

Acronis

Cyber Foundation
Program

#CyberFit

Cyber safety basics

Level 1



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.



Trusted sources of information

In your opinion, how would you
recognize **untrustworthy**
online resources?

Trustworthy apps and games

- Always download games or apps only from Play Market (for Android phones) or AppStore (for iPhones).
- If you want to download something (a game, a book, a movie, a video, etc.) from a website, ask your parents if it is trustworthy. Otherwise you might download a virus and harm your computer, tablet or phone.



Trustworthy links

Check that links which you open have a closed padlock sign in front of the website address. A secure website has “https” rather than “http” before its name. The “s” at the end of “http” stands for “secure”.

 <https://website.com> 

 <http://website.com> 



Unsafe website example



The screenshot shows a red warning banner with a white exclamation mark icon on the left. The text reads: "Deceptive site ahead". Below this, it states: "Attackers on **your-site.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). [Learn more](#)". There is a checkbox option: " Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. [Privacy policy](#).". At the bottom left is a "Details" button, and at the bottom right is a "Back to safety" button.



Don't trust strangers

- Never download any files or click any links sent to you by unknown people.
- If unknown people promise you a prize or something else cool, it is most likely to be a scammer who harm your device or steal personal data from it. Nothing is free.



Never share your personal data online

- Don't share name, surname, address, date of birth, passwords, bank card details of yourself and your parents or friends with anyone.
- In case an app or a website asks for such data, for example, when you are setting an account on them, check with your parents if it is safe.



Kahoot time!

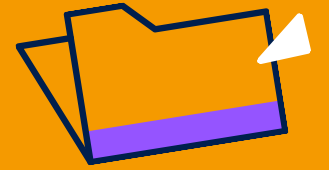




Quiz time!



Question 1

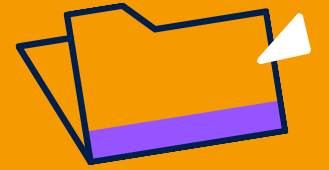


Which of the following is a good practice to determine if a website is trustworthy?



1. Checking if there is a closed padlock before the website's name and if its name is spelt properly.
2. Looking for spelling and grammar errors on the website.
3. Believing everything you read without questioning.
4. Choosing the source that has the most exciting and eye-catching design.

Question 1



Which of the following is a good practice to determine if a website is trustworthy?



1. Checking if there is a closed padlock before the website's name and if its name is spelt properly.

2. Looking for spelling and grammar errors on the website.

3. Believing everything you read without questioning.

4. Choosing the source that has the most exciting and eye-catching design.

Question 2



You've gone on a gaming website and it asks you to download a link before you play. What should you do?

1. Download it anyway.
2. Don't download it, it must be illegal.
3. Ask your friends what to do.
4. Show the link to an adult and ask them if it's safe.

Question 2



You've gone on a gaming website and it asks you to download a link before you play. What should you do?

1. Download it anyway.
2. Don't download it, it must be illegal.
3. Ask your friends what to do.



4. Show the link to an adult and ask them if it's safe.

Question 3



You are playing a computer game Fortnite when suddenly an advertisement for «Free Fortnite skins» pops up! Cool!!! All you have to do is enter your parents credit card number, but it won't cost anything. What do you do, and why?

1. Click on it, it's free, what's the harm?
2. Ignore it, it is a spam message that will steal money from your parents bank account.
3. Ignore it, skins are never really free.
4. It looks safe, click on it and then ask your parents for the information.

Question 3

You are playing a computer game Fortnite when suddenly an advertisement for «Free Fortnite skins» pops up! Cool!!! All you have to do is enter your parents credit card number, but it won't cost anything. What do you do, and why?

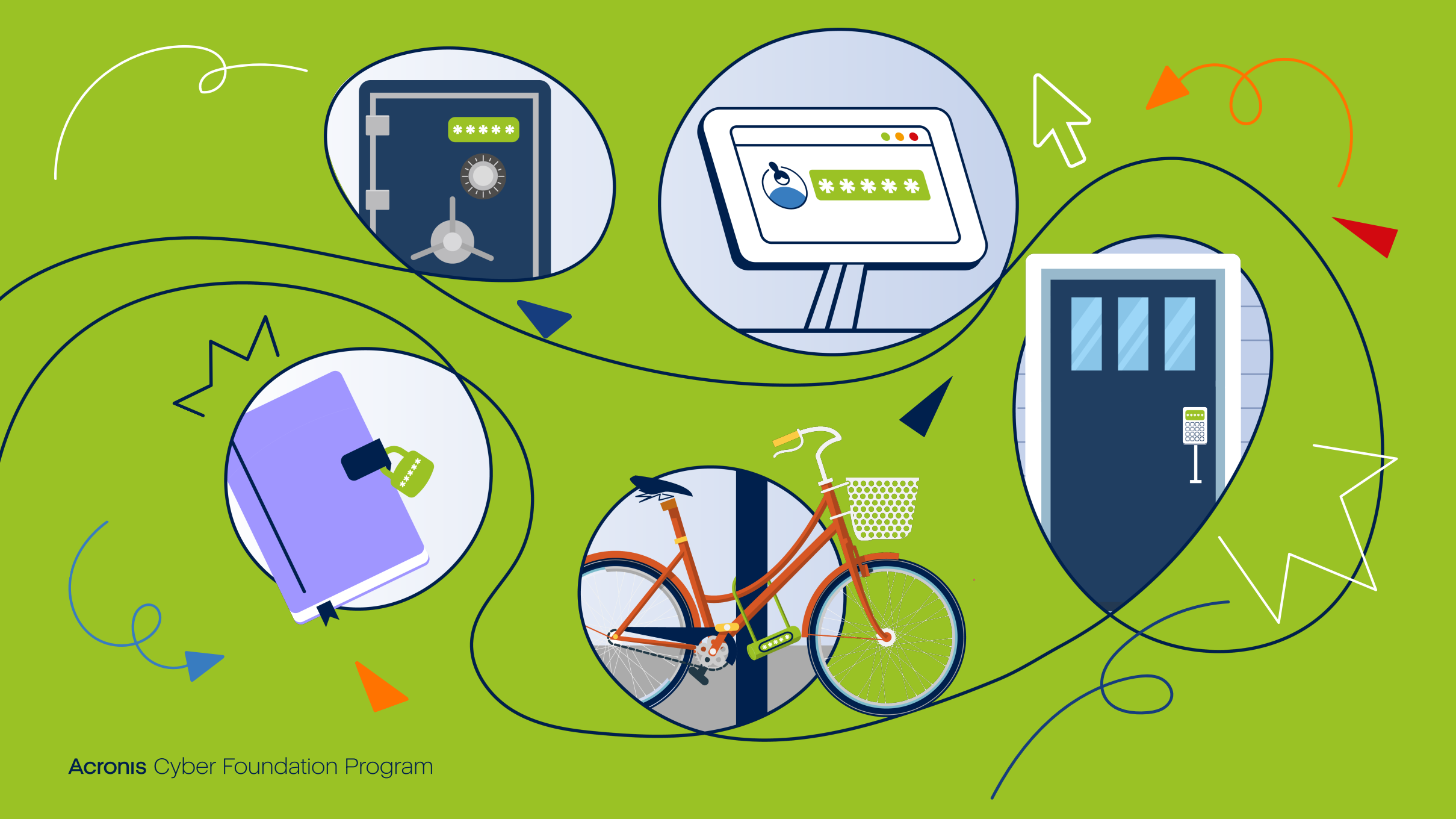
1. Click on it, it's free, what's the harm?

2. Ignore it, it is a spam message that will steal money from your parents bank account

3. Ignore it, skins are never really free

4. It looks safe, click on it and then ask your parents for the information.

Creating a strong password



Let's think about when we use devices, like a phone or computer, how do you limit who can access something that you want to protect, and why would you limit access?



A password

is a secret string of letters, symbols, and numbers that you can use to restrict who can access something digital. Some passwords, however, are stronger than others because they are harder for someone to figure out.



How to create a **strong** password?

- **It should not be easy to guess:** never use your name, surname, date of birth, telephone number, mother's name or any other information which others may know about you for creating a password. I.e. if all your classmates know you adore dogs, never use a password like "Ilovedogs".
- **Never use simple words or numbers:** 123456, password, Minecraft, etc.



How to create and remember a **strong** password?

A password must be 8 characters long at least (but better 14). The longer your password is, the safer it is.

If you find it difficult to remember a password with different types of characters, use a passphrase:

- MinecraftIsCool246\$
- WhoRulesTheWorld?5

Or take out the first letters of each word from your phrase and add number and special symbols to create a password:

- McKdIW!23 (My cat Kitty doesn't like Whiskas ! 23)
- P&Mm@8ntc (Paul and Mary meet at 8 near the cinema)

Choose a passphrase/password that is hard to guess.



Some people think that safe passwords should contain different types of characters:

- **Capital letters** – e.g. AZ
- **Lowercase letters** – e.g. az
- **Numbers/digits** – e.g. 0-9
- **Other characters**, including punctuation marks and special symbols – e.g. !@#\$%^&*()_+|~=\`{}[]:;'<>?,,



BUT cyber criminals use such computer programs which “guess” passwords. They iterate over options of passwords (combinations of all symbols) until they guess the right one. The longer your password is, the more difficult it is to guess your password.

Password manager

A password manager is a software application which acts as a digital vault where users can store their login credentials, such as usernames and passwords, for websites, apps, and other online platforms.

Its main purpose is to improve online security by generating strong, unique passwords for each account and storing them in an encrypted database. Instead of trying to remember multiple passwords, users only need to remember one master password to access the password manager.

They are absolutely legitimate and must be downloaded from AppStore or Google Play.



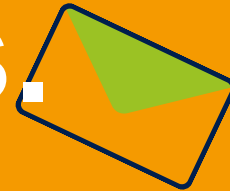
Other things to remember

- Don't write your passwords on paper, notebooks, your computer desktop documents or any other place where someone else can find them. Instead, use password managers, it is safer and more convenient.
- Change your passwords every 12 months. Don't re-use old passwords.
- Use different passwords for different accounts. If criminals steal your password from one account, they won't be able to apply it to other your accounts if you have different passwords everywhere.
- Passwords are secret and should never be told to anyone except for your parents. Even to close friends. Imagine, you have a quarrel with your friend, and he/she decides to make a joke on you...
- Don't enter your passwords when other people can see it.
- If you suspect that someone might know your password, change it immediately!





Now let's try to create a few strong passwords.



Kahoot time!

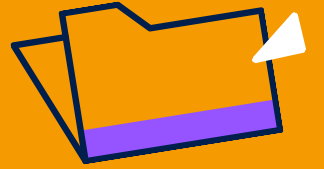




Quiz time!



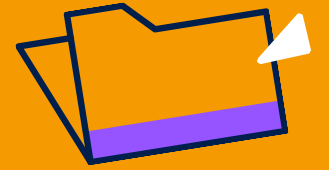
Question 1



Complete the sentence. When you create a new password for an account, you should never _____.

1. Tell your parents what your password is.
2. Use at least eight characters.
3. Start with a memorable phrase.
4. Use private information like your name, phone number, or address.

Question 1



Complete the sentence. When you create a new password for an account, you should never _____.

1. Tell your parents what your password is.
2. Use at least eight characters.
3. Start with a memorable phrase.

4. Use private information like your name, phone number, or address.


Question 2



If a friend asked you for a tip about how to create a strong password, what would you tell them?

1. Use your name.
2. Make it short.
3. Share it with a friend.
4. Make it as long as possible but not longer than 64 symbols.

Question 2



If a friend asked you for a tip about how to create a strong password, what would you tell them?

1. Use your name.

2. Make it short.

3. Share it with a friend.

4. Make it as long as possible but not longer than 64 symbols.

Question 3



Which of the below is a good password?

1. Password

2. 12345678

3. angela111909

4. lh2pacaad
(I have 2 pets a cat and a dog)

Question 3



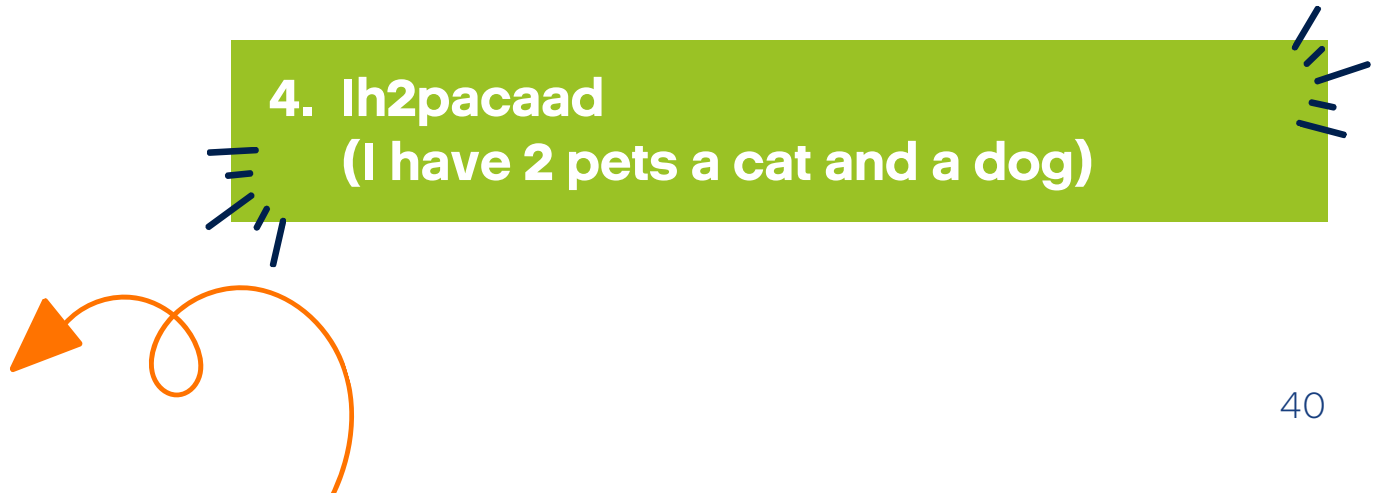
Which of the below is a good password?

1. Password

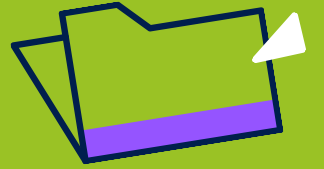
2. 12345678

3. angela111909

**4. lh2pacaad
(I have 2 pets a cat and a dog)**



Question 4

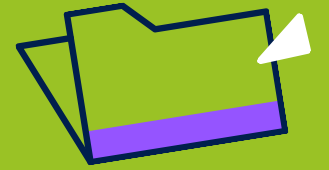


Alex created a password with his name and favorite sport. His password is “AlexSoccer.” Why should Alex choose another password?



1. AlexSoccer is too long.
2. AlexSoccer is hard to remember.
3. AlexSoccer uses his name.
4. Alex likes basketball, too.

Question 4



Alex created a password with his name and favorite sport. His password is “AlexSoccer.” Why should Alex choose another password?



1. AlexSoccer is too long.

2. AlexSoccer is hard to remember.

3. AlexSoccer uses his name.

4. Alex likes basketball, too.



Personal data

Posting on the internet can be as fun as jumping on a trampoline.

Sharing the right info can send you flying high. Sharing the wrong info can make you tumble and fall.

Can you make the right choices?



Please, never share your private information

on the internet with friends or strangers. Even if your friends are good people and will never share it with anyone else, your account or your friend's account can be hacked and all data will be in the hands of criminals.



What is private information?

- Your name and surname
- Date of birth
- Phone number
- Email address
- Home address
- School address and school name/number
- Your parents' credit card details
- Logins and passwords
- Any other information about you and your family that can be used to identify you

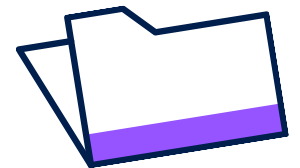




Let's check how safe you are!



If you think this is private information and should not be shared with anyone, please stand up. If you think it is personal information which is ok to be shared, stay seated.





Home address



Email address



Date of birth



Favorite song





**How many brothers
and sisters you have?**

Your dad's phone number



Your favorite video game

A decorative graphic featuring a white question mark at the top center, a white mouse cursor arrow pointing towards the bottom right, and several blue and white arrows and lines scattered around the text. The lines are curved and some have arrowheads, suggesting movement or flow.

Your mom's credit card information



#CyberFit

Name of your pet

#CyberFit

Photo of your pet

Name of your school

Your hobby

#CyberFit

Your favorite sport

Kahoot time!





Quiz time!



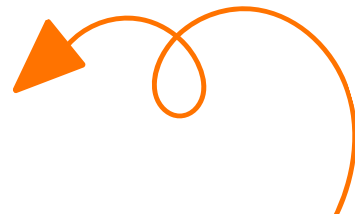
Question 1



Anna receives a message online from someone she does not know asking for her address. The person says she works with Anna's mom and wants to send her mom a birthday card. Why is this a risky situation for Anna?



1. A person she does not know is asking for private information.
2. Her mom might not get a birthday card.
3. The person might get mad if Anna doesn't provide the information.
4. This isn't a risky situation.



Question 1



Anna receives a message online from someone she does not know asking for her address. The person says she works with Anna's mom and wants to send her mom a birthday card. Why is this a risky situation for Anna?

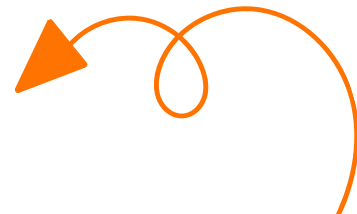


1. A person she does not know is asking for private information.

2. Her mom might not get a birthday card.

3. The person might get mad if Anna doesn't provide the information.

4. This isn't a risky situation.



Question 2



What should Anna do if a person who claims to know her mom asks for her address?

1. Ask a trusted adult for permission before responding.
2. Send the address. It's OK because the person says she works with Anna's mom.
3. Give a fake address because she doesn't really know who the person is.

Question 2



What should Anna do if a person who claims to know her mom asks for her address?



1. Ask a trusted adult for permission before responding.

2. Send the address. It's OK because the person says she works with Anna's mom.

3. Give a fake address because she doesn't really know who the person is.

Let's recap



- **All your actions online leave digital footprints. They can influence your future**, so be careful about what you do and post online.
- When surfing the 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.





Identity. Digital footprints.

What do you see in this image?

What can you infer about the animal which left it?



What do you see in this image?

What can you say about the animal which left it?



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

This data could be leaked and used by scammers against you.

Passive footprints



- Using a search engine like Google
- Online shopping
- Using location services like maps or tagging your location on Instagram
- Using password managers

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

**The internet saves all the data,
even the one which you delete!**



Data sharing responsibilities


Responsibilities to ourselves

Responsibilities to others


Data sharing responsibilities



Responsibilities to ourselves

- Show your best self when you are online
 - Only send things to your friends which you feel comfortable sharing online with the whole internet
- 

Responsibilities to others

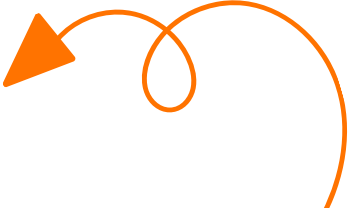


- Get permission before posting a photo of someone or tagging them
 - Treat others online like you want to be treated yourself
- 



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!

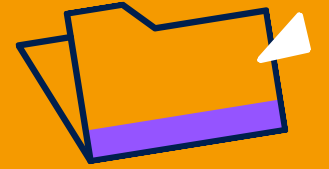




Quiz time!



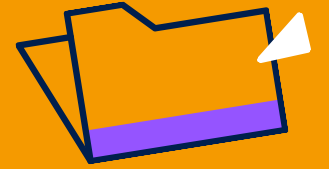
Question 1



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

Last week Anna went on a field trip to a museum with her classmates. Beth, one of Anna's friends, posted a picture showing Anna making a silly face. Anna didn't like the picture and was upset Beth posted it. What should Beth 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 2

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

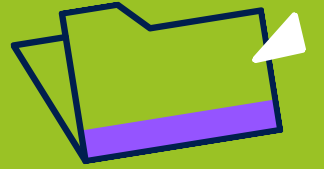
1. Not gone on the field trip.

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 3

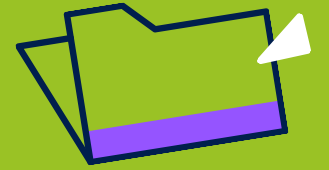


You see a social media post that does not align with your views. Do you _____?



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.

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.



Cyberbullying

What should you do when someone uses mean or hurtful language on the internet?

Cyberbullying



Bullying

is unwanted and aggressive verbal, social, or physical behavior towards another.



Cyberbullying

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

Bully and target

A bully is a the person who is doing the bullying.



A target is a person who is on the receiving end of the bullying.





The bullying or cyberbullying can occur for many different reasons. Has anyone here ever seen or experienced a situation involving bullying? What happened?

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

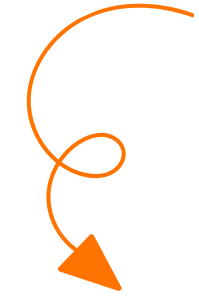


- Ignore the messages
- Block the bully
- Use reporting tools
- Take a screenshot of messages
- Tell a trusted adult (parent, teachers, etc.)

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.**

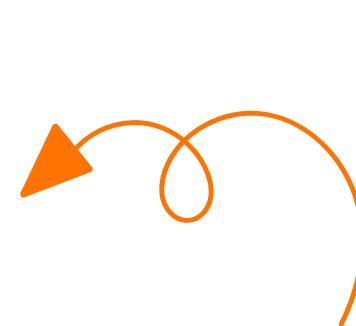
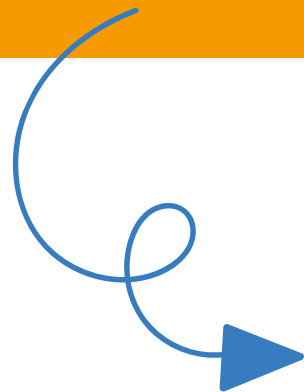
Bystander and upstander



A bystander is a the person who observes a conflict but doesn't take part in it.



An upstander is a person who supports and stands up for someone else.



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.)

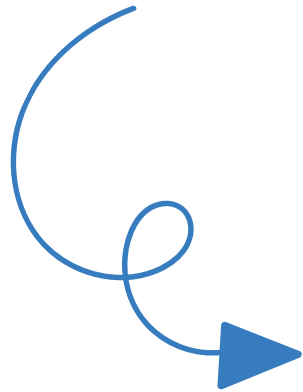
Ways to be an upstander

- 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

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



Kahoot time!





Quiz time!

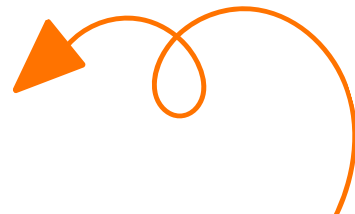


Question 1



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

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



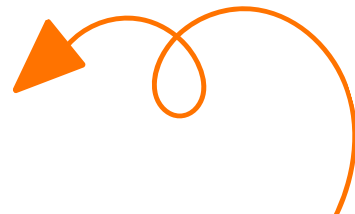
Question 1



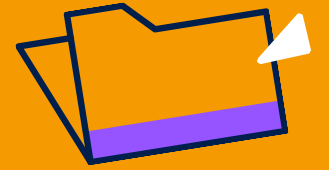
Emma takes a picture of Olivia making a goofy face and posts it online. She leaves the comment, “Olivia, you look so silly!” Olivia should respond by:

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

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



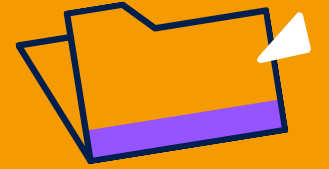
Question 2



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, do not rate them as this information could be shared or published and you really never know who created that site.
2. Shut down your computer immediately.
3. Rate them. You're anonymous so they'll never know it was you.

Question 2



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, do not rate them as this information could be shared or published and you really never know who created that site.

2. Shut down your computer immediately.

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


Question 3



Emma doesn't get along with Mia. Mia has been emailing Emma's friends saying mean things about her. What should Emma do?

1. Say mean things about Mia to her friends.
2. Talk to Mia in person and see if they can work things out.
3. Tell her friends not to be friends with Mia.

Question 3



Emma doesn't get along with Mia. Mia has been emailing Emma's friends saying mean things about her. What should Emma do?

1. Say mean things about Mia to her friends.
2. Talk to Mia in person and see if they can work things out.



3. Tell her friends not to be friends with Mia.

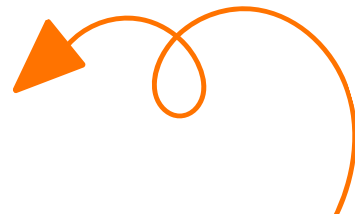
Question 4



James likes to post his videos online, but recently people have been posting mean comments about them. What should he do:



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



Question 4



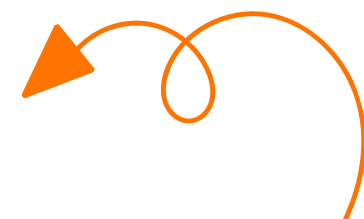
James likes to post his videos online, but recently people have been posting mean comments about them. What should he do:



1. **Block the people making the negative comments.**

2. Take down his videos.

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



Question 5



You are in a chatroom when a bunch of people you don't know come in. They start calling you names and making fun of you. You should:



1. Leave the chatroom for a while and try again later.
2. Tell your parents that some people are really mean.
3. Stop going online completely.

Question 5



You are in a chatroom when a bunch of people you don't know come in. They start calling you names and making fun of you. You should:



1. Leave the chatroom for a while and try again later.

2. Tell your parents that some people are really mean.



3. Stop going online completely.

Question 6



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

1. Do nothing. It’s not Amelia’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.

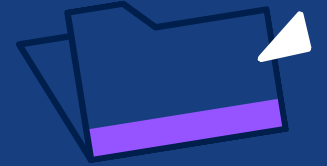
Question 6



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

1. Do nothing. It’s not Amelia’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.

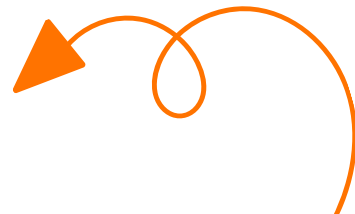
Question 7



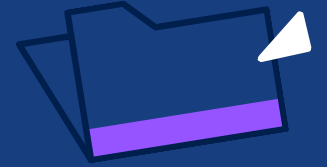
Someone has logged into your online profile and is posting mean things about your friends. You've tried to get back in to take down the mean things, but your password has been changed. What should you do?



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



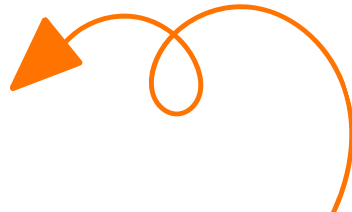
Someone has logged into your online profile and is posting mean things about your friends. You've tried to get back in to take down the mean things, but your password has been changed. What should you do?



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.

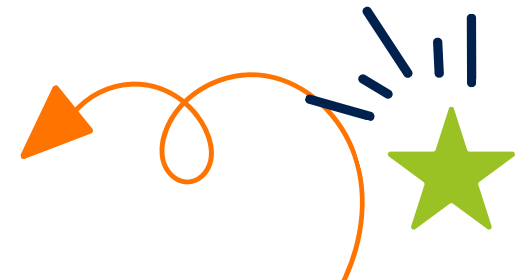
3. Tell your friends that you're sorry, but there's nothing you can do.



Let's recap



- **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 will be stored in internet archives.
- **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.
- 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.



Acronis Cyber Foundation Program

#CyberFit



foundation@acronis.org

acronis.org