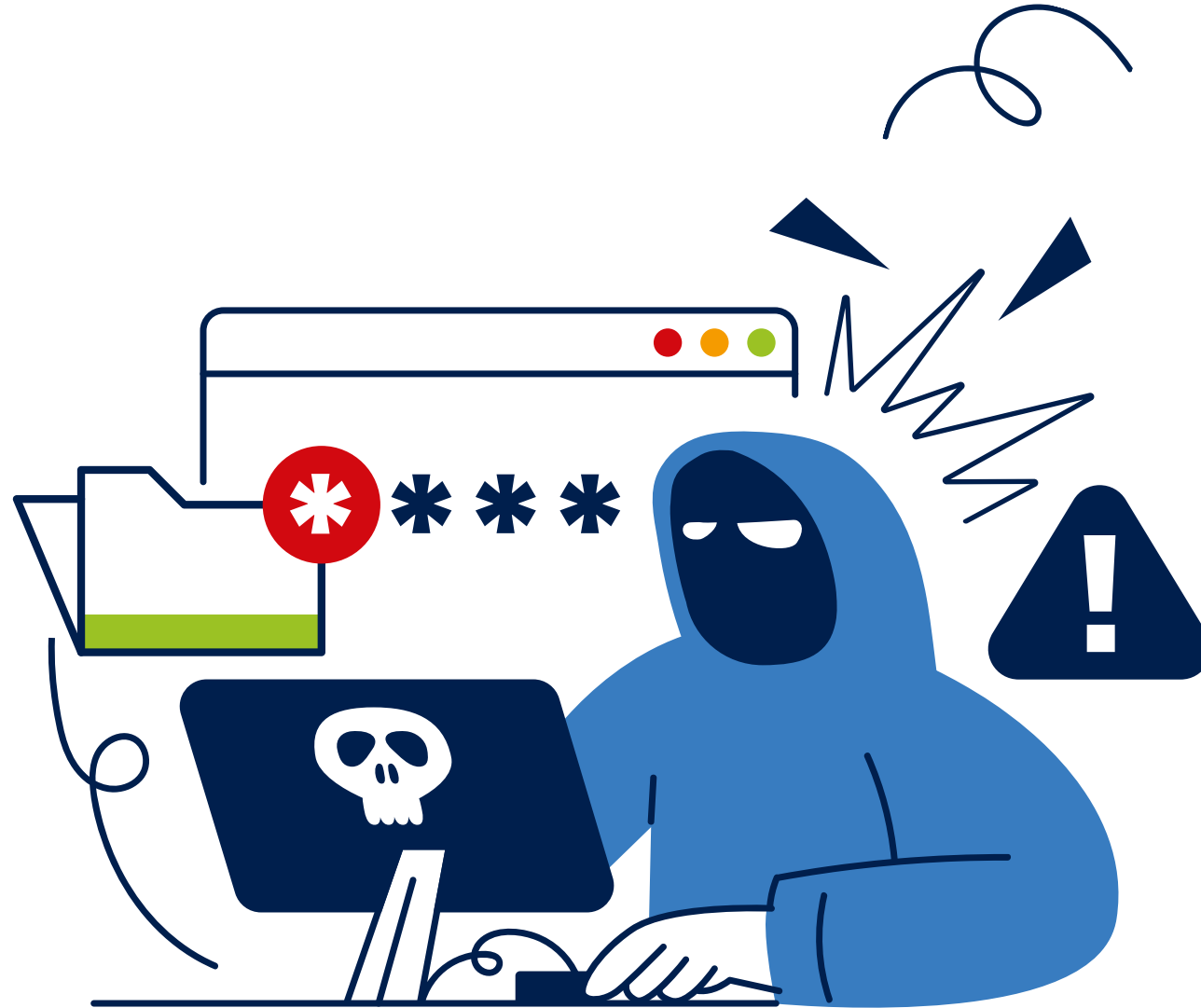
7. Sometimes, a phishing email can be **not personal**. If you are registered at a service and in its email it refers to you as “Dear client”, it’s most likely to be a fraud. However, referring to you by your name does not automatically mean it is a safe email. Advanced cybercriminals can steal organizations’ databases and use people’s personal data.



The future of phishing

Technologies and creative industries progress non-stop, so do cybercrimes. They get more and more difficult to recognize and deal with. It is considered that in future phishing and other types of cybercrimes will be more spread.

So, always stay alert and apply general logic rules while using internet and digital devices!



Malware

Malware is a contraction of malicious software.

Under this term, almost any type of damaging or fraudulent software is meant. The most common of them are viruses, Trojans, spyware, and ransomware.

By using malware, cybercriminals harm or exploit devices, services and networks, which usually results in financial losses for users.



Types of malware



Viruses



Ransomware

Worms



Spyware

Trojans

Scareware

Adware

Common symptoms that your device is infected with malware:

- Slow performance of the device
- Frequent pop-up advertisements and infection warnings, often urging to buy anti-virus software
- Shutting down and starting up your device without any apparent reason
- Your browser takes you to websites which you did not click on



Who and why uses malware?

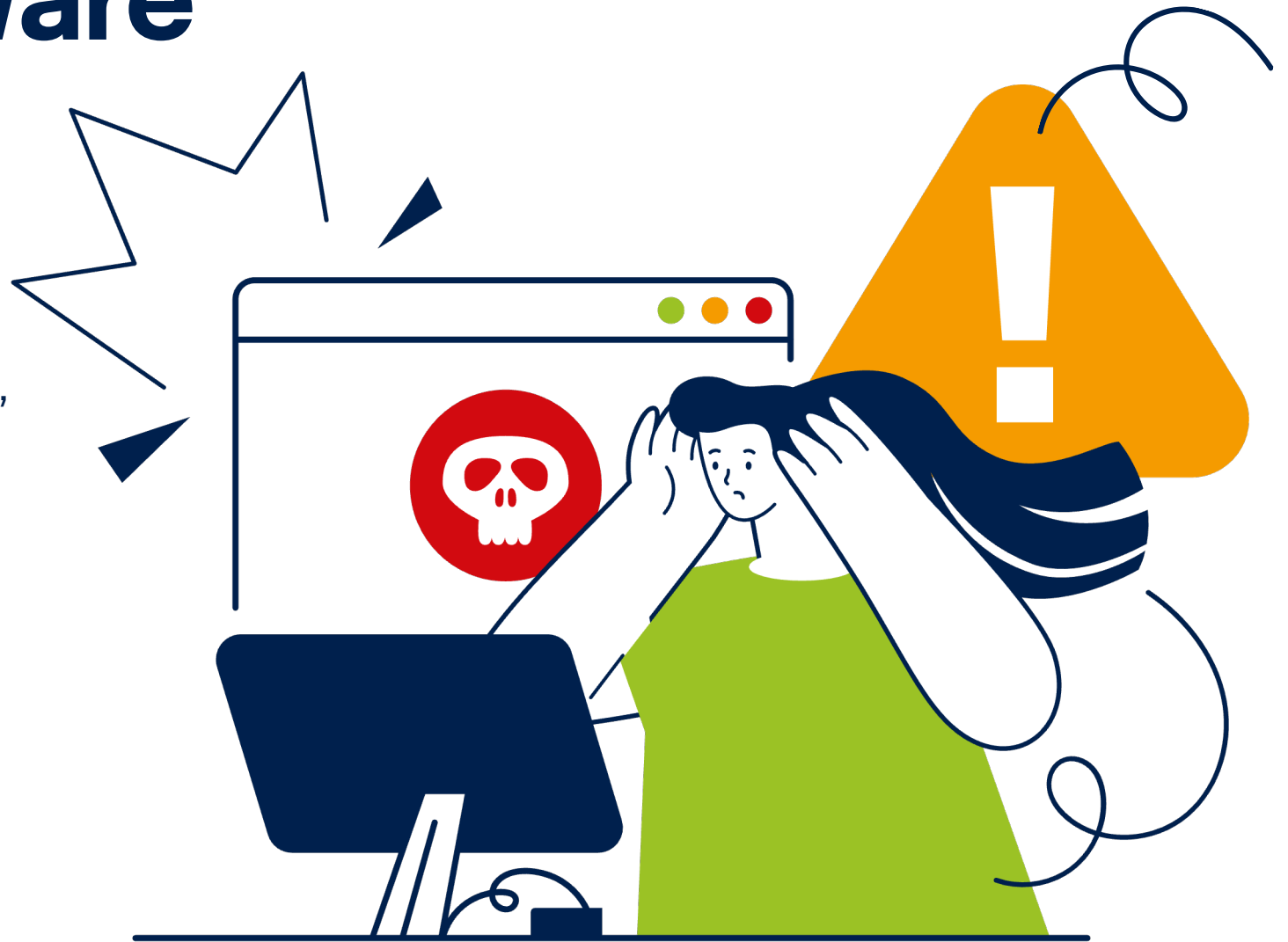
Hackers create malicious programmes to:

- steal people's money
- steal personal data
- sell their software to other fraudsters
- attack companies and get control over their computers
- use them to mine bitcoin or other cryptocurrencies



How is malware spread?

It attacks people and devices via infected attachments, applications, software and USB drives, banners or links leading to an infected source in the internet.



Antimalware software

Antimalware software are created to protect IT systems and individual computers from malware.

Antimalware programs scan a computer system to prevent, detect and remove malware.



Remember:

Combine healthy internet surfing habits with anti-malware software, because hackers have found ways to steal and damage data in all the ways possible and a lot of malware have outstanding protection tools and are even unable to be deleted once installed on a device.

Only always staying aware and alert you will be able to avoid threats and enjoy the digital world.



Kahoot time!





Quiz time!

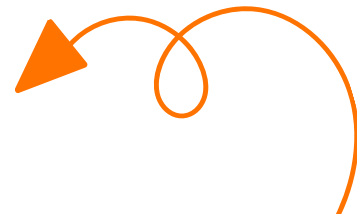


Question 1



You get an email from john.smith@yahoo.com. It says: “Hey, look what I found. Do you remember when we were taking this picture?” and has an attachment. Will you open it?

1. Yes, though I don't remember who John Smith is. He must be some of my schoolmates, frankly speaking, I do not remember all of them.
2. Sure, John is one of my old buddies, but I haven't heard from him for a while and not sure that it's his email address. Nonetheless, it's so nice to get a note from him.
3. No, John is one of my old buddies, but I haven't heard from him for a while and not sure that it's his email address. I will call him to confirm if the email is really coming from him or will just ignore it.



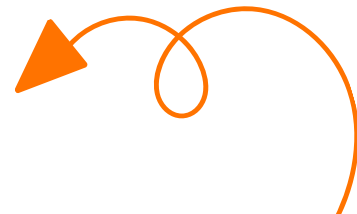
Question 1



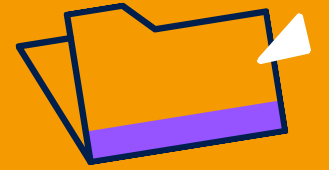
You get an email from john.smith@yahoo.com. It says: “Hey, look what I found. Do you remember when we were taking this picture?” and has an attachment. Will you open it?

1. Yes, though I don't remember who John Smith is. He must be some of my schoolmates, frankly speaking, I do not remember all of them.
2. Sure, John is one of my old buddies, but I haven't heard from him for a while and not sure that it's his email address. Nonetheless, it's so nice to get a note from him.

3. No, John is one of my old buddies, but I haven't heard from him for a while and not sure that it's his email address. I will call him to confirm if the email is really coming from him or will just ignore it.



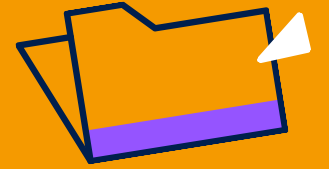
Question 2



Which of the below is the indicator that a message is phishing?

1. It says “Alert! Alert!”
2. There is a grammar mistake in the message.
3. The greeting is generic: “Dear customer”.
4. All of the above.

Question 2



Which of the below is the indicator that a message is phishing?

1. It says “Alert! Alert!”
2. There is a grammar mistake in the message.
3. The greeting is generic: “Dear customer”.
- 4. All of the above.**

Question 3



You see a message: “Special offer from Netflix! Why waits MONTHS for your favorite series to return? Watch free at Free_NFlixTV.” What should you do?

1. Open the message, it is from Netflix, everyone knows Netflix.
2. Forward the message to your friend, he also likes the series.
3. Don't open the message, it is scam.
4. Open the message, passing a free offer is stupid.

Question 3



You see a message: “Special offer from Netflix! Why waits MONTHS for your favorite series to return? Watch free at Free_NFlixTV.” What should you do?

1. Open the message, it is from Netflix, everyone knows Netflix.
2. Forward the message to your friend, he also likes the series.

3. Don't open the message, it is scam.

4. Open the message, passing a free offer is stupid.

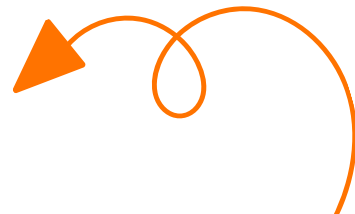
Question 4



What should you do if you accidentally clicked on a suspicious link?



1. Ignore it and do nothing.
2. Tell your friends about it.
3. Inform a trusted adult immediately.
4. Download an anti-virus software and apply it.



Question 4

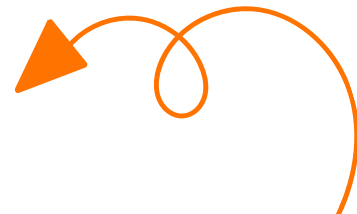


What should you do if you accidentally clicked on a suspicious link?

1. Ignore it and do nothing.
2. Tell your friends about it.

3. Inform a trusted adult immediately.

4. Download an anti-virus software and apply it.



Question 5



Malware is a malicious software, such as a virus, which is specifically designed to disrupt or damage a computer system.

1. True.

2. False.

Question 5



Malware is a malicious software, such as a virus, which is specifically designed to disrupt or damage a computer system.

1. True.

2. False.

Question 6



Malware can be installed without your knowledge

1. True.

2. False.

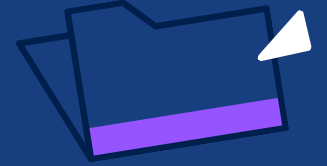
Question 6



Malware can be installed without your knowledge

- 1. True.
- 2. False.

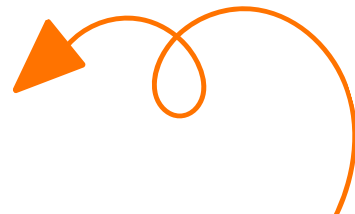
Question 7



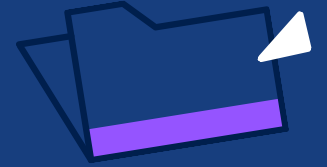
Which of the options are symptoms of malware? Select all which apply:



1. Broken speakers.
2. Random pop-ups.
3. Browser crashing.
4. Keys breaking on keyboard.
5. Poor system performance.



Question 7



Which of the options are symptoms of malware? Select all which apply:

1. Broken speakers.

4. Keys breaking on keyboard.

2. Random pop-ups.

5. Poor system performance.

3. Browser crashing.

Let's recap



- **When surfing internet, apply general logic rules.** If something seems too good to be true, it is most likely to be a scam.
- **Never share your personal data in the internet.**
- **Beware of strangers:** don't click any links or attachments coming from unknown resources.
- **Download games, apps and files only through Play Market, Appstore** or only from known and trustworthy resources like your school's digital library.
- **Pay attention to where you browse.** Stick to official and reputable websites and apps. Safe website must have a closed padlock in front of their name in the address line of the browser.
- **Use strong passwords or passphrases** to defend your devices and accounts.
- **Don't share your passwords** with anyone except parents and keep them in places which can't be accessed by other people.
- **Don't leave your devices unattended and unlocked.**





**Credible news
VS.
fake news**

What is fake news?

False information distributed deliberately, usually for political or commercial purposes.



There are two kinds of fake news:

- 1. Not all stories are true.** Some stories are designed to deceive people with false information, sometimes to buy a certain product or bait you to visit a certain website.
- 2. Some stories have truth but not 100 percent accurate.** For example, a part of a quote is only given, to give a false impression, instead of the full context. This is done deliberately, to convince the readers to give their support to a certain viewpoint or to attract the audience to an “urban myth”.



Why fake news appear and spread?

1. Misinformation and rumors, lack of media literacy
2. Clickbait and sensationalism
3. Financial gain
4. Manipulation and disinformation campaigns
5. Mistrust in mainstream media
6. Just for fun
7. Emotional manipulation
8. Identity and community building



Why fake news is a problem?

- They influence how people make decisions
- They disorient and confuse people
- People stop trusting all information sources




Topic vocabulary

A decorative orange arrow graphic that starts as a thin line, loops around, and ends as a solid arrowhead pointing towards the top left.

- **Bias** is an underlying opinion, point of view, or perspective of the world that guides your actions.
- **Corroboration** – an additional source that confirms or supports a news story, article or piece of information.
- **Credible** – able to be believed; trustworthy.
- **Evaluate** – to carefully examine something to figure out its value.

How to spot fake news



- **Read closely.** Does it make sense? Is it believable?
 - **Source.** Who is providing the information? Does it come from a credible, unbiased source?
 - **Look for corroboration.** Do other credible sources say the same thing?
 - **Motivation.** Why are they telling me this? Is there any bias? Is it promoting / advertising something?
 - **Evidence.** What evidence is provided for generalization?
 - **Clickbait images.** Fake news articles frequently use unrelated or sensational images to entice clicks, and some individuals profit from click counts.
- 

the **daily** mash

Thursday, 27th July 2023

POLITICS SOCIETY RELATIONSHIPS LIFESTYLE SPORT PREM

Woman leaves house to give her cat some space



?

England apologises after remembering cricket is all Australia has

3rd July 2023





BREAKING NEWS

Biggest Benefits Slaves Got From Slavery

Following Florida’s decision to release new standards for teaching African American history in schools, *The Onion* examines the biggest benefits slaves got from slavery.

BREAKING NEWS

Elderly Senators Amused To Discover Their Strokes Syncing Up

Published 5 hours ago



WASHINGTON—Discovering the phenomenon as they all received emergency medical attention at the same time, several elderly senators reportedly found it amusing Thursday that their strokes seemed to be syncing up. “I’ve heard of this

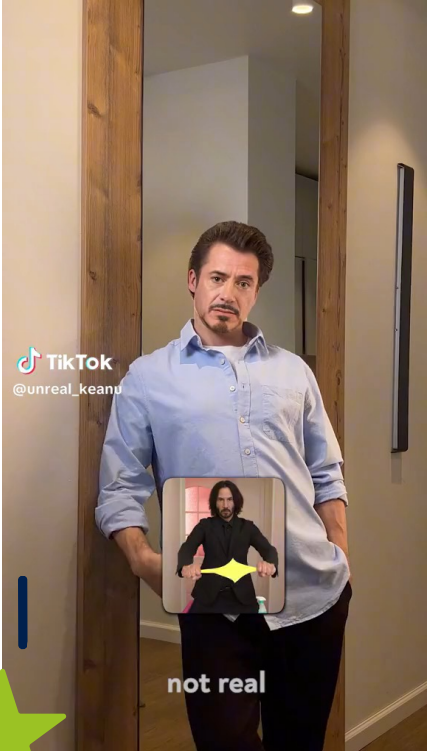


What is fake and what is real?

1. Voting age lowered to 12 in Romania
2. Top ten reasons to lower the voting age
3. Shocking UFO Sighting Captured on Tape!
4. Scientists Discover Immortality Elixir: Fountain of Youth Found in Amazon Jungle!
5. Stolen car owner tracks his vehicle to Texas shopping center lot where he shoots dead one thief and wounds the other while waiting for cops
6. Worldwide Pizza Shortage Predicted: Apocalypse of Cheesy Goodness!
7. Breaking News: Celebrities to Build Luxury Colony on Mars!
8. The pet of the future? Creepy robot dog can talk, perform handstands, and even take photos of you
9. New Study Reveals: Eating Ice Cream Every Day Leads to Weight Loss!
10. Exclusive! Thomas Brodie-Sangster and Talulah Riley are engaged!
11. Government Implements Mind-Reading Technology in All Smartphones!
12. Plastic surgeons detail the many cosmetic procedures they believe the reality star could have undergone
13. Flying Cars to Replace Traditional Vehicles: Traffic Jams to Become History!
14. Kim Kardashian rocks rare Hermes Birkin bag to soccer match in Japan

Deep fakes

Pictures, videos, or audios that fake events. They usually duplicate someone's voice and/or facial features and paste them onto an existent recording or a photograph.



Kahoot time!





Quiz time!

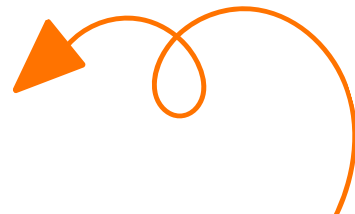


Question 1



What is fake news?

1. News that is fun to read but not necessarily true.
2. News articles that are shared by famous celebrities.
3. False or misleading information presented as if it were true.
4. Breaking news reported by reputable media outlets

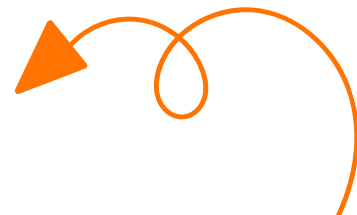


Question 1

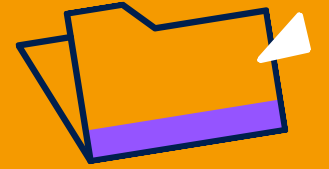


What is fake news?

1. News that is fun to read but not necessarily true.
2. News articles that are shared by famous celebrities.
- 3. False or misleading information presented as if it were true.**
4. Breaking news reported by reputable media outlets



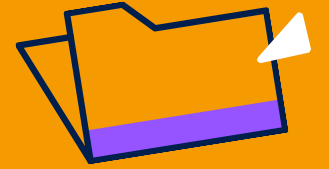
Question 2



How can you spot fake news?

1. Trust everything you read online.
2. Look for reputable sources and check if other news outlets are reporting the same information.
3. Share it immediately without verifying the facts.
4. Believe news that supports your opinions without questioning.

Question 2



How can you spot fake news?

1. Trust everything you read online.

2. Look for reputable sources and check if other news outlets are reporting the same information.

3. Share it immediately without verifying the facts.

4. Believe news that supports your opinions without questioning.

Question 3



What can you do to help stop the spread of fake news?

1. Share fake news articles on your social media to warn others.
2. Only believe news that aligns with your opinions.
3. Be critical of the information you encounter, fact-check, and don't share fake news.
4. Encourage your friends to share fake news to see how far it can go.

Question 3



What can you do to help stop the spread of fake news?

1. Share fake news articles on your social media to warn others.
2. Only believe news that aligns with your opinions.

3. Be critical of the information you encounter, fact-check, and don't share fake news.

4. Encourage your friends to share fake news to see how far it can go.

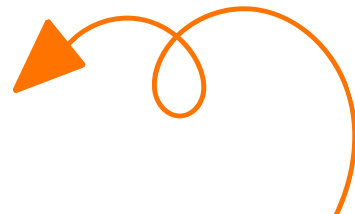
Question 4



What is a deepfake?



1. A type of fake news about the ocean.
2. A video or image that has been manipulated using artificial intelligence to make it look real.
3. A funny meme shared on social media.
4. A new dance move popular on TikTok.



Question 4



What is a deepfake?



1. A type of fake news about the ocean.
- 2. A video or image that has been manipulated using artificial intelligence to make it look real.**
3. A funny meme shared on social media.
4. A new dance move popular on TikTok.

Question 5



Why are deepfakes concerning?

1. They can spread false information and deceive people.
2. They are harmless pranks.
3. They are entertaining and should be shared widely.
4. They are created by professional filmmakers for movies.

Question 5



Why are deepfakes concerning?

1. They can spread false information and deceive people.

2. They are harmless pranks.

3. They are entertaining and should be shared widely.

4. They are created by professional filmmakers for movies.



Big data



Each time we go online, we are disclosing information about ourselves.

Every online activity contributes to sharing our personal data.





**How do you think companies
collect and use our data?
Why is it valuable for them?**

Consumer

A person who buys products or services.



Data

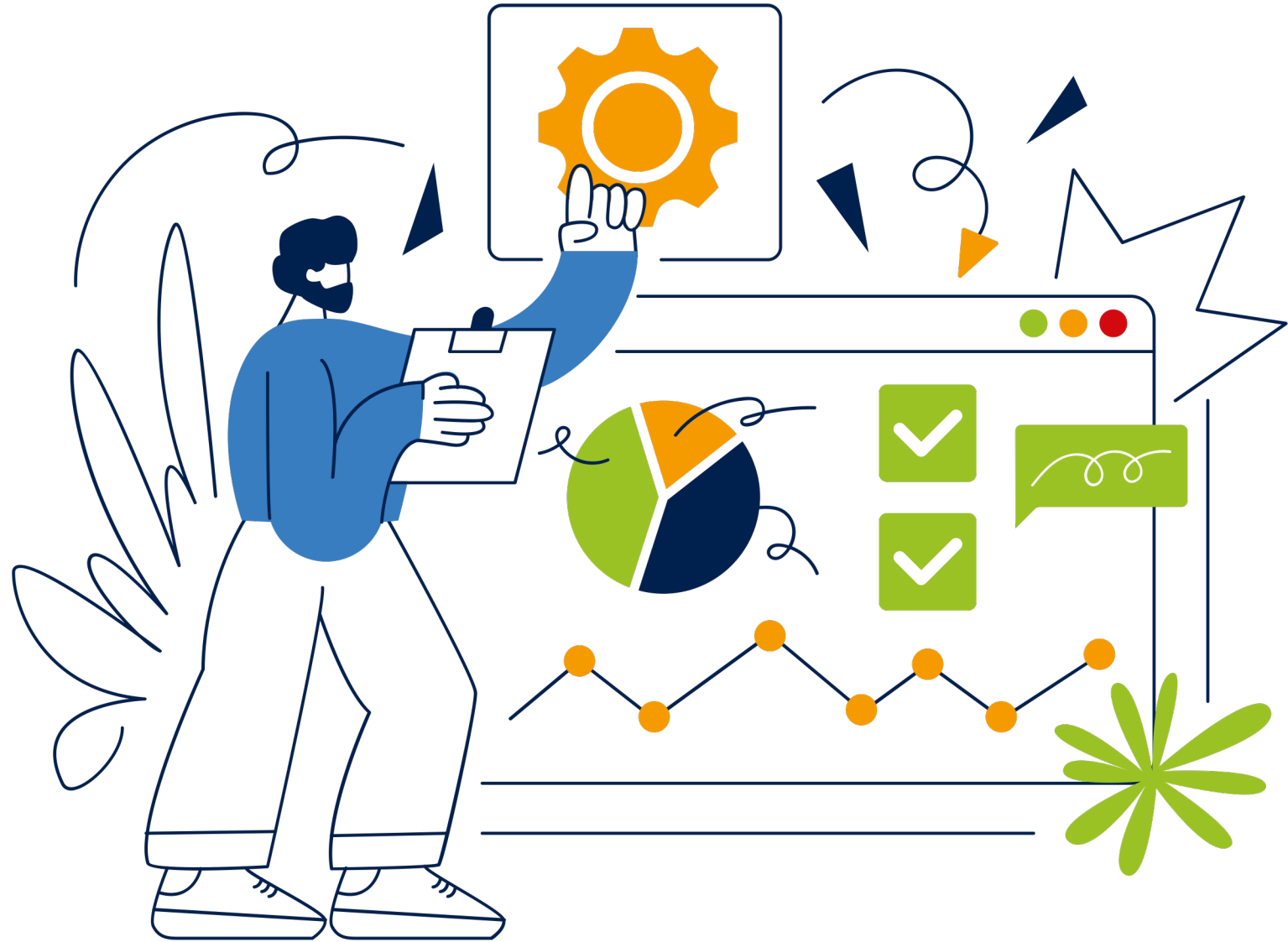
Facts and statistics collected together to be used for different purposes.

It can be numbers, words, pictures, or even sounds, and when companies put all the puzzle pieces together, they have a “portrait” of you and other consumers of their goods or services.



Big data

Extremely large data sets that are analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.



Targeted advertising



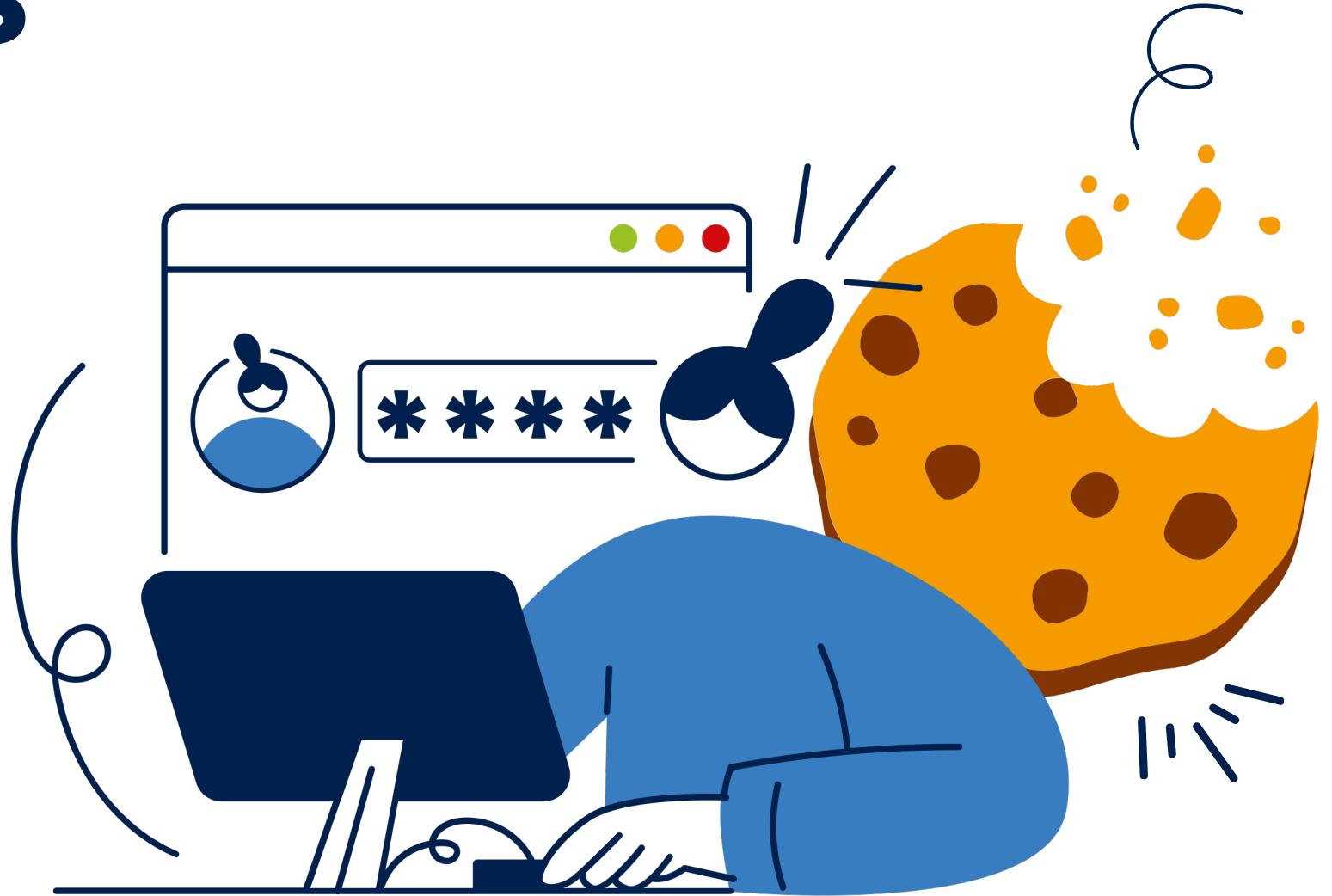
- Targeted advertising is when companies use information which they have about you to show you specific ads based on your interests and needs.
- In most cases the goal of targeted advertising is to sell you specific products or services which might be interesting to you.
- It can be both good and bad: some people find it nice to see items which are interesting for them, others find it manipulative as such ads incline people to spend more money or to watch more movies instead of doing chores, etc.



Cookies

Cookies are like tiny helpers that some websites use to remember things about you.

They are small pieces of information — like a username and password — that your computer or device saves when you visit a website.



What cookies are used for?



- Some cookies are used to improve your web browsing experience: they help the website remember your preferences, like your favorite games or music, so that the next time you visit, everything feels familiar and fun.
- Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.



How safe are cookies?

Cookies from trusted websites are safe. They don't know your name or personal information, or can't be used to download malicious software so you can explore the internet with a big smile! 😊



Why cookies can be dangerous

Since the data in cookies doesn't change, cookies themselves aren't harmful.

However, in some cases, cookies can be exploited by hackers or malicious actors to steal sensitive information, such as login credentials or credit card details, if the website does not have strong security measures in place.

Attackers can also inject malicious scripts into cookies, causing harm to your computer or device.



Hello, hello, hello

Who is B23A? Listen to a song called *Hello, hello, hello* and sing along.

[Watch the video](#)

We use both first and third-party cookies to personalise web content, analyse visits to our websites and tailor advertisements. Some of these cookies are necessary for the website to function, whilst others require your consent. More detail can be found in our cookie policy and you can tailor your choices in the preference centre.

[Accept All Cookies](#)

[Cookies Settings](#)

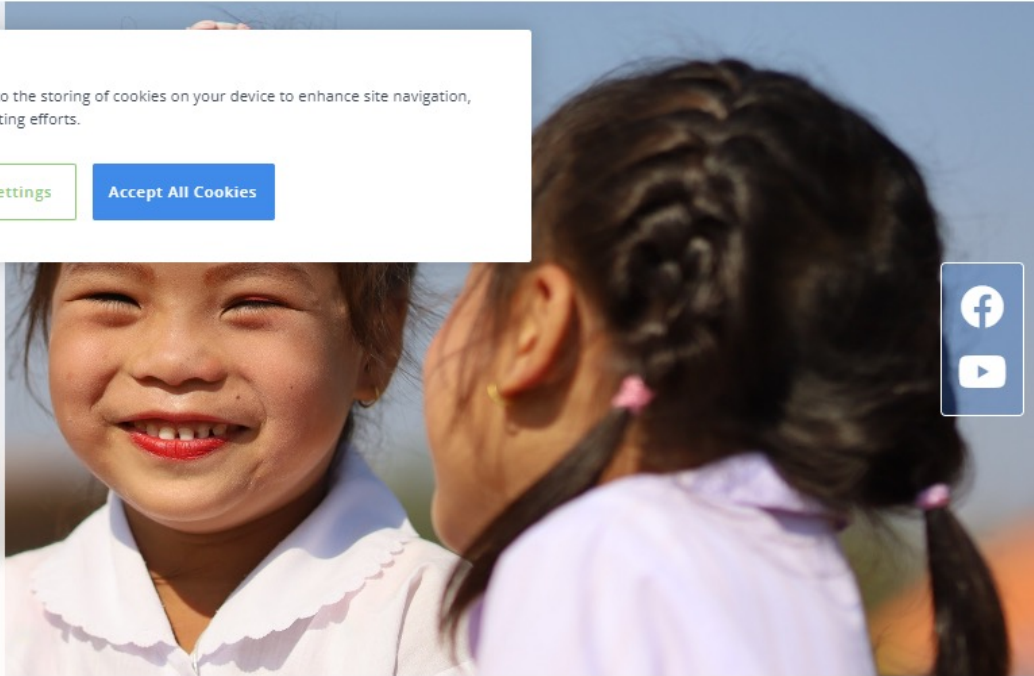
5 years of trans lives through education

Let's work together to create new knowledge, putting our diverse experiences and strengths towards a brighter future!

Partner with us

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

[Cookies Settings](#) [Accept All Cookies](#)



The Acronis Cyber Foundation Program is a corporate social responsibility project by IT company Acronis. To implement our philanthropic initiatives, we work with a vast network of non-profit organizations and government institutions. The dedication and hard work of like-minded Acronis employees, partners and friends makes the projects organizationally and financially possible.

Since the program's start in 2018, we have been strongly focused on education. We engaged in school construction (implemented in partnership with the [Groundbreaker](#)), IT skills training (in collaboration with [Yellow Ribbon Fund](#), [IMDA](#) and [Integres](#)) and other educational and humanitarian aid initiatives for children and adults.

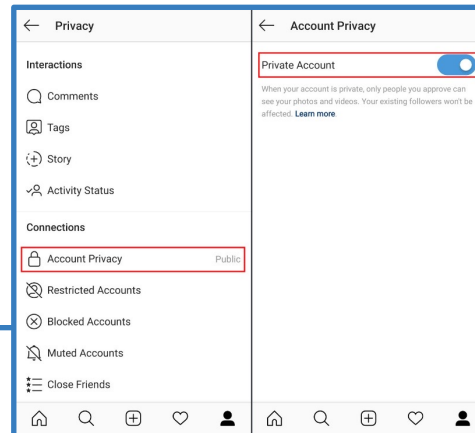
Limiting what is tracked about you

Turn off cookies

You can reject them when visiting a website for the first time or turn them off using your privacy settings.

Adjust privacy settings

Almost all apps let you change privacy settings to control what information they collect. You can keep your account private, and decide not to share your location or contacts with the app.



Limit what you share

Unless necessary, don't share your email address and telephone number with unknown websites or apps. If these are required, check the privacy policy to see how that information is being used.

Kahoot time!





Quiz time!

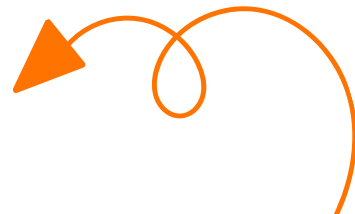


Question 1



Why do companies use targeted ads?

1. To show random ads to everyone.
2. To personalize ads based on what people like.
3. To make people bored.
4. To send secret messages



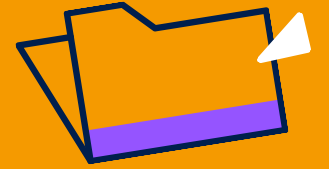
Question 1



Why do companies use targeted ads?

1. To show random ads to everyone.
- 2. To personalize ads based on what people like.**
3. To make people bored.
4. To send secret messages

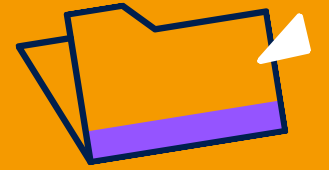
Question 2



What are cookies used for on the Internet?

1. Giving an opportunity to hackers to steal your information.
2. Tracking online activities and preferences.
3. Sending secret messages.
4. Letting your parents know when you are online.

Question 2



What are cookies used for on the Internet?

1. Giving an opportunity to hackers to steal your information.
- 2. Tracking online activities and preferences.**
3. Sending secret messages.
4. Letting your parents know when you are online.

Question 3



Which of these can Internet cookies not do?

1. Collect personal information about a user.
2. Contain a unique ID for a computer.
3. Store information from a Web server on a user's computer.
4. Remember the items you add to your cart when you leave the website.

Question 3



Which of these can Internet cookies not do?

1. Collect personal information about a user.

2. Contain a unique ID for a computer.

3. Store information from a Web server on a user's computer.

4. Remember the items you add to your cart when you leave the website.

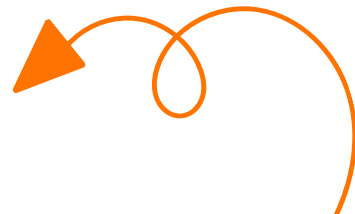
Question 4



Why is it essential to limit tracking of your online activities?



1. To keep your personal information safe.
2. Because cookies need a break sometimes.
3. To make the internet faster.
4. All of the above.



Question 4



Why is it essential to limit tracking of your online activities?

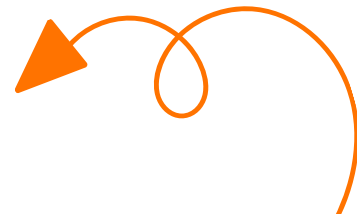


1. To keep your personal information safe.

2. Because cookies need a break sometimes.

3. To make the internet faster.

4. All of the above.



Question 5



 What happens if you make your account private on social media?

1. You'll have to pay for every time you login into your account.
2. Only your approved friends can see your posts and pictures.
3. Your account disappears from the Internet.
4. You can't use social media anymore.

Question 5



What happens if you make your account private on social media?

1. You'll have to pay for every time you login into your account.
2. **Only your approved friends can see your posts and pictures.**
3. Your account disappears from the Internet.
4. You can't use social media anymore.



Digital footprints



Digital footprints

A record of what you do online, including the sites you visit and the things you post.

Includes all parts of your online activity that you both knowingly and unknowingly leave behind.



Active footprints



- Posting or commenting on social media
- Sending an e-mail or instant message
- Video calling a friend
- Accepting cookies

While this allows you to receive more accurate advertisements, it is also a privacy concern as this data could potentially be leaked. This could reveal your data to other parties who may use it to target you in scams.

Passive footprints



- Using a search engine
- Online shopping
- Enabling location services
- Using password saving services

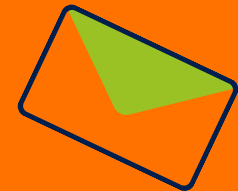
These processes all collect information about the user, often without them even knowing.



How can our digital footprints shape our future?



**Who could be in the invisible audience
that looks for information about you
or what you posted online?**



Possible invisible audience

- Old friends and teachers
- Colleges or schools you apply to
- Possible employers
- Scholarship committees
- Leaders of groups or organizations you want to join
- Etc.

**Your digital footprints
shape your future, your
reputation and
opportunities.**



Responsibility to yourself and others

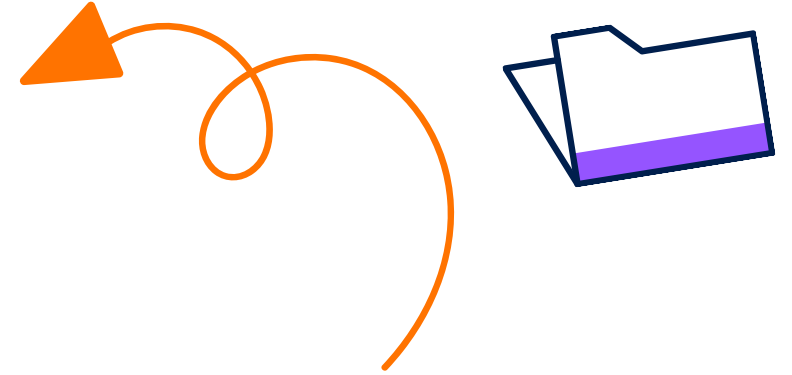
Your comments and shares can also influence your friends' reputations.

And vice versa.

Always ask your friend if you can post his / her photo online and always think whether your comments shared in public about your friends won't harm them.



Case study



A university in Bucharest, Romania, is seeking students to participate in an environmental conference in Geneva, Switzerland. The trip will span 5 days, featuring not only strategic sessions but also ample opportunities for sightseeing and entertainment.

There are more than 8,000 people studying at the university, but only 5 can represent Romania at the conference. The selection process involves an evaluation of applicants' academic performance, their engagement in university activities, and their involvement in volunteer work outside of the academic sphere. Additionally, students are required to submit a motivational letter explaining their reasons for wanting to attend.



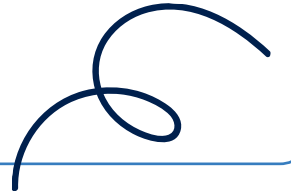
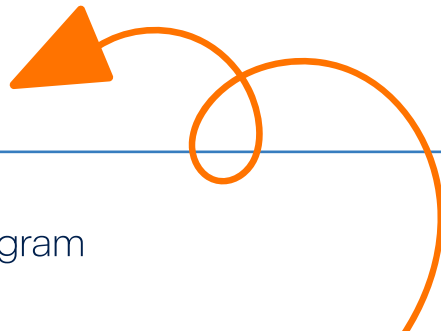
Study the motivational letter submitted by Anna Adams:



Dear Conference Selection Committee,

I am writing to express my deep enthusiasm and commitment to representing our university at the upcoming environmental conference in Geneva, Switzerland. As an ardent eco-activist in our community, I have dedicated myself to initiatives aimed at fostering a greener, more sustainable environment. Over the years, I have actively participated in tree-planting drives, where we have successfully added many vibrant, oxygen-producing companions to our city's landscape. Additionally, I have taken part in numerous clean-up campaigns in and around Bucharest, working relentlessly to maintain the pristine beauty of our natural surroundings. My passion for environmental conservation and my desire to learn and collaborate with like-minded individuals on a global scale drive me to seek this invaluable opportunity. I genuinely believe that my experiences and unwavering commitment make me a fitting representative of our university at this prestigious conference. Thank you for considering my application, and I eagerly anticipate the chance to contribute to the discourse on sustainable living and eco-consciousness.

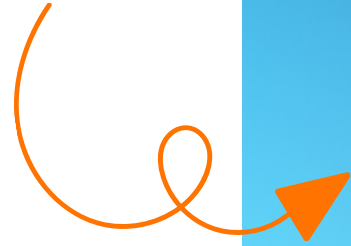
Sincerely,
Anna Adams



What committee saw at Anna's Instagram account: these two photos of Anna planting trees published 1 day ago.



The committee also saw videos of Anna and her friends having a party letting dozens of balloons into the sky, happily smiling and clapping.



Customer feedback made by Anna on a shopping site

Customer feedback

Anna Adams

July 14



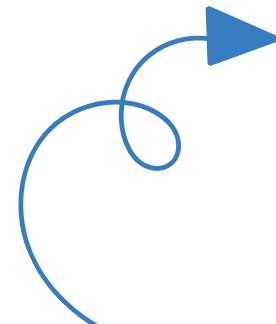
This shovel is great! Light, small, convenient, perfect for a newbie in planting like me :)

In your opinion, what would be the decision of the university committee regarding Anna and why?

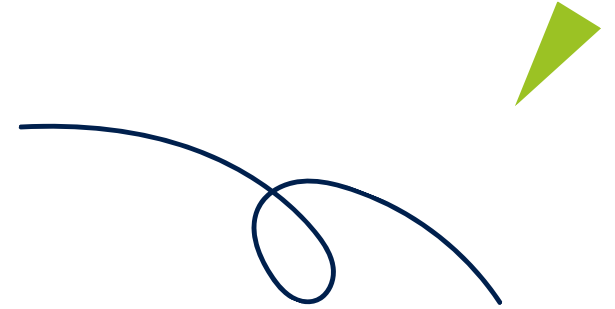
How can I manage my digital footprints?



- 1. Look yourself up online.** Search your name on a reputable search engine (i.e. “John Doe”) and take note of website domains that appear. If you find any inaccurate or bad information about you, consider contacting the company running the search engine, and requesting they remove the links related to you. Turn on Google alerts for your name so you are notified if something about you pops up online.
- 2. Avoid posting personal information** on social media, especially, on a public account, like your home or mobile number, credit card information, full name, birth date, school name, and other personal details that identity thieves can easily take advantage of.
- 3. Change your accounts to private.**



How can I manage my digital footprints?



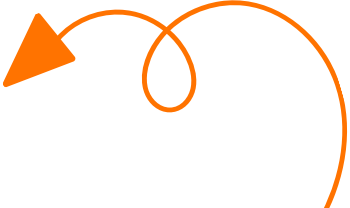


- 4. Set privacy settings** like who can see your photos, who can add you as a friend, who can tag you, etc. on social media.
- 5. Deactivate your old and inactive accounts.**
- 6. Keep things professional.** Make sure what you say or share is factual and is something that you would not mind a future employer or admissions officer reading.
- 7. Delete unflattering content.** Go through all your social media posts and delete content that you find questionable or unflattering.
- 8. Check your browser for cookies** from sites you haven't visited. Block third-party cookies.
- 9. Never share your password** with anyone else.



Worst-case scenario: delete your digital footprints



If you suffer from negative information published about you online, you can partially wipe out your existence from the Internet:

1. Delete social media accounts;
 2. Delete forum comments and blog posts;
 3. Delete email accounts.
- 
- 
- 

Kahoot time!





Quiz time!

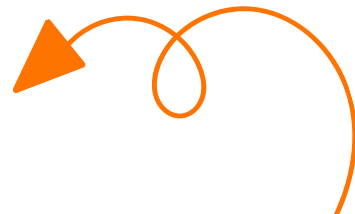


Question 1



Digital footprints are:

1. Invisible and can't be tracked.
2. Evidence of what you do online, including the things you post.
3. Not permanent and go away after you log off the internet.
4. Erased if you delete an email, a text, or a post.



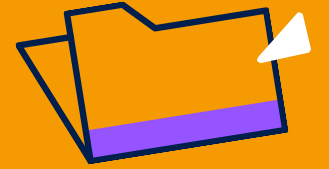
Question 1



Digital footprints are:

1. Invisible and can't be tracked.
- 2. Evidence of what you do online, including the things you post.**
3. Not permanent and go away after you log off the internet.
4. Erased if you delete an email, a text, or a post.

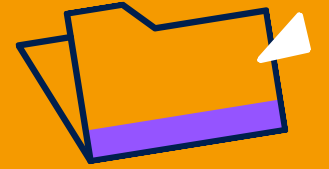
Question 2



Which of these practices can help manage your digital footprint?

1. Avoid updating your software.
2. Avoid sharing negative comments on social media.
3. Stop others from sharing negative comments on social media.
4. All of the above.

Question 2



Which of these practices can help manage your digital footprint?



1. Avoid updating your software.
- 2. Avoid sharing negative comments on social media.**
3. Stop others from sharing negative comments on social media.
4. All of the above.

Question 3



You see a social media post that does not align with your views. Do you _____?

1. Avoid commenting, and instead have a discussion with friends or family about the topic.
2. Mock the poster for having a wrong opinion by leaving a negative comment.
3. Report the post to the website/app administration.
4. All answers are correct.

Question 3



You see a social media post that does not align with your views. Do you _____?

1. Avoid commenting, and instead have a discussion with friends or family about the topic.

2. Mock the poster for having a wrong opinion by leaving a negative comment.

3. Report the post to the website/app administration.

4. All answers are correct.

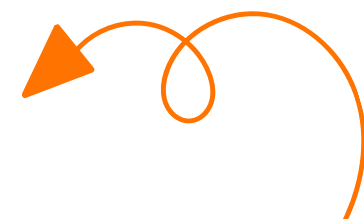
Question 4



Last week Avi went on a field trip to a museum with her classmates. Tal, one of Avi's friends, posted a picture showing Avi making a silly face. Avi didn't like the picture and was upset Tal posted it. What should Tal have done in this situation?



1. Not gone on the field trip.
2. Not brought his phone on the field trip.
3. Asked for permission before posting the picture online.
4. Posted the picture anyway since it was from his camera.



Question 4

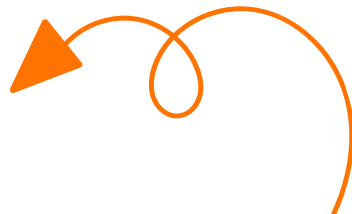


Last week Avi went on a field trip to a museum with her classmates. Tal, one of Avi's friends, posted a picture showing Avi making a silly face. Avi didn't like the picture and was upset Tal posted it. What should Tal have done in this situation?

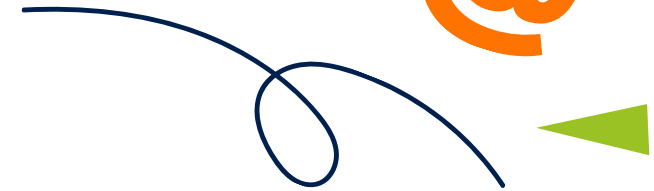
1. Not gone on the field trip.
2. Not brought his phone on the field trip.

3. Asked for permission before posting the picture online.

4. Posted the picture anyway since it was from his camera.



Let's recap



- **Don't trust anything you see online.** Before believing something, check if it fake or real by asking yourself: Does this information come from a credible, unbiased source? Do other credible sources say the same thing? What evidence is provided?
- **All of the websites and apps collect information about you** both to improve your browsing experience and to show you targeted ads to get financial gain. Also, when hacked, cookies can be stolen and all your browsing history and personal information will be in hands of criminals. If you decide to avoid such digital risks, limit your online tracking: turn off cookies, adjust privacy settings in all apps (make your account private, restrict who can send you messages, etc.) and don't share your personal information online unless necessary.
- **All your actions online leave digital footprints.** They can influence your future, so be careful about what you do and post online.
- **Digital footprints can be partially removed** if you delete your posts, comments, accounts, etc. but there is a chance someone has made a screenshot of them. Moreover, they still be stored in internet achieves.
- **We are responsible for not defaming not only ourselves, but our friends and relatives:** before posting something online about other persons, ask for their permission.





Cyberbullying

Does anyone of you have a nickname, either positive or negative? What is it?





Cyberbullying is using digital devices, sites, and apps to intimidate, harm, and upset someone.

Why do you think it might happen?

Cyberbullying



Reasons why cyberbullying occurs

- Someone acts or looks differently than others
- Someone is angry or resentful towards another person
- Someone is jealous of another person
- Someone feels bad because he or she has been bullied

Ways to respond if you are cyberbullied

- Ignore the messages
- Block the bully
- Use reporting tools
- Take a screenshot of messages
- Tell a trusted adult (parent, teachers, etc.)

Ways to be an upstander

- Reach out to the target to see how he or she is feeling and listen to him/her
- Inform a teacher, a coach, a parent, or another trusted adult
- Encourage the target to not respond or retaliate
- Encourage the target to reach out to a trusted adult

Remember:

The best way to react to a bully's messages is to ignore them.

When bullying a person, a bully is awaiting for your reaction or emotions (making you scared, sad, worried).

By ignoring a bully you don't give him/her what they want.

If you see cyberbullying happening, be an upstander: help the target to feel better and tell a trusted adult about what's happened.



Empathy

When you put yourself in someone else's shoes and imagine what they are feeling and might be going through.

When you show empathy, you are being kind and caring towards others, making the world a better place!



Kahoot time!





Quiz time!

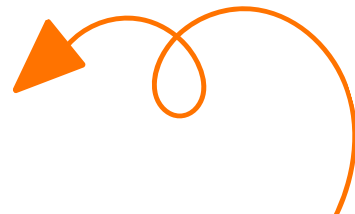


Question 1



Empathy is ...

1. Having the same feelings as your friends.
2. Being in love with someone.
3. Understanding how someone else is feeling and being kind and caring towards them.
4. None of the above.



Question 1



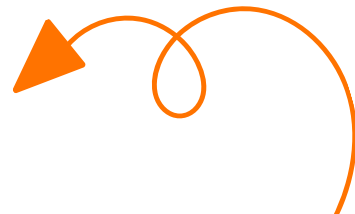
Empathy is ...

1. Having the same feelings as your friends.

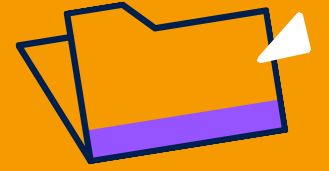
2. Being in love with someone.

3. Understanding how someone else is feeling and being kind and caring towards them.

4. None of the above.



Question 2

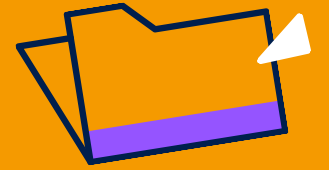


Which of the below does not describe an upstander?



1. Tells a trusted adult about a happening embarrassing situation.
2. Tries to stop bullying when it is happening.
3. Uses digital media tools to respond to a bully and offend him/her in return.
4. Empathizes with someone who is being bullied.

Question 2



Which of the below does not describe an upstander?




1. Tells a trusted adult about a happening embarrassing situation.
2. Tries to stop bullying when it is happening.



3. Uses digital media tools to respond to a bully and offend him/her in

4. Empathizes with someone who is being bullied.

Question 3



Tori takes a picture of Asha making a goofy face and posts it online. She leaves the comment, “Asha, you look so silly!” Asha should respond by:

1. Posting a comment saying she is not friends with Tori any more.
 2. Pretending she doesn't care and telling Tori she thinks it's funny.
 3. Telling Tori to ask first before posting photos of her.
- 

Question 3



Tori takes a picture of Asha making a goofy face and posts it online. She leaves the comment, “Asha, you look so silly!” Asha should respond by:

1. Posting a comment saying she is not friends with Tori any more.
2. Pretending she doesn't care and telling Tori she thinks it's funny.

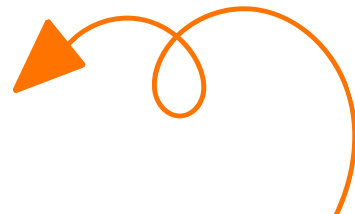
3. Telling Tori to ask first before posting photos of her.

Question 4



You get a link to a website. When you go to the website, you are asked to rate the kids in your class based on how cute and smart they are. You should:

1. Log off, figure out who created the site, and ask them to take it down.
2. Shut down your computer immediately.
3. Rate them. You're anonymous so they'll never know it was you.



Question 4



You get a link to a website. When you go to the website, you are asked to rate the kids in your class based on how cute and smart they are. You should:

1. Log off, figure out who created the site, and ask them to take it down.

2. Shut down your computer immediately.

3. Rate them. You're anonymous so they'll never know it was you.

Question 5



Annali likes to post her videos online, but recently people have been posting mean comment about them. What should she do:

1. Block the people making the negative comments.
2. Take down her videos.
3. Respond to the comments, telling them that they're wrong.

Question 5



Annali likes to post her videos online, but recently people have been posting mean comment about them. What should she do:



1. Block the people making the negative comments.

2. Take down her videos.

3. Respond to the comments, telling them that they're wrong.

Question 6



Sofie says to Nita, “Why did you post that I was a loser on my page?”. Nita never posted anything on Sofie’s page and guesses that someone else has been logging in as her. After talking to Sophie, what should Nita do?

1. Do nothing. It’s not Nita’s fault that it happened.
2. Change the password, and then delete the mean comments.
3. Delete the mean comments and hope that it doesn’t happen again.

Question 6



Sofie says to Nita, “Why did you post that I was a loser on my page?”. Nita never posted anything on Sofie’s page and guesses that someone else has been logging in as her. After talking to Sophie, what should Nita do?

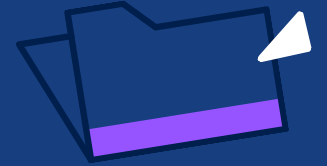
1. Do nothing. It’s not Nita’s fault that it happened.

2. Change the password, and then delete the mean comments.



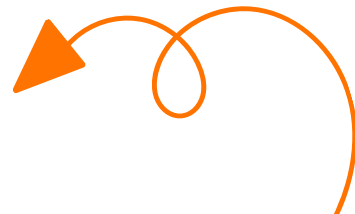
3. Delete the mean comments and hope that it doesn’t happen again.

Question 7

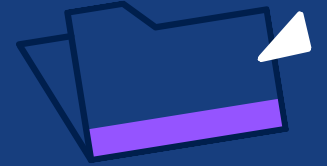


Someone has logged into your online profile and is posting mean things about your friends. You've tried to get back in to take down the mean things, but your password has been changed. What should you do?

1. Let your parents know and contact the people running the online site.
2. Post a comment saying you'll find who wrote the comments and you'll get back them.
3. Tell your friends that you're sorry, but there's nothing you can do.



Question 7



Someone has logged into your online profile and is posting mean things about your friends. You've tried to get back in to take down the mean things, but your password has been changed. What should you do?

1. Let your parents know and contact the people running the online site.

2. Post a comment saying you'll find who wrote the comments and you'll get back them.

3. Tell your friends that you're sorry, but there's nothing you can do.



Copyright

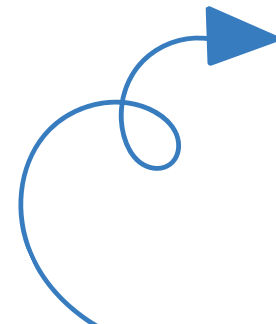


Imagine a situation



You and your friends attended a course on creation of animated videos for three months. You've spent all your free time and weekends studying hard. As a final project, together you created a cool video and shared it with your classmates in a group chat on a messenger. In a couple of weeks you found this video published on Youtube by some unknown person. The video has lots of likes, positive comments and the publisher receives money for the big number of views. There is no mention of your name or your friends' names.

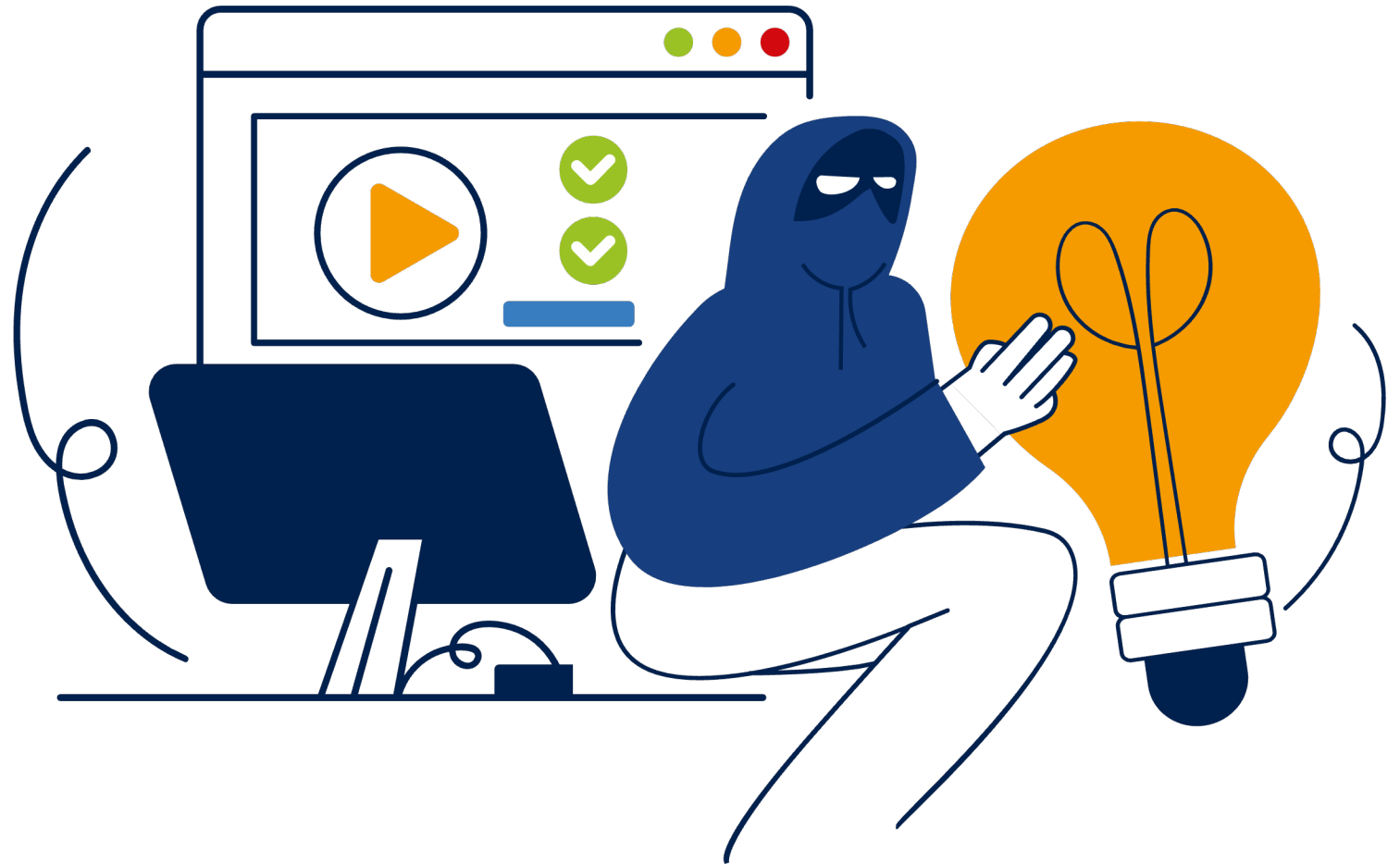
How would you feel if something you worked so hard to create was being shared by others without giving you credit for it?



Plagiarism

In virtual life as in real one the same rules and regulations are applied to people. One is not allowed to take property of other people, including virtual one such as photos, videos, documents, manuscripts, and other pieces of artwork or other **intellectual property**.

Taking someone else's work or ideas and passing them off as one's own is called **plagiarism**.



Copyright



It is both unfair and illegal to use other people's intellectual property without permission or citing them.

There are laws in every country that protect creative works and for violating them **people can get fined and put into prison.**

Copyright

Copyright is legal protection that creators have over the things they create.

Copyright is like a special superhero cape that protects someone's original work, like a story, a drawing, or a song. It means that no one else can use or copy their work without their permission. Just like how you wouldn't take someone's toys without asking, you shouldn't use someone's creative work without their permission!

When we create something, it's automatically ours. We have protections in place (copyright) to make sure others don't use our work and say it's theirs.



What types of content does copyright protect?



Photographs



Artistic works



Literary works



Films



Musical works



Broadcasts

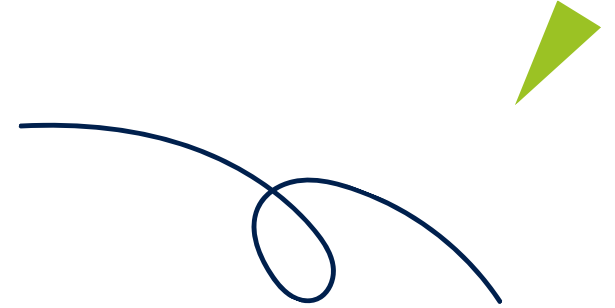


Architecture



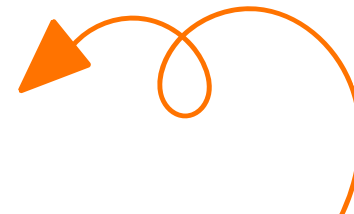
Computer software

Borrowing content for educational purposes



A person **can borrow someone's work** without necessity to obtain a special right for it if he/she uses it **for educational purposes**. For example, a student can take a picture from the internet and use it in his/her paper, slides, or whatever other type of document is being created and give credits to the source of this picture. It presupposes only illustrating the student's idea with the created work not being sold or copied and distributed.

Educational purposes **do not include** cases like when a person wants to create his/her own educational course and teach it publicly, even for free. It forbids any form of distributing the copyrighted material.



Public domain



Creative work that's not copyrighted and free to use without permission. Such works are either made for public to use for free or they are very old and their copyright has expired.



Fair use



The ability to use copyrighted work without permission, but only in certain ways and specific situations.

Four factors of fair use



Amount

only a small part of the original work is used, or the most important part ("heart") is not included.

Purpose

the new work is for educational purposes or changes the original work into something very different.

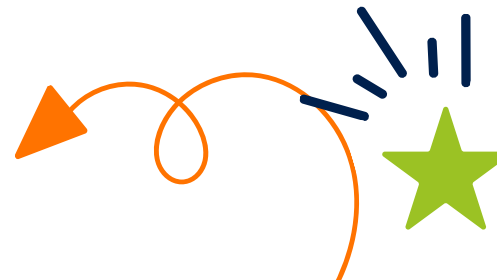
Nature

the original work is nonfiction or based on facts, not creative or fictional.

Effect

the new work doesn't harm the creator or the value of the original work.

**Remember to give credits to the author or source when reusing someone else's content.
And make sure to put your name on the works which you've created.**



Common examples of fair use



**Schoolwork
and education**



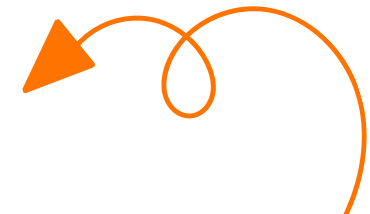
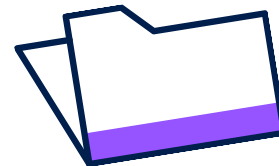
**Criticizing or
commenting**



News reporting



Comedy



Is it fair use? Example 1.

Anna is an owner of a small flower shop. She is making a digital flyer to post it on her Instagram account to promote her shop.

She found a beautiful logo of another flower shop online and used part of it in her flyer.



Is it fair use? Example 2.

As part of their school project, a group of students are making a video about gambling.

They use the song "Poker face" by Lady Gaga in the background.



Is it fair use?

Example 3.

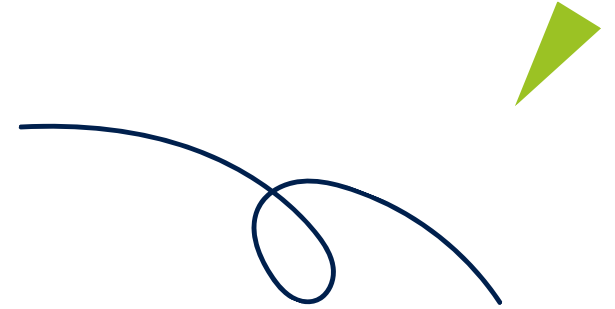
Alex is doing a presentation on climate change for his school project.

As part of the presentation, Alex includes a short clip from a documentary about the effects of climate change on polar bears.

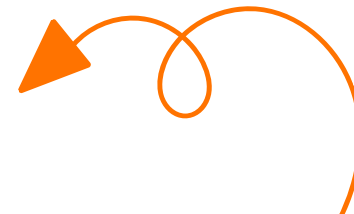
The clip is used to support the information in the presentation and educate the audience about the impact of climate change on wildlife.



What to do not to violate copyright?



- 1. Always assume that the work is copyrighted.** Do not assume that because a work is freely downloadable then it is free to use.
- 2. Do not copy, share or alter without seeking permission.** Identify the author, seek for his/her written permission, agree about the terms of usage.
- 3. Use public domains:** works with expired copyright like classic literary works as Shakespeare's plays, Mark Twain's novels, and Jane Austen's books, ancient artwork, vintage photographs, etc; government works and publications; folklore like folktales and myths; facts and ideas; works with waived copyright.
- 4. Give proper attribution.**



Kahoot time!





Quiz time!

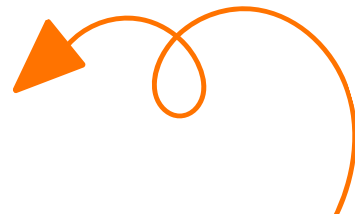


Question 1



What does “copyright” mean?

1. Legal protection that a creator has over the things they create.
2. Creative work that can be used by anyone.
3. Using someone's creative work without giving credit.
4. Giving credit to the person who created something.



Question 1



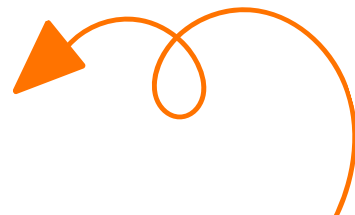
What does “copyright” mean?

1. Legal protection that a creator has over the things they create.

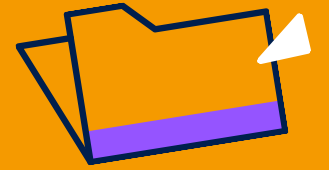
2. Creative work that can be used by anyone.

3. Using someone's creative work without giving credit.

4. Giving credit to the person who created something.



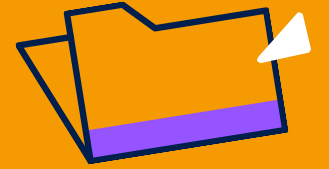
Question 2



What types of work are copyrighted?

1. Literary
2. Facts
3. Ideas
4. Dramatic
5. Musical
6. Artistic
7. Speeches

Question 2



What types of work are copyrighted?



1. Literary

2. Facts

3. Ideas

4. Dramatic

5. Musical

6. Artistic

7. Speeches



Question 3



When does someone's work start being copyright protected?

1. Once the author receives monetary compensation for the work.
2. When it is published with a copyright symbol ©.
3. As soon as the work is created.
4. Once it is registered for copyright by a special authority.

Question 3



When does someone's work start being copyright protected?

1. Once the author receives monetary compensation for the work.
2. When it is published with a copyright symbol ©.

3. As soon as the work is created.

4. Once it is registered for copyright by a special authority.

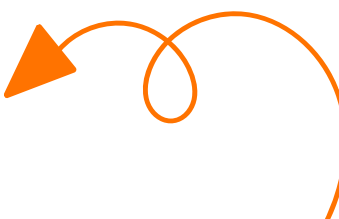
Question 4



It is not considered as a copyright violation when a student lends a book to his friend, right?



1. True, he bought the book and now can use it the way he likes.
2. True, because the student is sharing the book with a friend for personal use, which is allowed.
3. True, as long as the friend promises to return the book after reading it.
4. False, every bought copy of a book, CD, movie or other type of intellectual property is not meant for distribution unless otherwise stated in its terms and conditions.



Question 4



It is not considered as a copyright violation when a student lends a book to his friend, right?

1. True, he bought the book and now can use it the way he likes.
2. True, because the student is sharing the book with a friend for personal use, which is allowed.
3. True, as long as the friend promises to return the book after reading it.

4. False, every bought copy of a book, CD, movie or other type of intellectual property is not meant for distribution unless otherwise stated in its terms and conditions.

Question 5



A student writes a paper for a class in which she uses images from the internet. She credits the source. The student submits her paper for a competition and wins a prize for the school. Is it considered a fair use?

1. Yes, the source of images is cited, the work is not used for commercial purposes.
2. No, the work has been passed to a third party (competition organizers).

Question 5



A student writes a paper for a class in which she uses images from the internet. She credits the source. The student submits her paper for a competition and wins a prize for the school. Is it considered a fair use?

1. Yes, the source of images is cited, the work is not used for commercial purposes.

2. No, the work has been passed to a third party (competition organizers).

Question 6



Which of the following situations is least likely to be fair use?

1. A teacher using a photograph in a presentation to his class.
2. A journalist using a video clip in a news story.
3. A late-night comedian using a photo as part of a political joke.
4. A sports fan using a team logo to make his own souvenirs to sell.

Question 6



Which of the following situations is least likely to be fair use?

1. A teacher using a photograph in a presentation to his class.
2. A journalist using a video clip in a news story.
3. A late-night comedian using a photo as part of a political joke.
- 4. A sports fan using a team logo to make his own souvenirs to sell.**

Let's recap



- **There is a lot of hatred and cyberbullying in the internet.** Never respond to it, block the bully and tell a trusted adult. Don't forget to take a screenshot of offensive messages to have a proof.
- **Be an upstander:** if you see that someone is bullied, support the person and ask a trusted adult for help.
- **Don't borrow intellectual property of other people** without their permission. Use copyrighted work without permission only applying four factors of fair use.
- **Use public domains for taking free content** and always give proper attribution to content owners.



Acronis

Cyber Foundation Program

#CyberFit

foundation@acronis.org

acronis.org

Level 2

