CYPRUS POLICE

For a safer community

Staying SAFE online!

CYBERCRIME UNIT

The internet links the world, regardless of place and time, allowing us to access information on a variety of topics, for leisure or to communicate with friends. The websites's content is not checked before it is published, enabling anyone to upload anything they want on the internet without any restrictions.

Legitimate websites typically provide information on the **design company** and its **owner** at the end of the page. In addition, legitimate websites provide **information about the owner** as well as their **purpose**. Moreover, they provide the user with **means to communicate.**

This enables the user to check and evaluate whether the website is legitimate and safe for browsing.

WHAT TO WATCH OUT FOR

- Be careful in the emails and messages you receive. Avoid opening items from an unknown sender.
- Avoid sending any personal data, especially personal videos or photos.
- Change passwords often and do not disclose them to anyone but your parents or guardians.
- Avoid visiting websites with inappropriate content.
- Ensure that internet addresses begin with “https”, as the **“s”** indicates a secure connection.
- Excessive use of the internet and online games may cause addiction with serious consequences on your physical and mental health.

SOCIAL MEDIA

Social media is a public space for modern communication, where through various platforms, users have the opportunity to communicate in real time and exchange files. Some of the most popular ones are: *Instagram, TikTok, X, Facebook, YouTube, WhatsApp, Viber,* etc. Online games also become “meeting places” for users, who connect, chat and play with each other.

The wide use of these channels by users from all over the world increases the risks, as numerous tricksters use the internet to approach children and young people for various reasons.

Regularly change your nickname and your password and never use the same password in multiple social media.

HOW CAN YOU PROTECT YOURSELF?

- Limit the number of your online friends and choose people who you know personally.
- Avoid publishing your personal photos.
- Your username should not refer to your name, age, phone number, location, or any other personal information.
- Take time to explore the security and privacy settings of your online accounts.
- Through the privacy settings of your account, you can choose who can tag you so that you can prevent someone from using your name without your consent.

Limit the number of your online friends and choose people who you know personally.

Think twice before posting anything online. Anything you send or upload will never be deleted even if you change your mind. At any given time, your videos and photos may end up in the hands of random users.

HOW CAN YOU PROTECT YOURSELF?

- You have the choice of ending any form of communication when someone asks very personal, sexually-related questions or questions that make you uncomfortable.
- Block any undesirable communication. Moreover, you can report any account for further investigation by the platform administrators.
- If your account is breached, inform your acquaintances and friends that you no longer have access to it.
- Think twice before posting anything online. Anything you send or upload will never be deleted even if you change your mind. It is possible that a post or a photo you upload may cause personal or professional issues in the future.

Can I meet someone I met through social media?

In general, you should not meet people you have met online since, you can never be sure that these people use their actual data. They might even pretend to be someone you know. However, if you do decide to meet:

- Arrange to hold this meeting in a public place, where you go often and where people know you.
- It would definitely be safer to be with someone else there. Ask a friend or relative to accompany you.
- Before you go, you absolutely need to tell your parents or guardians about the meeting.

People you meet online may not be who they say they are or they might not use their real picture. Do you really want to meet with them?

Our behavior online has legal consequences. It is important to report any illegal behavior to the Police so that offenders can be identified and punished.

YOUR CONTACTS ON SOCIAL MEDIA

Do not hesitate to speak to your parents and the Police.

Paedophiles chat with their prospective victims with the purpose of collecting as much information as they can about them. They create a friendly relationship and find out about your interests. They then lead the conversation to sexually-related content on issues of sexual content and often send photos of child pornography to create a sense that it is not something bad. That's how they try to embarrass you so that you don't mention anything to your parents.

Such actions aim at weakening you and persuading you to participate in sexual acts at a later stage.

Don't let anyone take advantage of you!

Move any email messages you consider suspicious or are from an unknown sender to the spam/junk mail folder to get rid of suspicious and annoying correspondence

Can I protect my computer from "INTRUDERS"?

Of course! There are various ways to achieve this:

- Install only genuine antivirus software on your devices and avoid pirating as well as the installation of software or applications from unknown sources.
- Activate the automatic lock on the screen. Do not share the unlock codes of your device.
- Move any suspicious unsolicited emails or messages to your junk mail folder to identify potential threats.
- Do not open suspicious links or links that come from unknown persons.
- Keep your data backed up in a different location from the original files.
- Log out from your On-line accounts after each use.
- Never use the same password for your online accounts and change passwords often.
- Avoid using public wireless networks (Wi-Fi).

Do not allow anyone to insult you, mock you, or threaten you online. Block any communication, report it, and immediately inform a trusted adult or the Police.

YOUR SAFETY IS ESSENTIAL

ANONYMITY ON THE INTERNET

The internet is a vast source of knowledge that enables people to access information they never had before. But it needs attention. Any user can create their own online account, to express unfounded opinions, or create fake online accounts.

This fake content can misinform you, harm your mental and physical health or even just deceive you. Use your critical thinking and cross check any information that you read online.

Not everything that goes online is real (fake news).

Any user can create online accounts and spread false information or create fake online IDs.

CONTACT US

Police Headquarters

Evangelou Floraki 1478, Nicosia

Citizen's Line 1460

Tel.: 22808080
Fax.: 22808598

Cyber Crime Unit

Tel.: 22808200
Fax.: 22808465
Email: cybercrime@police.gov.cy
https://cyberalert.cy

Other useful information

https://www.police.gov.cy
https://cybersafety.cy (Tel: 1480)
https://pegi.info

Online complaints platform for cases involving:

- Computer related fraud (Internet)
- Child sexual exploitation (on line)
- Illegal access (Hacking)
- Xenophobia
- Intellectual Property

Through our website: **www.cyberalert.cy**
and choose *"Report Crime"*

or through application for smartphones *"Cyprus Police"*.

www.cyberalert.cy

GET IN ON Google Play

Download on the App Store

Find us:

P.I.O. 58/2024-6.000
ISBN 978-9963-50-648-4

Published by the Press and Information Office
Printed by the Government Printing Office