

# Internet Safety

"Even when the human being creates the most advanced security systems or technology, there will always be someone who can decipher it's access."

- Paulo Silva, Programmer, 2021



## What can I do to use the Internet safely?



- Use safe passwords;
- Don't download pirated software;
- Don't give your passwords away;
- Don't click on random pop-ups;
- Use a safe anti-virus;
- Use safe browsers;
- Don't download virus.



# Safe on the Internet

E-safety



### Create strong passwords.

Use passwords that are difficult to guess, don't always use the same one, and don't tell anyone.

### Be careful what you download.

Do not download content from untrustworthy sites. They may contain viruses.

### Turn on privacy settings.

Take control of how companies use your data by enabling privacy settings.

### Think before posting.

Avoid posting confidential personal information online.

### Be careful who you talk to.

Be careful who you talk to and the information you share. You don't know who might be on the other side.



37%  admit having been affected by **CYBER-BULLYING!!**



## Social Engineering

The weakest link of a system is the users. No security protocol can withstand bad use.



### INTERNATIONAL INTERNET SAFETY DAY



- WATCH OUT! Don't talk to strangers on the internet.
- BE CAREFUL! With who you talk to on the internet.
- DON'T! Just trust any person.
- DON'T! Share personal information with anyone.

## Social Engineering

The weakest link of a



# SAFER INTERNET DAY





# The Portuguese students created websites about internet safety



<https://sites.google.com/aecarcavelos.com/cybersecurityy/home-page?pli=1&authuser=1>



Important Solutions

### Solutions

Malware	Phishing
<ul style="list-style-type: none"><li>- Install and use anti-malware software and run updates</li><li>- Avoid clicking on links or opening attachments from suspicious emails</li></ul>	<ul style="list-style-type: none"><li>- Be wary of emails or messages that ask for confidential information or links you need not be providing</li><li>- Carefully check the sender of emails and messages</li><li>- Do not click on links or open attachments</li></ul>

<https://sites.google.com/aecarcavelos.com/os-migueis/solu%C3%A7%C3%B5es>

### Solutions

- Keep the system up to date
- Use anti-malware and applications
- Avoid using unsecured Wi-Fi networks
- Use strong passwords
- Do not click on suspicious links

<https://sites.google.com/aecarcavelos.com/cybersecurity1/solutions?pli=1&authuser=1>



<https://sites.google.com/aecarcavelos.com/omar-diogocosta-tiago/home-page>



# SAFER INTERNET DAY \_ IIS LORENZO GIGLI ROVATO 4LL

SAFER INTERNET DAY FEBRUARY 6TH

## WHAT ARE THE POSITIVE ASPECTS OF THE INTERNET?

- QUICK WAY TO FIND INFOS
- MEDIUM TO GET IN TOUCH WITH THE WHOLE WORLD
- MEDIUM TO LEARN NEW THINGS
- MEDIUM TO GET TO KNOW NEW PEOPLE
- MEDIUM TO ENTERTAIN YOURSELF

4LL, IIS. GIGLI ROVATO, ITALY  
LINDA BRAVO, ANDREA MAIREDI, ANNA MAZZINO DELBARBA, LETIZIA SALVONI

Stay safe online!

# Cyber >>> Safety Advises

**Create strong passwords.**  
Use passwords that are hard to guess, and keep track of it using a password manager.

**Think before you post.**  
Avoid posting sensitive personal information online. Don't share too much information either.

**Use a secure VPN connection.**  
A Virtual Private Network (VPN) will ensure your anonymity on the internet.

**Practice safe browsing.**  
A single careless click can expose your sensitive information. Think before you click!

**Be careful of what you download.**  
Avoid downloading apps or software that look suspicious. It may result in malware.

**Don't trust immediately people you meet online**  
People you meet on websites can be fake and have bad intentions

Aurora Bracchi, Lorrishia Amankwah, Sabrina Mugnai and Francesco Martinelli 4L (IIS GIGLI ROVATO)

06/02/2024

Protect yourself when you're online!

# Online Security Tips

- Create strong passwords.**  
Use passwords that are hard to guess, and keep track of it using a password manager.
- Be careful of what you download.**  
Don't download content from sites that are not trustworthy. These may contain malware.
- Turn on privacy settings.**  
Take control of how companies use your data by enabling privacy features.
- Think before you post.**  
Avoid posting sensitive personal information online. Don't share too much information either.
- Use an anti-virus program.**  
Keep your anti-virus software updated so it can detect potential threats in your system.

Ficarra Angelica, Brunori Alice, Peri Alessandro & Piva Luca

SAFER INTERNET DAY

## HOW TO CONSCIOUSLY USE INTERNET:

1. Choose your privacy policy carefully.
2. Don't spend too much time on social media.
3. Do not offend and discriminate against others.
4. Do not share content that is offensive or harms the privacy of others.
5. Don't trust strangers.
6. Immediately report to the social network or the postal police any profile theft or other illegal phenomena.
7. Do not publish personal data of minors or persons who are unable to defend themselves, unless strictly necessary and in any case with the authorisation of the parents or responsible persons.

GIULIA BUCUR, DENISA CRETU, GIULIA ROSSI, VANESSA TONELLI, CRISTIANA V...  
4LL IIS GIGLI ROVATO



5ALL

### STOP CYBER-BULLYING

**WHAT IS CYBERBULLYING?**  
Cyberbullying is similar to other types of bullying, which takes place online and through text messages. Cyberbullies can be classmates, online acquaintances, and/or even unknown people, who usually target their victims.

**SOME EXAMPLES OF WAYS KIDS BULLY ONLINE INCLUDE:**

- Sending mean text or e-mails to other people or posting mean e-mails or photos of other people, such as messages or pictures, to a classmate's teacher.
- Using words to create posts on social media to provoke others.
- Making mean comments on social media or posting embarrassing information about someone's location.
- Posting hurtful comments on social media or sending mean messages via instant messaging or social media.
- Posting false information on social media or making mean comments on someone's profile.

**WHAT ARE THE EFFECTS OF CYBERBULLYING?**  
Cyberbullying causes emotional, social, and physical harm. It can cause a child to feel sad, angry, and a change in behavior. The child may also have trouble sleeping, eating, and concentrating in school. They also may experience physical symptoms, such as headaches, stomach aches, and changes in weight.

**WHY DO PEOPLE CYBERBULLY?**  
Cyberbullying can be a sign of anger, jealousy, or a desire to control someone. Some people cyberbully because they are jealous of someone's success, or they are trying to get revenge. They may also be trying to control someone's behavior.

**HOW TO DEAL WITH IT?**

- If you are being cyberbullied, tell a trusted adult, such as a parent, teacher, or counselor. They can help you deal with the situation.
- Do not respond to the cyberbully. This will only make them feel more powerful.
- Block the cyberbully. This will prevent them from contacting you.
- Report the cyberbully to the appropriate authorities.

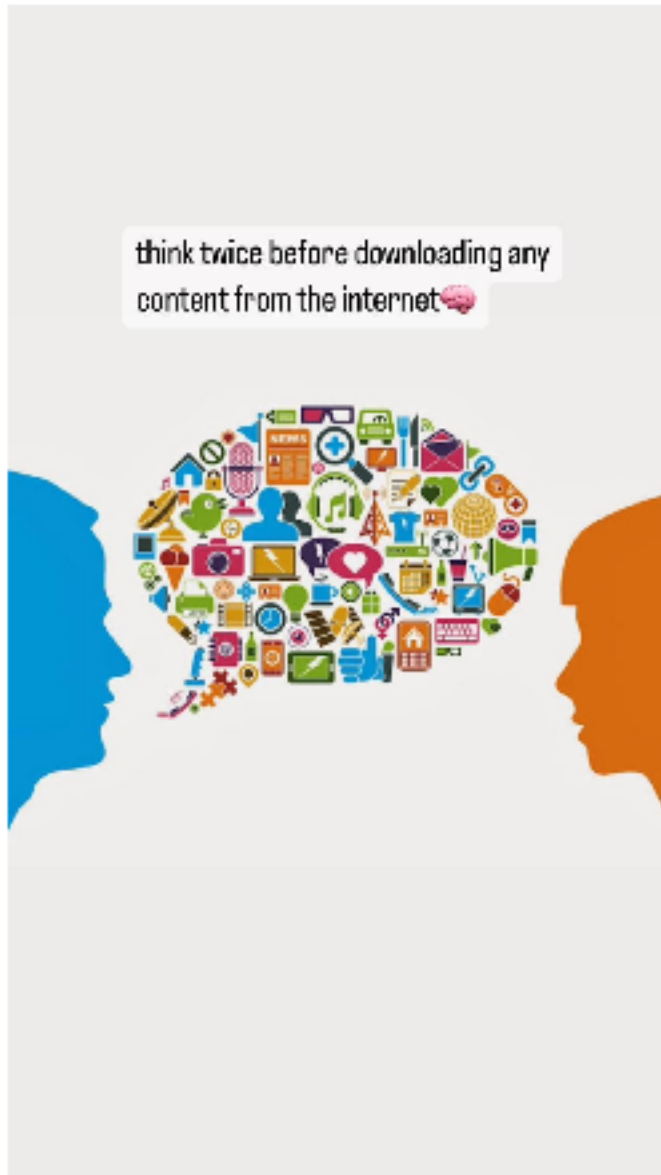
**STOP CYBERBULLYING**





5BLL







# Internet Safety

- 1) Use strong unique passwords
- 2) Make sure your internet connection is secure
- 3) Do online shopping on encrypted sites
- 4) Download apps from verified stores only
- 5) Use an antivirus extension on your browser

Hatice T.

# E-SAFETY

- 01 We should have strong passwords and we should use different passwords
- 02 Make sure your devices are safe before using them.
- 03 We should be polite and kind, we should avoid disrespectful behaviour
- 04 Be careful with the links you click on, make sure they are safe before clicking on them
- 05 Think before sharing things, never share your personal information with anyone

e-Safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (eg text messages, gaming devices, email, etc).

Flanaz G.



# WHAT IS E-SAFETY

If we want to explain e-safety; we can say "being safe in internet." But the internet can be dangerous sometimes. We must protect ourselves from these dangers by taking some precautions.

Ecrin Ö.

# E-SAFETY RULES

How to prevent online scams?

- Protect your personal information with strong passwords.
- Make sure your devices are secure.
- Keep personal information private.
- Pay attention to software updates.
- Set up two-factor authentication.
- Be careful about wifi.
- Back up your personal data.
- Use caution while traveling.
- Shred documents containing financial or personal information.
- Be on the lookout for unusual statements or bills.
- Monitor your credit reports.

Çiğdem D.



## E-SAFETY RULES

Protect yourself from risks!

### CREATE STRONG PASSWORDS.

Use passwords that are hard to guess and remember. Don't reuse passwords.

### BE CAREFUL OF WHAT YOU DOWNLOAD.

Don't download software from untrusted sources.

### TURN ON PRIVACY SETTINGS.

Check the privacy settings on your devices.

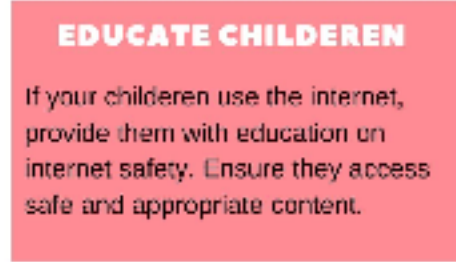
### THINK BEFORE YOU POST.

Think before you post anything online.

### USE AN ANTI-VIRUS PROGRAM.

Use an anti-virus program to protect your device.





Azra D.

### E-SAFETY RULES

What we should and should not do use the internet

- We should research and use the applications we download, the sites we log into and more. We have to make sure it is safe.
- Do not share your personal information with the person you are talking to online or with another person.
- We shouldn't trust everyone and everything in the virtual world.
- If your family or other people around you do not know about it, we should not log in to sites we do not know about without informing them.
- We should be respectful. We shouldn't use bad words.

B. Ece D.

### WHAT YOU SHOULD DO FOR INTERNET SAFETY?

- 01** **EXERCISE YOUR INFORMATION**  
Keep your information safe and secure through a strong password.
- 02** **BEWARE BEFORE YOU POST**  
Consider the possible public effects before posting anything to the internet world.
- 03** **BE CAREFUL**  
Be careful when clicking on links or downloading files.
- 04** **BEET FAMILIES**  
Keep the internet safe by using a secure and reliable browser and antivirus software.
- 05** **USE PERSONAL PASSWORDS**  
Create a unique and strong password for each account and use it only on the intended website.

BERKAY.

### E-SAFETY RULES

Don't post personal photos publicly	Use screen names
Be careful with online ads	Don't respond to messages from strangers
Report cyberbullying	Don't reuse passwords
Don't open attachments from unknown sources	Check the source of emails before clicking links

00

