GUIDELINES FOR PARENTS AND EDUCATORS

CYBERSECURITY

Why Is Digital Security Important?
Unprotected devices and online accounts can seriously compromise your privacy, financial stability, and even personal safety. What's more, one insecure device can spread malware to others, putting the wider online community at risk.

What Are the Most Important Steps to Stay Safe?

- Use strong, unique passwords—and never share them
- Avoid clicking on suspicious links or pop-up messages
- Install trusted security software
- Keep your apps and operating system regularly updated
- Download apps only from verified sources
- Stay alert to online scams and phishing attempts

Are Children and Teens at Risk?
Yes. Young people are particularly vulnerable to digital threats. Their curiosity and frequent online presence can expose them to scams, hacking, and harmful content.
They are also common targets for identity theft, as their clean credit records are attractive to cybercriminals and misuse is harder to detect.
That's why early digital safety education is essential—to empower youth with the knowledge and habits to protect themselves and others online.

How Can I Create a Password That is Both Secure and Easy to Remember?
Think of a personal sentence that's easy for you to recall—something like: "I met Marta Petrova at Josip Broz High School in 2012."
Now take the first letter of each word, add numbers and a special symbol to form a strong password:
➡ **IMMPaJBHSin#12**
To make it even more secure, personalize it for each website by adding a few identifying letters—like "Fb" for Facebook or "Ig" for Instagram:
➡ **IMMPaJBHSin#12Fb**

What is 2-Factor Authentication?

Two-factor authentication (2FA), also known as multifactor authentication, adds an extra layer of security to your online accounts. Similar to using an ATM card, it requires two things: something you know (your password) and something you have (usually your phone).

When you try to log in from a new or unrecognized device, you'll receive a temporary code via SMS, app, or email that you must enter along with your password. This step helps confirm that you are the one trying to access the account.
We strongly recommend enabling 2FA wherever it's available—it greatly reduces the risk of someone hacking into your accounts, even if your password is stolen.

What is "phishing?"
Phishing is when you receive a fake email or message that looks like it's from a trusted source—like your bank or school—asking you to click a link and log in. But the link leads to a fake site designed to steal your login details, credit card, or personal info.
It's one of the most common ways hackers gain access to accounts.

More Advice for Staying Safe

Be Careful Where You Click

Some websites may look safe but are actually designed to trick you. They may contain harmful links that can infect your device with malware—sometimes without you even clicking. This is known as a "drive-by download." These fake sites often offer "free" or tempting content, like movies, gambling, or adult material.

Watch out for clickjacking too—links on social media that seem interesting but lead to spam or harmful sites, or even post bad links on your profile.

How to Recognize a False Link?

Cybercriminals are clever at making fake links look real.

- Check for HTTPS. While not foolproof, a secure website will start with https://. Still, even bad actors can get SSL certificates, so don't rely on this alone.
- Look closely at the URL. Fake links often have misspellings or extra characters. For example, go0gle.com instead of google.com.
- Don't trust shortened links. Services like bit.ly hide the actual URL. Use a URL expander tool or avoid clicking.
- Be cautious with urgent or emotional language. Phrases like "Your account will be locked!" or "Click here to claim your prize!" are common tricks.

Think before you click!

Keep Software and Apps Updated

Always update your operating system, browser, and apps. Updates fix security flaws and protect your device. Turn on automatic updates, and after any update, check your privacy settings—they may reset to default.

More Tips to Stay Safe Online

- **Watch out for scams**. Be cautious of fake charities, messages from "friends" asking for money, or emotional appeals after disasters. Always verify by visiting the official website directly.
- **Be careful what you download.** Avoid downloading apps, files, or software from unknown sources.
- **Use anti-malware protection**. Protect your device with reliable security apps. For a list of trusted tools, visit: www.mksafenet.mk

Fake or hacked websites can put your device and data at serious risk.

For more info, visit www.mksafenet.mk

Co-funded by the European Union