CYBER SECURITY FOR KIDS 2

JOAS ANTONIO

ABOUT PDF

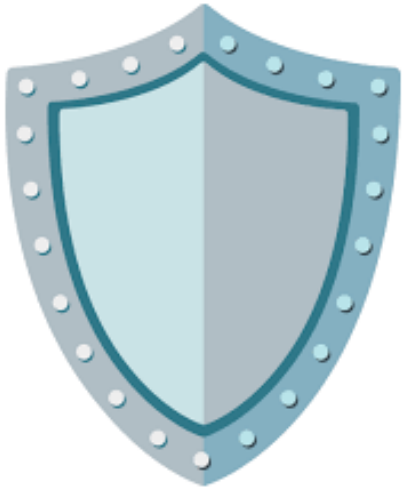
- This document was made for parents, teachers, teenagers and children with basic computer skills or who want to learn more about cybersecurity
- Intended for children from 10 years of age

WHAT IS CYBERSECURITY?

- Cybersecurity is the act of **protecting** the **internet** and its **technologies** from unwanted **intruders.** Quite simply, those who work with **cybersecurity** have a **responsibility** to prevent **evil hackers** from committing some kind of **improper** act against a company.

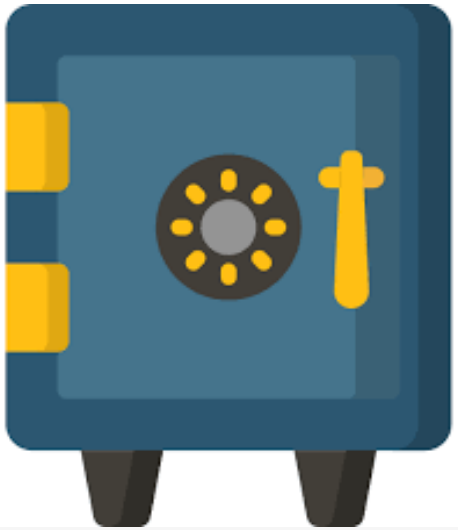
Availability

Ensuring that the website or application must always be active for you to use.
Example: Ensuring a game server is always up and running



Integrity

Ensuring that no information is changed by unauthorized persons.
Example: Ensuring that your friend does not change their nickname or password for their account in an online game



Confidentiality

Prevent unauthorized access and ensure your privacy.
Example: Prevent your colleague from knowing your account information in an online game

TRIAD OF CYBERSECURITY

HACKER VS CHEATER

You must have already come across these two words - Hacker and Cheater, but what's the difference?

MALICIOUS HACKER

The Hacker is a person with great computer skills, knowing in depth how technology works and ways to improve, modify and create something new. In that case he uses his abilities for evil.

There are those malicious hackers like the character shown to the side, **villain** from the **Cyberchase** series, who use their skills to break into computers and steal passwords for example.

CHEATER

The Cheater or the famous cheater, is the one who takes advantage of gaps in games to win a video game match or even get the best items.

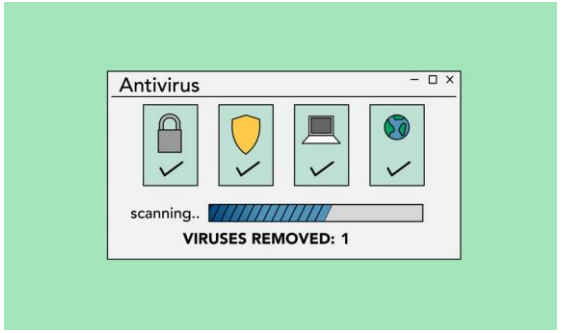
Being through programs known as cheats, or taking advantage of game bugs. We can compare it to **Marvel's Loki**, who uses his powers to overcome himself in various challenges.

NETWORK COMPUTER SECURITY

- The goal is to protect a computer network, which are your devices like computers and cell phones that are connected and exchanging information with each other. Ensuring that no person with bad intentions does not hack your device.

PROTECT YOUR COMPUTER

1. Use antivirus software: Think of antivirus as a vaccine, it ensures that your computer is not infected by any virus that destroys your computer or cell phone;



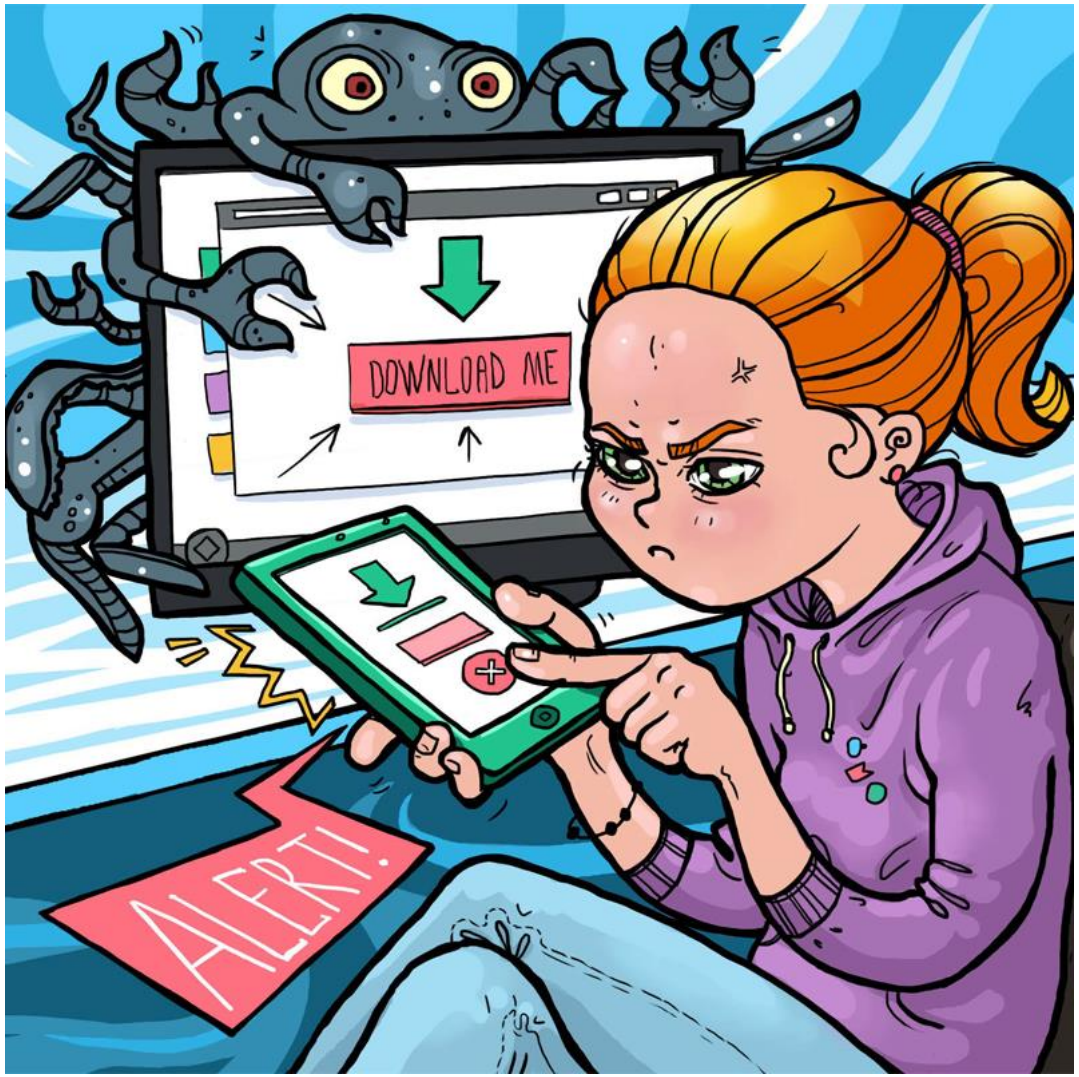
2. Put a strong password: Passwords are the secret that will restrict access to unauthorized people;

3. Backup or copy of information: It is very important to ensure that you do not end up losing any kind of information from your computer. Think of backup as copying keys, so you always have a spare key in case you lose one;

4. Safe internet browsing: It is an important point of security, because when you search the internet you are exposed to various threats, so always search on trusted sites and don't click on anything you see around, consult someone before that.

COMPUTER VÍRUS

- Computer viruses are like diseases that affect us, without proper care, we can get sick and contract a virus that can be weak or strong.
- But unlike the virus that affects us humans, computer viruses aim to do actions that can harm your computer, lock your files or even steal money and passwords.
- Some Malicious Hackers create virus to steal game account passwords or even spy on you without your awareness



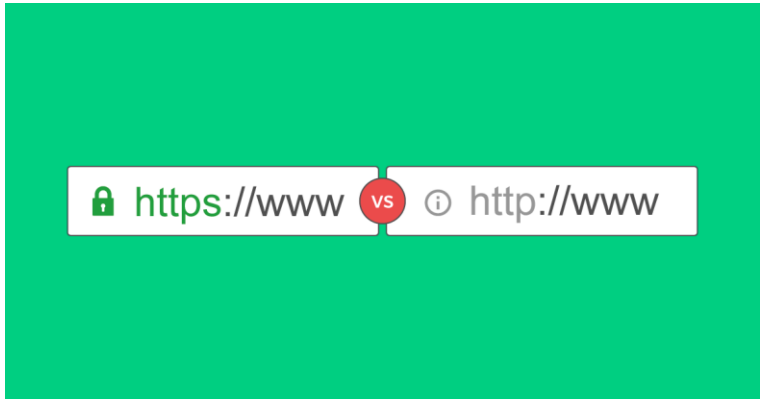
COMPUTER VÍRUS - DEFEND

1. Use antivirus;
2. Do not click on any website or download button;
3. Do not download any apps from unknown websites;
4. If you receive something sent by your friend or family member, confirm that they sent it;
5. Do not download anything that comes by email, whatsapp and telegram for example.

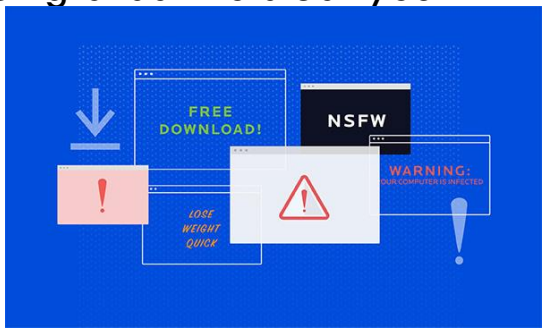
SAFE BROWSING SECURITY

- Be careful when accessing websites or downloading files on the internet, you could end up being hacked;

- Before entering a password or making a purchase, make sure that the site has a closed lock, so you are guaranteed that the information you enter will be more "secure"



- Do not click on advertisements that appear on the websites you are browsing, it may end up being a bait to steal your information or invade your device.

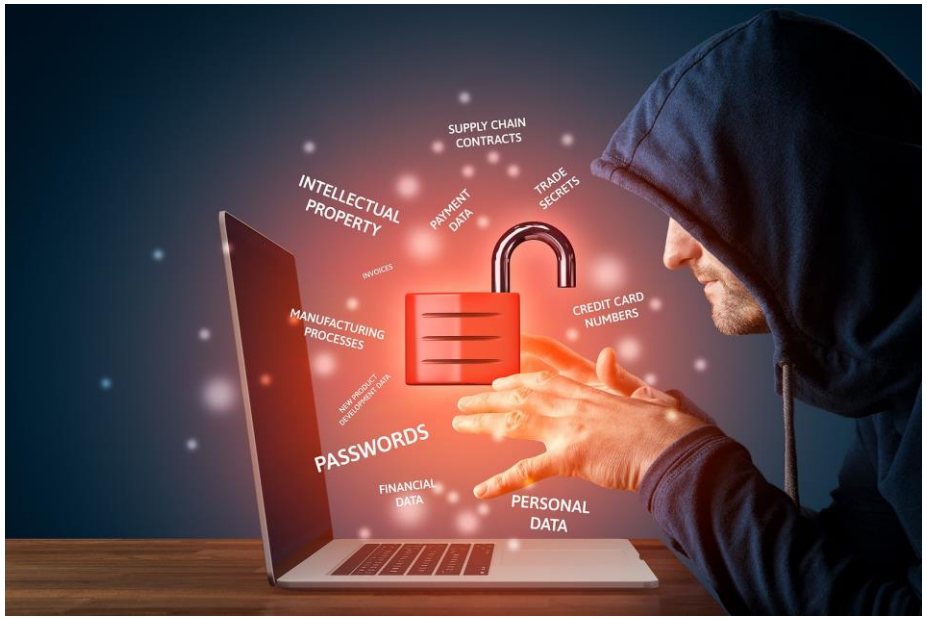


- Do not write down the passwords of your game accounts, Netflix, Amazon Prime, Disney and among other services in notepad, whatsapp conversations or anywhere else.

- Do not access public internet networks, called wifi, as criminals can end up stealing your information and breaking into your devices.

SOCIAL NETWORK SECURITY

- Avoid talking to strangers on social media;
- Avoid posting any kind of photo on your social media, as people with bad intentions can use it for evil;
- Avoid accessing online chats without knowing the people who are participating, as you can avoid numerous risks;
- Do not click on links or download files from unknown people, you can use a site called *__Virus Total__* to help you analyze the origin of this file
- Put strong passwords on your account and enable the second access factor for extra protection



The Dangers Of Social Media (Child Predator Experiment)
https://www.youtube.com/watch?v=6jMhMVEjEQg

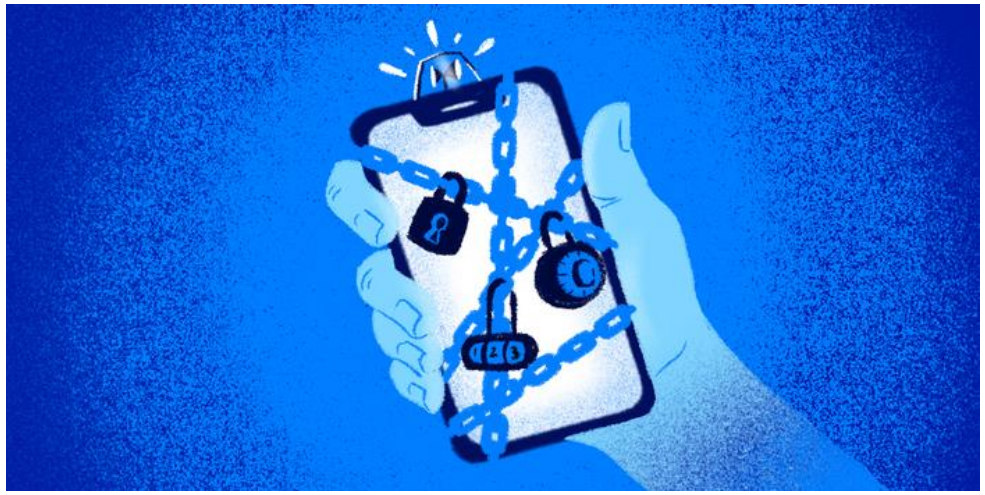
The Dangers of Social Media 2
https://www.youtube.com/watch?v=c4sHoDW8QU4

5 Ways to Protect Yourself Online https://www.youtube.com/watch?v=-ni_PWxrsNo

PROTECT YOUR CELL PHONE

- Always put a screen lock on your phone;
- Do not download apps outside official stores like Apple Store or Play Store;
- Keep your phone and apps up to date;
- Avoid downloading files and applications that you see in tutorials on the internet, many can end up harming your phone;
- Do not register credit cards in your accounts;
- Make backup copies of your data, especially your conversations on whatsapp and other social networks;
- Always keep Bluetooth off if you don't use a wireless headset;
- Don't write down passwords on your cell phone;
- See the security options that your cell phone offers, there are always great options to be activated;

Mobile Security Tips -
https://www.youtube.com/watch?v=ahNb6kA0Lms



ONLINE SHOPPING SECURITY

Shop on trusted sites, remember that sometimes the cheap ends up costing more

Do not save your credit card on any shopping site

Beware of fraudulent emails that arrive in your inbox;

Always make a purchase using the payment system offered by the website you are buying from, any problem with the payment, communicate directly to the website

Check the website reputation of the store you are shopping for

Use secure wifi networks to shop

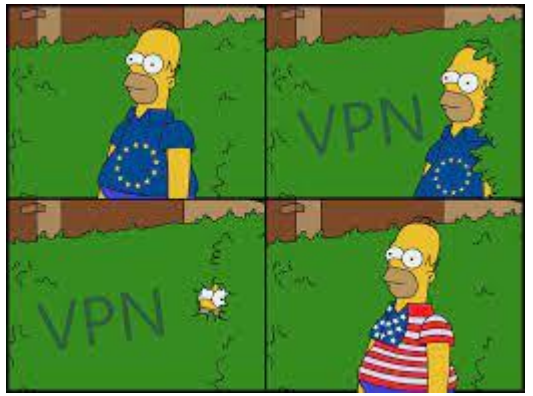
Create strong passwords on any shopping site

Monitor your credit card statement

Do not send credit card information by email

PROTECT YOUR NETWORK COMPUTER

Disable automatic connection to unknown or unexpected Wi-Fi networks.



Use a virtual private network (VPN) when accessing the Internet on public or unknown networks.

Make sure network devices like routers and switches are also protected with strong passwords and security updates.

Limit access to your network to only trusted and authorized devices.

CYBERBULLYING

- Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
  - spreading lies about or posting embarrassing photos or videos of someone on social media
  - sending hurtful, abusive or threatening messages, images or videos via messaging platforms
  - impersonating someone and sending mean messages to others on their behalf or through fake accounts.

HOW TO AVOID CYBERBULLYING

- Talk about the topic in schools;
- Explain the consequences of Cyberbullying;
- Explain about local government laws on Bullying and Cyberbullying;
- Talk to the country about it;
- Seek psychological support;
- Be careful what you post on social media and the friends you have;
- Ignore the bully, if possible block any unwanted comments;

Stop Cyberbullying: https://www.youtube.com/watch?v=zASfp7_-lhg

How to prevent Cyberbullying:
https://www.youtube.com/watch?v=4g8w7GV3-iA

SECURITY DEFINITIONS

- Authentication: The process of verifying a user's identity before allowing access to systems or network resources.
- Backup: A backup copy of important data that can be used to restore data in the event of a system failure.
- Encryption: The process of transforming data into an encrypted format to protect it from unauthorized access.
- Firewall: A software or hardware that protects a network by controlling incoming and outgoing traffic.
- Malware: Any malicious software designed to cause system damage or steal confidential information.
- Phishing: A social engineering technique used to steal sensitive information, such as passwords, through fraudulent emails or fake websites.
- Security policy: A set of rules and practices that guide users' actions regarding security.
- Virtual Private Network (VPN): A secure connection that allows a user to connect to a network from a remote location.
- Strong Password: A complex password that is difficult to guess or hack.
- Security vulnerability: A flaw or weakness in a system or application that could be exploited to allow unauthorized access or damage the system.

SECURITY DEFINITIONS #2

- Spam: Unsolicited emails that often contain advertising or phishing.
- Security Update: A software patch designed to fix a security vulnerability or other issue.
- Security Token: A physical device or application that generates a temporary passcode for two-factor authentication.
- Digital certificate: A digital credential that confirms the user's identity and is used for data encryption.
- Secure DNS: A technology that protects against spoofed DNS attacks, redirects, and other threats.
- Social engineering: A technique used to trick users into providing confidential information.
- Patch Management: A process for applying software updates to vulnerable systems to fix known vulnerabilities.
- Admin Password: A password used to access system or device administration functions.
- Security monitoring: A security practice that involves analyzing logs and tracking suspicious activity on the network.
- Guest network: A separate network that allows guests to access the Internet without accessing the main network.
- Privacy: The user's right to keep personal and confidential information private and secure.
- Ransomware: A type of malware that encrypts user data and demands payment in exchange for a decryption key.
- Physical security: The protection against unauthorized access to physical facilities that contain confidential information.
- Network security: The protection of a network from external and internal threats, including malware, denial of service attacks, and other threats.

BOOKS RECOMENDATIONS