Connecting Minds

Co-funded by the European Union

Be online
Be safe

A guideline about cyber security for young people

Page of Contents

What is cyber security ?

Cybersecurity is all about keeping internet-connected systems safe, including hardware, software, and data, from digital threats and unauthorized access (Be@CyberPro Project Consortium, 2021).

The International Telecommunications Union (ITU) describes it as a mix of tools, policies, security ideas, protective measures, risk management strategies, training, and technologies that help safeguard the cyber environment and the assets of users and organizations (International Telecommunication Union, n.d.).

In short, cybersecurity's goal is to promote **responsible** and **informed** use of digital technologies and encourage safe online behavior.

> ***Being safe online isn't about fear - it's about confidence, awareness, and control.***

Why is cyber security important?

Cybersecurity plays a vital role in keeping individuals, organizations, and important infrastructure **safe** from a variety of **online threats** that are becoming more advanced. These threats can result in serious financial losses, theft of personal information, online harassment and exploitation. That's why cybersecurity is **essential** for ensuring safety in our ever-evolving digital landscape.

Tips for cyber security

Based on Austrailan Goverment advices

1 Use strong passwords or passphrases!

A passphrase is even better than a password because it's tougher for cybercriminals to guess and easier for you to remember.

Aim for a secure passphrase that has at least **14 characters** and includes **four** or more random words, like "purple duck potato boat."

It's also a great idea to use a **different passphrase** for each of your accounts, especially if they include personal information like your name, address, or birthday.

This way, if someone hacks one account, they’re less likely to access your others.

2 Turn on multi-factor authentication!

MFA,or Multi-Factor Authentication, adds an extra layer of security when you log in by requiring **two or more** forms of identity verification.

For instance, you might enter your login details and then provide an authentication code.

This extra step helps keep your account safe from cybercriminals.

Even if someone manages to guess or steal your password, they’ll still need that additional verification to access your account.

Connecting Minds

Tips for cyber security

Based on Austrailan Goverment advices

3 Update!

Make sure your devices and software are always **updated**. Regular updates help keep your devices secure. Cybersecurity experts stress the importance of installing updates **as soon as** they are available. In practice, **regular** updating is not just about protecting your device - it also helps to protect everyone connected to you online.

4 Back up your data!

A backup is simply a **digital copy** of your files, like photos. If your device is lost or stolen, a backup lets you **recover** your data easily. You can save your backups in the cloud or on an external hard drive.

5 Turn off geolocation services!

Geolocation allows **tracking** of your device's location, so it's important to be cautious about sharing your location online with strangers or on public sites (sometimes is better to post holiday's picture after you come back home). Remember to review the location settings for **each of your apps** in your device settings. Most apps **don't need** to know your location. Consider removing apps that don't let you disable this feature.

Connecting Minds

Tips for cyber security

Based on Austrailan Goverment advices

6 Turn off access to photos and camera.

Some apps may request this access, so it's a good idea to review and **modify** these settings for each app. Most apps don't really need to access your camera or photos. You can also select **specific** photos to share instead of sharing everything.

7 Family devices!

If you share devices with your family, it's important to **help them** stay safe online. Encourage them to:

- use strong passphrases
- enable multi-factor authentication
- keep their devices updated.

By **working together**, you can create a safer digital environment for everyone!

8 Using your device outside home!

When you take your devices to school or other public places, please keep these tips in mind:

- **Lock** your device when you're not using it.
- Be cautious about connecting to **unfamiliar Wi-Fi** networks.
- Think carefully about what you **share** or **access** while on your school network.

And don’t forget to follow your school's rules on device use and security!

Connecting Minds

Password hygiene

Good password hygiene involves practices that help you create **strong, secure** passwords and manage them well. This is important for keeping your accounts and personal information **safe** from unauthorized access. Unfortunately, many people don't follow good password practices, which can lead to security issues. Studies show that a lot of hacking incidents happen because of weak or reused passwords (CSO Cyber Handbook, 2023).

1.Make it strong and complex

Make your password **long, random, and unique**. Aim for at least 12 to 16 characters, mixing uppercase letters, lowercase letters, numbers, and symbols.

2. Use a Unique Password for Every Account

Each account, especially those with **personal informagtions** like your bank details, should have its own unique password.

3. Use a Password Manager

Since it's hard to remember many complex passwords, use a secure **password manager**. These tools can create, store, and manage your passwords, so you just need to remember one strong "primary password" to access it.

4. Never Share Your Passwords

Keep your passwords to **yourself.** Don't share them over the phone, text, or email.

5. Avoid Using Personal Information

Stay away from using **easily guessable** personal information in your passwords, like your name, birthday, pet's name, or hometown.

Connecting Minds

Scams

Scams are a type of fraud where cybercriminals deceive people for **financial** gain by tricking them into sharing personal information (LifeLock, 2024). These scams can happen on different digital platforms, such as social media, messaging apps, gaming sites, emails, and phone calls (Webwise, n.d.). Fraudsters often **use tactics** that play on curiosity, peer pressure, and emotions to access sensitive information like bank details, passwords or money.

Common scams

✓ Phishing

Scammers often send messages that appear to be from **trusted platforms** or even from **someone** you know. These messages usually contain a **link** that leads to a fake website, where they try to get you to enter your login details. The goal is to **take over** your accounts or install harmful software. These scams can come through emails, text messages (often called smishing), messaging apps or social media. One trick they use is to create a sense of urgency, making you feel rushed to act quickly.

✓ Impersonation and Social Engineering

Scammers often set up **fake profiles** that look like friends, influencers or other trusted people to gain your trust. After that, they might send you a harmful link or ask for your personal information. Sometimes, they pretend to be someone you know to reach out to their contacts. This can result in **account takeovers**, as seen in cases where hackers impersonated activists to disable their social media accounts.

Common scams

✓ Sextortion

This is a type of financial cybercrime where someone, often **pretending** to be a young person online, forms a **relationship** with a victim to get **nude or semi-nude pictures**. These images are then used to blackmail the victim for money, more pictures, or to target others. The threats usually include sharing the images with the victim's friends and family, leading to feelings of panic, shame, and fear. Young males aged **14 to 18** are especially at risk of falling victim to this crime.

✓ Gaming and "Too Good to Be True" Offers

Scams are quite common on gaming platforms. Some fraudsters create fake offers for **in-game rewards**, free upgrades, or rare items to trick users into giving away their **login details** or making small "verification" payments. Likewise, scams that say "You've Won!" promise fun prizes but ask for **personal information** or **processing fees** to claim them, which is a way to steal your data or money.

✓ Money Mule Recruitment

Criminal networks often target teenagers and young adults through social media ads to get them involved in receiving and transferring **stolen money**. Victims are usually tempted with a **share** of the money or a **gift** and many don't realize this is illegal and can have serious consequences, like a criminal record. While this scam is most common among people aged **18 to 24**, victims can be as young as 14.

✓ Romance Scams and Catfishing

Scammers often create fake profiles on dating sites, social media or online forums to form **relationships**. Once they've gained trust, they might **ask for** money, gifts or personal information, turning the interaction into something harmful. This is a type of **online grooming,** where someone befriends a child online with bad intentions.

Know How to Respond and Get Help

(UNICEF, 2020)

If something goes wrong online, it's really important to act quickly and speak up.

Share Your Experience: If you're facing cyberbullying, grooming, sextortion or any other online harm, the first thing to do is talk to a trusted adult -like a parent, family member, teacher or school counselor. They can provide support and help you decide what to do next.

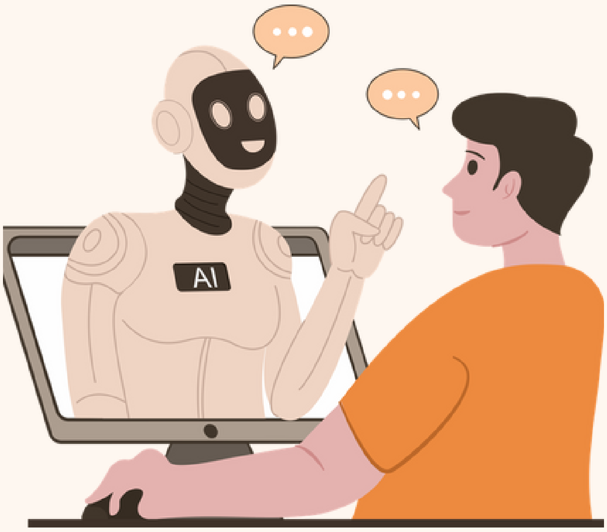
Report and Block Harmful Behavior: Use the reporting tools available on social media and gaming platforms to flag harmful content and block anyone who is bothering you. Reporting is usually anonymous and helps keep you and others safe.

Save Evidence: If you're being bullied or harassed, it’s a good idea to save things like screenshots of messages or posts to show what’s been happening.

Reach Out for Help: If you're feeling overwhelmed, anxious, or unsafe, consider calling a national helpline to chat with a professional counselor anonymously. In case of an emergency, don’t hesitate to contact the police. You can also reach out to organizations like the CyberTipline to report child sexual exploitation.

AI ethics

Artificial intelligence is changing the way we live, learn, and connect with each other. It assists us in writing, creating art, translating languages and even identifying illnesses. However, with every technology that enhances our abilities, it also increases our **choices**. AI ethics focuses on using these tools **responsibly**, ensuring that the decisions made by machines align with our human values, and making certain those values are fair, clear and compassionate.



AI systems learn from vast quantities of images, voices, and texts gathered online. If this data shows **stereotypes** or **unfair treatment**, the AI might echo those patterns. That's why we should consider not just what AI can achieve, but what it ought to accomplish.

Ethics in AI goes **beyond preventing harm**; it's about making sure that technology benefits everyone fairly, fosters human creativity, and honors privacy and dignity.

Deepfakes and Misinformation

AI can now create realistic videos, voices, and images that aren't real. While some of these creations are fun and harmless, others can be used to **trick, scam, or bully people**. It's important to learn how to spot manipulated content as a key digital skill.

Look out for unusual shadows, lips that don't match the words, or movements that seem off. Always check the **source**. If you're unsure, take a moment to pause, think, and talk it over before sharing.

Fairness, Accountability, Transparency

Fairness means AI systems should treat everyone equally, no matter their gender, race, age or background.

Accountability reminds us that behind every algorithm, there are real people. Designers, developers and users all share the responsibility for how technology is created and used.

Transparency is all about being open. Knowing how an algorithm works or what data it uses helps us make better choices. Asking questions like “Who created this?” or “What data was used?” is part of being a responsible digital citizen.

> ***AI is likely to be either the best or the worst thing to happen to humanity - Stephen Hawking***

What you can do

Explore: Have conversations about AI ethics in schools or youth groups. Check out short videos or real-life examples showing how algorithms influence opinions online.

Act: Take a moment to think before you share, post or comment. Consider how AI content might impact others. Show your support for creators who use technology in a responsible way.

Reflect: How much do you trust what you see online?
What would “ethical technology” mean to you?
How can you use AI tools in a creative way that doesn’t harm anyone?

Misinfrmation, Disinformation, and Malinformation

Misinformation is false information shared without the intent to mislead. A person might share an outdated article believing it is true.

Disinformation is false information shared intentionally to deceive or harm. It is often used to manipulate opinions or political decisions.

Malinformation is information that is based on facts but used out of context to cause harm. An example is publishing private messages or selective facts to damage someone's reputation.

False information is **not only an online issue.** It shapes opinions, influences elections and affects trust in institutions. Research shows that false news spreads **six times** faster than the truth, especially on social media, because emotional and shocking content attracts more attention.

Misinformation, Disinformation, and Malinformation

Before you believe or share something, take a moment to:

- **STOP** – Take a pause before you react.
- **QUESTION** – What feelings does this story bring up? Why do you think that is?
- **CHECK** – Who published this? Is the author legitimate? Is this information found elsewhere?
- **DECIDE** – If you choose to share it, think about how and why you're doing so.

(NABH, 2024)

Connecting Minds

Quiz yourself

1. What is the primary goal of cybersecurity?

A. To focus exclusively on protecting hardware from physical damage.
B. To promote the responsible and informed use of digital technologies.
C. To ensure that all online information is publicly accessible.
D. To prevent the development of new digital technologies.

2. Passphrase like 'purple duck potato boat swimming with a glossy coat' is a good security measure. What makes this type of passphrase effective?

A. It uses personal information that is easy for the user to remember.
B. It can be used for all online accounts to simplify login procedures.
C. It is long, uses multiple random words, and is difficult for others to guess.
D. It is short and can be typed quickly on any device

3. How does Multi-Factor Authentication (MFA) enhance account security, even if a cybercriminal has your password?

A. It deletes the account permanently after one failed login attempt.
B. It makes the password invisible to anyone trying to steal it.
C. It automatically reports any login attempt to the authorities.
D. It requires a second form of verification that the criminal is unlikely to possess.

4. A scammer sends an email that appears to be from a trusted platform, containing a link and a message that says 'Your account will be suspended in 1 hour unless you verify your details.' What is this tactic an example of?

A. Money Mule Recruitment
B. Sextortion
C. Catfishing
D. Phishing

5. What is the primary purpose of creating a data backup?

A. To allow for easy recovery of your files if your device is lost or stolen.
B. To prevent anyone from accessing your device without permission.
C. To increase the processing speed of your device.
D. To automatically install the latest security updates on your software.

Quiz yourself

6. What is the key difference between misinformation and disinformation, as defined in the source material?

A. Misinformation is always based on facts, while disinformation is completely fabricated.

B. The intent of the person sharing the information.

C. Disinformation spreads faster than misinformation.

D. Misinformation is spread online, while disinformation is spread offline.

7. In the context of AI ethics, what does the principle of 'Transparency' involve?

A. The AI's ability to operate without any human supervision.

B. Being open about how an algorithm works and what data it uses.

C. The AI system treating every user equally, regardless of their background.

D. The people who create and use AI being responsible for its actions.

8. Which of the following is considered a poor password hygiene practice according to the handbook?

A. Creating a password that is at least 12 characters long with mixed character types.

B. Including your birthday or pet's name to make it easier to remember.

C. Using a unique password for each of your online accounts.

D. Using a password manager to store credentials.

9. If you are experiencing online harassment, what is suggested as the most important first step?

A. Talk to a trusted adult like a parent, family member, or teacher.

B. Post screenshots of the harassment publicly to expose the person.

C. Confront the person directly and ask them to stop.

D. Immediately delete all of your online accounts.

10. How might scammers on gaming platforms trick users?

A. By helping other players complete difficult levels in the game.

B. By organizing official, developer-sanctioned online tournaments.

C. By creating fake offers for in-game rewards or free upgrades.

D. By offering technical support to fix bugs in the game.

Answers

1.What is the primary goal of cybersecurity?

B. To promote the responsible and informed use of digital technologies.

The cybersecurity's goal is to encourage safe and responsible online behaviour.

2.Passphrase like 'purple duck potato boat' is a good security measure. What makes this type of passphrase effective?

C. It is long, uses multiple random words, and is difficult for others to guess.

Secure passphrase is long (at least 14 characters) and contains several random words, making it tough to crack.

3.How does Multi-Factor Authentication (MFA) enhance account security, even if a cybercriminal has your password?

D. It requires a second form of verification that the criminal is unlikely to possess.

MFA adds another layer of security, such as an authentication code, which someone with only the password would not have.

4. A scammer sends an email that appears to be from a trusted platform, containing a link and a message that says 'Your account will be suspended in 1 hour unless you verify your details.' What is this tactic an example of?

D. Phishing

Phishing: impersonating a trusted source and creating sense of urgency to trick someone into providing login details on fake site.

5. What is the primary purpose of creating a data backup?

A. To allow for easy recovery of your files if your device is lost or stolen.

If a device is lost, a backup lets you recover your data easily.

Answers

6. What is the key difference between misinformation and disinformation, as defined in the source material?

B. The intent of the person sharing the information.

Misinformation is defined as fake informarion being shared without intent to mislead, whereas disinformation is shared intentionally to deceive.

7.In the context of AI ethics, what does the principle of 'Transparency' involve?

B. Being open about how an algorithm works and what data it uses.

Transparency is defined as being open and knowing how an algorithm functions or what data was used to train it.

8. Which of the following is considered a poor password hygiene practice according to the handbook?

B. Including your birthday or pet's name to make it easier to remember.

It is specifically underlined that using easily guessable personal information in passwords is a bad practice.

9. If you are experiencing online harassment, what is suggested as the most important first step?

A. Talk to a trusted adult like a parent, family member, or teacher.

The first thing to do is talk to a trusted adult who can provide support and help decide on next steps.

10. How might scammers on gaming platforms trick users?

C. By creating fake offers for in-game rewards or free upgrades.

Fraudsters create fake offers for rewards to trick users into giving away login details or making payments.

Bibliography

1. Addy Osmani. (2025, April 26). Avoiding skill atrophy in the age of AI [Blog post]. Substack. https://addyo.substack.com/p/avoiding-skill-atrophy-in-the-age
2. Balkan, E., & Ülgen, S. (2023). A PRIMER ON MISINFORMATION, MALINFORMATION AND DISINFORMATION. https://edam.org.tr/uploads/yukleme_resim/Report-Disinformation-Malinformation-Misinformation.pdf
3. Be@CyberPro Project Consortium. (2021). Teenagers and cybersecurity: A practical guide for teachers and parents (Erasmus+ Project 2018-1-ES01-KA201-050461). McGraw Hill.
4. Council of Europe, Haarmann, M., & Heise, R. (2020). DIGITAL RESISTANCE. In Democratic and Inclusive School Culture in Operation (DISCO). Council of Europe. https://wergelandcentre.org/content/uploads/2020/09/Digital-Resistance-Handbook-for-Teachers-ENG.pdf.pdf
5. CSO Cyber Handbook. (2023). Cybersecurity handbook for civil society organizations (Version or edition if given). https://cso.cyberhandbook.org/sites/default/files/2023-02/%5BEnglish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations_0.pdf
6. Cyber Safety Project. (2025). AI deepfakes parent toolkit [PDF]. https://cybersafetyproject.com/wp-content/uploads/2025/08/CSP-AI-Deepfakes-Parent-Tool-Kit-2025.pdf
7. Foundation European Institute Outsourcing. (2019, October 20–27). Combating fake news: Handbook for youth workers. Zebrzydowice, Poland: European Commission Erasmus+ Programme. https://www.salto-youth.net/downloads/toolbox_tool_download-file-2402/Handbook%20-%20How%20to%20Fight%20Fake%20News.pdf
8. Grant, D., The American Psychological Association, National Advisor of Healthy Device Management, & Newport Healthcare. (2024). MISINFORMATION, MALINFORMATION, DISINFORMATION, AND FAKE NEWS. In Integrity Institute. https://www.nabh.org/wp-content/uploads/2024/12/NABH_cyber_misinformation_v2.pdf
9. International Telecommunication & Research Exchange (ITRex). (2024, August 27). What is AI bias: Definition, types, examples, and debiasing strategies. https://itrexgroup.com/blog/ai-bias-definition-types-examples-debiasing-strategies/
10. International Telecommunication Union. (n.d.). Cybersecurity (Study Group 17). https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
11. LifeLock. (2024, July 28). Get schooled: 8 ways to avoid college student identity theft. Norton LifeLock. https://lifelock.norton.com/learn/identity-theft-resources/college-students-identity-theft
12. Story-Maker. (n.d.). Lesson Three: Recognizing A.I. generated content. https://story-maker.org/library/lesson-three-recognizing-ai-generated-content/
13. UNICEF. (2020, April 8). 10 tips teens can stay safe online. UNICEF Armenia. https://www.unicef.org/armenia/en/stories/10-tips-teens-can-stay-safe-online
14. UNICEF. (2021). AI guide for teens [PDF]. https://www.unicef.org/innocenti/media/1381/file/UNICEF-Global-Insight-AI%20guide%20for%20teens-2021.pdf
15. Webwise. (n.d.). Online scams and young people: What parents need to know. Webwise. https://www.webwise.ie/parents/online-scams-and-young-people-what-parents-need-to-know/

Co-funded by the European Union