Project Number: 2023-2-LT01-KA210-ADU-000173746

POSITIVE DIGITAL PARENTING

Induction to Pedagogy for Parents

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project number 2023-2-LT01-KA210-ADU-000173746

Co-funded by the Erasmus+ Programme of the European Union

INTRODUCTION ✳

UNCRC defines positive parenting as ; parental behaviour that respects children's best interests and their rights. With the introduction of internet, new digital technologies and social media to families around the world, the fundamental role of parents and the goals of parenting remain unchanged: parents are still required to nurture, to protect, to provide for, to love, to connect with and to guide their children. It also holds true that parenting practices in the past and today are most effective when grounded in values and principles of positive parenting that foster open communication and trust. These models and values need to be extended into the online world in order to establish the connection between traditional values and the online world, but also to contain the risks linked to it for children.The digital environment offers tremendous benefits for children, opening new channels for education, creativity, and social interaction. But it can also pose serious risks, including cyberbullying, risks to privacy, neglecting of other activities, sedentary behaviour, online addiction, among others.

Co-funded by the
Erasmus+ Programme
of the European Union

INTRODUCTION ✳

POSITIVE DIGITAL PARENTING Erasmus+ project aims to empower parents with Media Literacy knowledge and tools to foster critical thinking skills in their children when interacting with digital media : analyzing online content, recognizing biases, identifying misinformation, and making informed decisions in the digital environment. By combining critical thinking with media literacy, parents can better prepare their children to navigate the digital world responsibly and discerningly.

This programme of learning will provide induction training for parents as they are the primary caregivers and educators within the family unit. This approach aims to educate parents in understanding the issues related to online learning and the use of dynamic online tools so that they can integrate with the digital lives of their children and support their parents and senior adults in their families to learn about the dangers and pitfalls of the internet. This learning material encourages online safety and tackles the digital divide that exists between different generations of the family.

Co-funded by the
Erasmus+ Programme
of the European Union

PARTNERS

ASOCİACİJA IVAIGO

- Project development through social research, focusing on the main issues society is facing nowadays: social inclusion, environmental concerns, any kind of discrimination, digital transformation, physical and mental health care, women empowerment, unemployment, entrepreneurship, etc.
- Gaining knowledge and boosting creativity, imagination, and critical thinking through all types of art and sport.
- Sustainable improvement of the professional and personal skills of participants in a multicultural context.
- Representing the interests of young people, especially minorities and social groups.
- Promoting formal and non-formal education among young people through local activities and international projects. IVAIGO creates inclusive environments that foster equity and equality.

Co-funded by the
Erasmus+ Programme
of the European Union

PARTNERS

INCİRLİOVA GENCLİK KULTUR SANAT VE GELİSİM DERNEGİ

- İ.ova Gençlik Kültür , Sanat ve Gelişim Derneği -IOVA is an organization of non-profit nature, counts more than one hundred (100) individuals as members, creative citizens, people who share values, ideas, thoughts, reflections and vision. IOVA is a young and dynamic organisation that was created as a response to the need for a vibrant, community based formation that will be able to recognise opportunities and respond to challenges related to the unique character of the local community and its members. The focus of IOVA is:
- To encourage civic participation and active involvement through non-formal education;
- Implementation of new social practices in the field of media safety, fake news, social network violence, convergence of media technologies, etc.;
- The value of ICT strategies as a means of bridging the digital divide and as a powerful tool for economic & social development around the EU;
- Providing digital education for youth workers,adult trainers . and teachers

Co-funded by the
Erasmus+ Programme
of the European Union

PARTNERS

EESTI PEOPLE TO PEOPLE

Eesti People to People is a non-profit organisation registered in Estonia in 1997 and with activities since 1993 as a chapter of People to People International NGO. The purpose of People to People aims to enhance international understanding and friendship through educational, cultural and humanitarian activities involving the exchange of ideas and experiences directly among peoples of different countries and diverse cultures. Eesti PTP is committed to enhance cross-cultural communication within each community, and across communities and nations. Tolerance and mutual understanding are central themes

Co-funded by the
Erasmus+ Programme
of the European Union

Context

Co-funded by the Erasmus+ Programme of the European Union

Internet usage is deeply ingrained in modern family life, with children and young adults actively embracing online activities and seniors gradually navigating the digital landscape. As parents increasingly take on the role of digital facilitators, it is crucial for them to be mindful of the inherent risks associated with internet use.

While the internet offers a plethora of benefits, including access to information and communication platforms, it also exposes users to various dangers such as inappropriate content, security breaches, misinformation, and cyberbullying. Parents must proactively safeguard their family members while respecting their privacy.

It's important for parents not to adopt a discouraging stance towards digital technology but rather to embrace the challenge of ensuring that children, young people, and seniors can safely enjoy the benefits of the internet. This involves equipping them with the skills and knowledge to identify and mitigate risks and threats online.

Therefore, comprehensive online safety education is essential for all family members, including children, teens, young adults, parents, and seniors. As the linchpin of the family unit, parents are uniquely positioned to provide support, assistance, and guidance to the most vulnerable members.

The POSITIVE DIGITAL PARENTING Erasmus+ project's A2 Guidelines for Safe Online Use aim to familiarize parents with online dangers, enabling them to adopt a preventive and informed approach to maximize the benefits of internet use while ensuring safety for their family unit.

Co-funded by the
Erasmus+ Programme
of the European Union

THE IMPORTANCE OF BEING SAFE ONLINE

Online safety, or internet safety, is a critical aspect of navigating the digital world responsibly. It encompasses a range of practices and behaviors aimed at protecting oneself and others from online threats and dangers. This includes safeguarding personal information, ensuring secure communication channels, and promoting positive digital citizenship.

In today's interconnected world, where smartphones, tablets, and computers are ubiquitous, being safe online is more important than ever. Individuals must be aware of the risks associated with online activities, such as cyberbullying, phishing scams, and exposure to inappropriate content. By staying informed and adopting safe practices, individuals can mitigate these risks and enjoy a safer online experience.

For parents and caregivers, ensuring the online safety of children is paramount. This includes monitoring their online activities, setting age-appropriate restrictions, and educating them about safe online behavior. Additionally, fostering open communication about online experiences can help children feel more comfortable discussing any concerns or issues they may encounter online.

Ultimately, online safety is about empowering individuals to make informed decisions and navigate the digital world with confidence. By staying vigilant and practicing good cyber hygiene, we can all contribute to a safer and more secure online environment for everyone.

Co-funded by the
Erasmus+ Programme
of the European Union

THE DIGITAL FOOTPRINT

The concept of a digital footprint is akin to leaving a trail of 'electronic breadcrumbs' as you navigate the internet. This trail consists of various activities and interactions, such as the websites you visit, the photos you upload, and your interactions on social networks. Much like footprints on a beach, your digital footprint can reveal a lot about you and your online activities.

However, unlike beach footprints that may fade over time, your digital footprint can remain indefinitely. This means that anything you do or post online has the potential to be permanent, even if you delete it later. This permanence underscores the importance of being mindful of what you share online and the potential consequences of your digital actions.

The information contained in your digital footprint can be used to create a detailed profile of you, including your interests, habits, and behaviors. It's crucial to consider who can access this information and to understand that even with strict privacy settings, there's always the possibility of content being copied and shared beyond your intended audience.

In essence, managing your digital footprint involves being aware of the trail you leave behind online and taking steps to ensure that it accurately reflects your intentions and values. This includes being mindful of the content you share, understanding your privacy settings, and being cautious of the potential long-term implications of your online actions.

Co-funded by the
Erasmus+ Programme
of the European Union

THE DIGITAL FOOTPRINT

Managing your digital footprint is crucial in today's digital age, where online activities can have long-lasting effects on your personal and professional life. Here are some tips to help you manage your digital footprint effectively:

1.**Be mindful of what you share**: Think before you post. Consider the potential implications of sharing personal information, photos, or opinions online. Remember that once something is posted, it can be difficult to remove it completely.

2.**Use privacy settings**: Familiarize yourself with the privacy settings on social media platforms and other online services. Adjust these settings to control who can see your posts and information.

3.**Regularly review your online presence**: Periodically review your social media profiles and online accounts. Remove or update any outdated or irrelevant information.

4.**Limit personal information**: Avoid sharing sensitive personal information such as your address, phone number, or financial details online.

5.**Use strong passwords**: Use strong, unique passwords for your online accounts to prevent unauthorized access. Consider using a password manager to keep track of your passwords securely.

6.**Be cautious of what you click**: Be wary of phishing scams and malicious links. Avoid clicking on links or downloading attachments from unknown or suspicious sources.

7.**Monitor your online reputation**: Use search engines to regularly check what information about you is available online. If you find any inaccurate or harmful information, take steps to address it.

8.**Educate yourself and others**: Stay informed about best practices for online safety and privacy. Educate your friends and family about the importance of managing their digital footprint.

By following these tips, you can effectively manage your digital footprint and protect your online reputation. Remember that your online presence is a reflection of you, so it's essential to take control of what you share and how you present yourself online.

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE PRIVACY

Online privacy, also known as internet privacy or digital privacy, is the extent to which personal, financial, and browsing information remains confidential when someone is online. With the increasing amount of personal data being shared and stored online, concerns about online privacy have grown significantly.

Protecting online privacy is crucial for several reasons. Firstly, individuals have the right to keep details of their personal lives private and not share them with strangers. Additionally, it can be challenging to know what personal information is being collected and by whom, as data collected by one company may be shared with others without your knowledge or consent.

Online data privacy should be treated with the same level of importance as privacy in the physical world. Just as you would have a confidential conversation behind closed doors or only share financial details with a bank, you should take steps to protect your online privacy. This includes using strong, unique passwords, being cautious about the information you share online, and regularly reviewing your privacy settings on social media and other online platforms.

By valuing and protecting your online privacy, you can reduce the risk of your personal information being misused or shared without your consent.

Co-funded by the
Erasmus+ Programme
of the European Union

DATA PRIVACY

Data privacy is a fundamental right that has gained significant attention, particularly with the implementation of the General Data Protection Regulation (GDPR) in the European Union. Enforced in 2018, GDPR was designed to protect the privacy and data of every EU citizen by establishing strict rules for how personal data is collected, processed, and stored.

GDPR comprises 99 articles that outline various aspects of data protection. Some key provisions include:

1.**Right to access**: Individuals have the right to know what data a company holds about them and how it is being used.

2.**Right to erasure**: Also known as the "right to be forgotten," individuals can request the deletion of their personal data under certain circumstances.

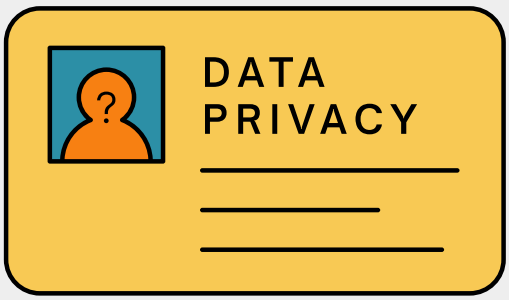
3.**Consent**: Companies must obtain explicit consent from individuals before collecting or processing their personal data. This includes clear and unambiguous consent for cookies and browsing history.

4.**Data minimization**: Companies should only collect and process data that is necessary for the purpose for which it was collected.

5.**Data portability**: Individuals have the right to receive their personal data from a company in a commonly used and machine-readable format.

6.**Data protection officers**: Some organizations are required to appoint a Data Protection Officer to oversee GDPR compliance.

GDPR has significantly impacted how companies handle personal data, requiring them to implement stricter data protection measures and provide greater transparency regarding data processing practices. GDPR has been instrumental in enhancing data privacy rights and empowering individuals to have more control over their personal information.



Co-funded by the
Erasmus+ Programme
of the European Union

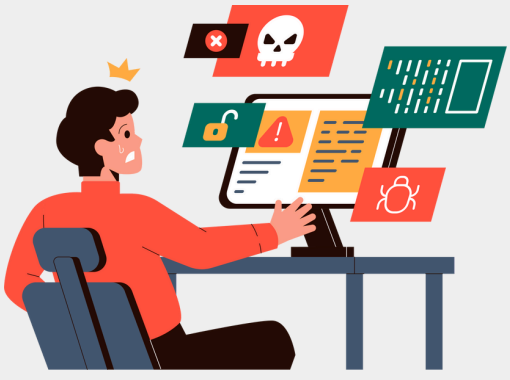
ONLINE THREATS

Cyber threats are malicious activities aimed at damaging data, stealing information, or disrupting digital operations. These threats encompass a wide range of actions, including cyber-attacks that target information technology assets, computer networks, intellectual property, and sensitive data. Cyber threats can originate from both internal and external sources.

Internal threats may arise from trusted users within an organization who misuse their privileges or access to sensitive information. External threats, on the other hand, originate from remote locations and are often perpetrated by unknown parties seeking to exploit vulnerabilities in digital systems.

Examples of cyber threats include malware, ransomware, phishing attacks, and denial-of-service (DoS) attacks. These threats can have severe consequences, including financial losses, data breaches, and damage to an organization's reputation.

To protect against cyber threats, organizations and individuals must implement robust cybersecurity measures. This includes regularly updating software, using strong passwords, encrypting sensitive data, and educating users about potential threats and how to avoid them. Additionally, implementing multi-factor authentication and regularly backing up data can help mitigate the impact of a cyber-attack.



Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

Internet dangers can be defined as anything that may cause harm to an internet user. This harm can come in many forms (e.g., physical, emotional, psychological, financial, social, and reputational). Many of the different types of internet dangers are outlined below:

Types of online dangers:
Today there is the possibility to access almost anything on the internet, from entertainment, credit and financial services to products from every corner of the world. While the internet affords a certain level of anonymity, there are increasing ways in which the user's personal information can be at risk.

1-**Cyberbullying** : Cyberbullying is a form of bullying that occurs using digital technologies, such as social media, messaging platforms, gaming platforms, and mobile phones. It involves repeated behavior that aims to intimidate, anger, or shame the targeted individual. Examples of cyberbullying include spreading lies or rumors about someone on social media, sending hurtful messages or threats via messaging apps, and impersonating someone to send mean messages.

One of the key differences between face-to-face bullying and cyberbullying is that cyberbullying leaves a digital footprint. This means that there is a record of the bullying behavior, which can be useful in providing evidence to stop the abuse. It's important for individuals to be aware of their digital footprint and understand that their online actions can have real-world consequences.

To combat cyberbullying, it's essential for individuals to report any instances of cyberbullying to the relevant platform or authority. It's also important to educate young people about responsible online behavior and the impact of cyberbullying. By working together, we can create a safer online environment for everyone.

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

2- **Cyber Predators** : A Cyber Predator is an individual, typically an adult, who uses the internet to exploit children and teens for various forms of abuse, including sexual, emotional, psychological, or financial harm. These predators target vulnerable individuals through various online platforms such as chat rooms, instant messaging, social networks, and video games.

One common tactic used by Cyber Predators is to create a false identity, pretending to be a child or teen themselves. They use this fake identity to establish relationships with their victims, gradually gaining their trust and manipulating them into engaging in harmful activities.

The grooming process is a key strategy employed by Cyber Predators, where they slowly manipulate their victims over time, often by exploiting their vulnerabilities and insecurities. This process can involve building a seemingly genuine friendship or relationship with the victim before exploiting them for their own gain.

It is crucial for parents, caregivers, and educators to educate children and teens about online safety and the dangers posed by Cyber Predators. Encouraging open communication about online interactions and setting boundaries can help protect young people from falling victim to these predators. Additionally, monitoring online activities and being aware of warning signs can help identify and prevent potential abuse.

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

3-**Posting Private Information Avoiding** sharing personal information is crucial to protect data, prevent identity theft, and stay safe online. This is important not only when surfing the web but also when using and sharing information on social media platforms.

Examples of personal information that should be protected include:
1.**Names**: Full name, family name, and parent's names.
2.**Personal ID numbers**: Social security number, driver's license number, passport number, patient ID number, taxpayer ID number, credit account number, or financial account number.
3.**Addresses**: Street address and email address.
4.**Biometrics**: Retina scans, fingerprints, facial geometry, or voice signatures.
5. **Vehicle ID or title numbers**.
6. **Phone numbers**.
7.**Technology asset information**: Media Access Control (MAC) or Internet Protocol (IP) addresses that are tied to a certain individual.

When using social media, it's important to be mindful of the information you share. Avoid posting personal details such as your full name, address, or phone number publicly. Use privacy settings to control who can see your posts and information, and be cautious about accepting friend requests or messages from unknown individuals. By being vigilant about protecting your personal information, you can reduce the risk of identity theft and other online threats.

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

4-**Phishing:** Phishing attacks are deceptive tactics used by cybercriminals to trick individuals into providing sensitive information, such as credit card numbers or login credentials. These attacks typically involve fake communication, such as emails or messages, that appear to be from legitimate sources. The goal of phishing attacks is to steal personal information or install malware on the victim's device.

Phishing attacks can take various forms, including emails that appear to be from your bank or a popular web service. These emails often contain links that, when clicked, lead to fake websites that mimic the appearance of the legitimate site. Once on the fake website, victims are prompted to enter their personal information, which is then captured by the cybercriminals.

While phishing attacks have traditionally been associated with emails, cybercriminals are now using other methods to target victims. This includes text messages, phone calls, fake apps, and social media quizzes. These tactics are designed to lure individuals into providing their personal information or clicking on malicious links.

To protect against phishing attacks, it is important to be cautious when opening emails or messages from unknown senders. Verify the authenticity of emails by checking the sender's email address and avoiding clicking on links or downloading attachments from suspicious sources. Additionally, use security software and keep it up to date to help detect and prevent phishing attacks

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

5-**Falling for Scams** : Internet scams are fraudulent schemes conducted by cybercriminals on the Internet. These scams can take various forms and are designed to deceive individuals into providing sensitive information or money. Internet scams can occur through various channels, including phishing emails, social media, SMS messages, fake tech support phone calls, and scareware.
The main goal of internet scams is often to steal personal information, such as credit card details or login credentials, or to trick individuals into sending money to the scammer. Some common types of internet scams include:

1.**Phishing emails**: Emails that appear to be from legitimate organizations, such as banks or government agencies, but are actually attempts to trick individuals into providing personal information or clicking on malicious links.

2.**Social media scams**: Scams that occur on social media platforms, such as fake profiles or advertisements that lead to phishing websites or malware downloads.

3.**SMS scams**: Scams that are sent via text message, often containing links to fake websites or requests for personal information.

4.**Fake tech support calls**: Scammers posing as technical support representatives who try to convince individuals that their computer has a problem and then request payment or access to the computer to "fix" the issue.

5.**Scareware**: Fake software or pop-up messages that claim a computer is infected with a virus and prompt the user to purchase unnecessary software or services.

To protect against internet scams, it is important to be cautious when receiving unsolicited messages or requests for personal information. Verify the legitimacy of the sender or organization before providing any information or clicking on links. Additionally, use up-to-date security software to help detect and prevent scams.

Co-funded by the
Erasmus+ Programme
of the European Union

ONLINE DANGERS

6-Accidently downloading malware: Accidentally downloading malware is a common computer security threat that can have serious consequences. Malware, short for malicious software, includes viruses, worms, Trojans, and other harmful programs designed to damage or disrupt your computer system.

A computer virus is a type of malware that is capable of replicating itself and spreading to other computers. It can alter the way your computer operates, often without your knowledge or permission, and can cause a range of problems, from minor annoyances to serious damage.

To avoid accidentally downloading malware, it is important to be cautious when downloading software from the internet. Carefully evaluate free software and avoid downloading from peer-to-peer file sharing sites, as these are common sources of malware. Additionally, be wary of emails from unknown senders, as they may contain malicious attachments or links.

Most web browsers today have built-in security settings that can help protect against online threats. It is important to keep these settings updated and to enable additional security features, such as pop-up blockers and anti-phishing tools.
However, the most effective way to protect against viruses and other malware is to use up-to-date antivirus software from a reputable provider. Antivirus software can help detect and remove malware from your computer, as well as provide real-time protection against new threats. Regularly updating your antivirus software and running scans of your computer can help keep your system safe from malware infections.

Co-funded by the
Erasmus+ Programme
of the European Union

KEY COMPETENCES TO BE SAFE ONLINE

Online safety is a catch-all word for encouraging children, young people and more vulnerable members of the family's safety when using any device connected to the internet. The online world can enrich the lives of children and teenagers in a variety of ways, both personally and educationally.
It is important to sum up the key competences for learners to stay safe online:

a.Recognize the risks: Recognizing the risks of online activity is crucial for staying safe on the internet. By identifying potential threats and dangers, individuals can take proactive steps to reduce their online exposure and protect themselves from harm.

To begin with, it's important to adopt a preventive approach to online safety. This means being aware of the potential risks and taking steps to mitigate them before they become a problem. By staying informed about common online threats, such as phishing scams, malware, and identity theft, individuals can better protect themselves from these dangers.

Reducing online exposure is another key aspect of staying safe online. This can involve limiting the amount of personal information shared on social media and other websites, using privacy settings to control who can see your information, and being cautious about clicking on links or downloading attachments from unknown sources.

Recognizing the risks of online activity and taking proactive steps to reduce exposure is essential for staying safe and secure in the digital world. By staying informed and being proactive, individuals can protect themselves from online threats and enjoy a safer online experience.

Co-funded by the
Erasmus+ Programme
of the European Union

KEY COMPETENCES TO BE SAFE ONLINE

b.Keep personal information safe:
Keeping personal information safe is essential for maintaining a secure online presence. To protect your identity and ensure a safe digital life for you and your family, it's important to follow certain guidelines:

1.**Use strong, unique passwords**: Passwords are the keys to your digital house. It's crucial to use strong, unique passwords for each of your accounts and avoid using easily guessable passwords. Consider using a reputable password manager to generate and store complex passwords securely.

2.**Avoid sharing passwords**: Never share your passwords with anyone, even with trusted individuals. Sharing passwords can compromise the security of your accounts and personal information.

3.**Backup your data**: Regularly backup your important data to protect it from loss or theft. This can be done using external hard drives, cloud storage services, or other backup solutions. Backup data should be encrypted and stored securely.

4.**Keep software up-to-date**: Ensure that all software on your devices, including operating systems, browsers, and applications, is regularly updated with the latest security patches and updates. This helps protect against vulnerabilities that could be exploited by cybercriminals.

5.**Use security software**: Install and regularly update reputable antivirus and anti-malware software on your devices to protect against viruses, malware, and other online threats.

6.**Enable two-factor authentication** (2FA): Enable 2FA on your accounts whenever possible to add an extra layer of security. This requires a second form of verification, such as a code sent to your phone, in addition to your password.

By following these guidelines, you can help protect your personal information and ensure a safer online experience for you and your family.

Co-funded by the
Erasmus+ Programme
of the European Union

KEY COMPETENCES TO BE SAFE ONLINE

c.Do not download unknown files : Downloading unknown files can expose your computer and personal information to various risks, including malware, viruses, and other malicious software. To protect yourself and your devices, it's important to follow these guidelines:

1.**Be cautious of email attachments**: Do not download attachments from unknown or suspicious emails. These attachments could contain malware that can harm your computer or steal your personal information.

2.**Verify the source**: Before downloading any file, verify the source to ensure it is legitimate. Only download files from trusted websites and sources.

3.**Use reputable antivirus software**: Install and regularly update antivirus software on your computer. This software can help detect and remove malware from downloaded files.

4.**Enable file extensions**: Enable file extensions on your operating system so that you can see the full file name. This can help you identify potentially malicious files.

5.**Avoid peer-to-peer (P2P) file sharing**: Be cautious when using P2P file sharing services, as they can expose you to malware and other risks. Only download files from trusted sources.

6.**Scan files before opening**: Use antivirus software to scan downloaded files before opening them. This can help detect any malware or viruses present in the file.

By following these guidelines, you can reduce the risk of downloading unknown files and protect your computer and personal information from online threats.

Co-funded by the
Erasmus+ Programme
of the European Union

KEY COMPETENCES TO BE SAFE ONLINE

d. Use critical thinking skills to analyse and evaluate information online;
Using critical thinking skills to analyze and evaluate information online is essential for protecting yourself from scams, phishing attempts, and misinformation. Here are some guidelines to help you stay safe:

1.**Be skeptical**: Question the source and validity of information you encounter online. If something seems too good to be true or doesn't seem quite right, it's best to investigate further before taking any action.

2.**Check for spelling errors and suspicious email addresses**: Be wary of emails, messages, or websites that contain spelling errors or use email addresses that are not legitimate. These can be signs of phishing attempts or scams.

3.**Verify the source**: Before clicking on any links or downloading attachments, verify the source of the information. Look for official websites or reputable sources to ensure the information is legitimate.

4.**Think before you click**: Avoid clicking on links or attachments in emails or messages from unknown or suspicious sources. Hover over links to see the actual URL before clicking.

5.**Be cautious of out-of-the-blue communications**: If you receive a communication from a friend or acquaintance that seems out of character or unexpected, verify the source before taking any action. Their account may have been compromised.

6.**Use security software**: Install and regularly update antivirus and anti-malware software on your devices. This can help detect and prevent malicious software from infecting your device.

By using critical thinking skills and following these guidelines, you can protect yourself from online threats and misinformation.

Co-funded by the
Erasmus+ Programme
of the European Union

KEY COMPETENCES TO BE SAFE ONLINE

e. Verify the web site you are on is safe :
Verifying the safety of a website is crucial to protect yourself from online threats, especially when entering sensitive information like payment details. Here are some steps to verify the safety of a website:

1.**Check the URL**: Look at the website's URL and ensure it starts with "https://" instead of just "http://". The "s" stands for secure and indicates that the website has an SSL certificate, which encrypts data transmitted between your browser and the website.

2. **Look for a padlock icon**: Check for a padlock icon in the address bar next to the URL. This indicates that the website is secure and uses HTTPS encryption.

3.**Verify the website's legitimacy**: Before entering any personal or payment information, verify the legitimacy of the website. Look for contact information, such as a physical address and phone number, and check reviews or ratings from other users.

4.**Use a secure payment method**: When shopping online, use a secure payment method, such as PayPal or a credit card, that offers buyer protection. Avoid using debit cards or bank transfers, as they offer less protection against fraud.

5.**Use a high-security browser**: Consider using a browser that offers additional security features, such as built-in phishing and malware protection. Some browsers also display a green address bar or other indicators to show that a website is safe.

6.**Update your browser and security software**: Keep your browser and security software up to date to protect against the latest threats and vulnerabilities.
By following these guidelines, you can help ensure that the websites you visit are safe and protect yourself from online threats while shopping or browsing the web.

f.Be aware of your digital footprint.
Once online, always online: anything posted online, it is out there for everyone to see, it is necessary to be careful with the identifiable information used in social media profiles and the sites visited, registered on, or that hold any type of the user's personal information.

Co-funded by the
Erasmus+ Programme
of the European Union

PROACTIVE MEASURES AND GUIDELINES FOR ONLINE SAFETY

• Adopting a safer mindset is crucial for staying safe online, as it helps individuals recognize potential risks and take proactive measures to protect themselves. Here are some key points to keep in mind:

1.**Be cautious of false sense of security**: While computers may seem safe, they can be vulnerable to various online threats. It's important to remember that cybercriminals can cause real harm through the internet, such as identity theft, financial loss, and damage to your devices.

2.**Stay informed**: Keep yourself informed about the latest online threats and security best practices. This can help you recognize potential risks and take appropriate action to protect yourself.

3.**Follow safety measures**: Implement the safety measures discussed above , such as using strong, unique passwords, keeping your software up to date, and avoiding clicking on suspicious links or attachments.

4.**Use common sense**: Use your common sense when interacting online. If something seems too good to be true or doesn't feel right, it's best to err on the side of caution and avoid it.

5.**Be proactive**: Take proactive steps to protect yourself online, such as regularly backing up your data, using security software, and being cautious of the information you share online.

6.**Stay vigilant**: Stay vigilant and be aware of your online surroundings. Be cautious of unsolicited emails, messages, or requests for personal information, and verify the source before taking any action.

Co-funded by the
Erasmus+ Programme
of the European Union

PROACTIVE MEASURES AND GUIDELINES FOR ONLINE SAFETY

By adopting a safer mindset and following these guidelines, you can help protect yourself from online threats and enjoy a safer online experience.

•Create stronger passwords.
A strong password is one of the best ways to defend your accounts and private information from hackers.

•Browser security features
Computers faces different threats whenever browsing the Web, including viruses, malware, and spyware. The good news is your web browser has a lot of built-in security features to help protect your computer.

•Avoiding spam and fishing
To be protected from email scams, malicious software, and identity theft, it is necessary to understand how to identify and avoid potentially dangerous content.

•Avoid malware with an anti-virus.
Malware is one of the most common hazards to your computer when you are online, but it is easy to avoid, securing your computer and learning how to identify and avoid suspicious links are the fundamentals.

•Safe online shopping
Online shopping is a convenient way to buy from the comfort of one's home. And while there are many benefits there are also some risks. There are ways to protect and ensure your financial data is secure, such as verifying the security and veracity of the website.

Co-funded by the
Erasmus+ Programme
of the European Union

PARENTAL CONTROLS

Parental controls are a vital tool for ensuring your child's safety online. Here are some key points to consider:

1. **Content filtering**: Parental controls allow you to filter the content your child can access online, blocking inappropriate websites and materials.

2.**Time limits**: Set time limits for your child's online activities to ensure they are not spending too much time online.

3.**App and game controls**: Control which apps and games your child can download and access, ensuring they are age-appropriate.

4.**Privacy settings**: Ensure your child's privacy settings are configured correctly to protect their personal information.

5.**Monitoring and tracking**: Some parental control tools allow you to monitor your child's online activities and track their location.

6.**Education and communication**: It's important to educate your child about online safety and the importance of responsible internet use. Encourage open communication so they feel comfortable discussing any concerns or issues they may encounter online.

7.**Regularly review settings**: Regularly review and update your parental control settings to ensure they are still appropriate for your child's age and maturity level.

Remember, while parental controls are a valuable tool, they are not foolproof. It's essential to also teach your child critical thinking skills and resilience so they can navigate the online world safely and confidently.

Co-funded by the
Erasmus+ Programme
of the European Union

BREAKDOWN OF DIFFERENT TYPES OF PARENTAL CONTROLS

Parental controls offer various features to help parents manage their children's online activities. Here's a breakdown of the different types of parental controls:

1.**Filtering and blocking**: These features limit access to specific websites, words, or images that parents deem inappropriate. They can help protect children from accessing harmful content online.

2.**Blocking outgoing content**: This feature prevents children from sharing personal information online and via email, helping to protect their privacy and safety.

3.**Limiting time:** Parents can set time limits for how long their children are allowed to be online and the times of day they can access the internet. This can help manage screen time and ensure children are not online at inappropriate times.

4.**Monitoring tools**: These tools alert parents to their children's online activity without blocking access. They can record which websites a child has visited and display warning messages when they visit certain sites. This allows parents to stay informed about their children's online behavior.

It's important to note that while parental controls can help protect children online, they are not a substitute for education, responsibility, and adult supervision. Parents should educate their children about the potential risks of the internet and establish rules about suitable and inappropriate websites. Open and honest conversations with children are key to creating a safe online environment where they feel comfortable discussing any concerns or issues they may encounter online.

Co-funded by the
Erasmus+ Programme
of the European Union

BASIC GUIDELINES FOR PARENTAL SUPERVISION

Parental supervision is crucial for ensuring children's safety online. Here are some basic guidelines for effective parental supervision:

1.**Spend time online together**: Teach children appropriate online behavior by spending time with them online. This allows you to monitor their activities and discuss any potential risks.

2.**Keep the computer in a common area**: Place the computer in a common area of the house, such as the living room, where you can easily monitor its use. Avoid placing computers in individual bedrooms, and monitor the time spent on smartphones or tablets.

3.**Bookmark children's favorite sites**: Bookmarking children's favorite sites for easy access helps them navigate the internet safely and reduces the risk of accessing inappropriate content.

4.**Check financial accounts**: Regularly check financial accounts, card statements, and phone bills for any unfamiliar charges, which could indicate unauthorized online purchases.

5.**Inquire about online protection**: Find out what online protection measures are in place at your child's school, after-school center, friends' homes, or any other place where children may use a computer without supervision.

6.**Take reports seriously**: If your child reports an uncomfortable online exchange or incident, take it seriously and investigate the issue promptly. Encourage open communication so that your child feels comfortable discussing any concerns they may have.

Co-funded by the
Erasmus+ Programme
of the European Union

TIPS FOR PARENTAL SUPERVISION

Will Gardner, director of the UK Safer Internet Centre, has some useful information parents or careers who want to manage their children's and family's relation with internet. Retrieved from: https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

• Ask your family members (particularly kids) how the internet makes them feel
"Talk regularly with your child about how they use technology, and find out what their digital life is like, including what their favourite sites and services are and also how being online makes them feel. Listening to your child will give you the best possible idea of how you can support them."

• Overwhelming kids with restrictions is not helpful
"As parents it's natural to feel worried about the risks posed by your child being online, but for young people the online world is exciting and fun, as it brings so many opportunities for them.
"Remember that your child will use technology and the internet differently given that they are growing up in a world immersed in all things digital. Try to look at both the positive and negative aspects of being online and empower your child with safe choices they can make instead of overwhelming them with restrictions."

• Get to know the apps and services they are using.
"You can take steps to support your child online by using features such as privacy settings on social media and understanding how to make a report on a range of apps, games and services."

• Use available tools to help.
"There are lots of tools to help you manage the devices used by your family. For example, knowing how to activate and use parental controls can help protect your child from seeing inappropriate content online."

Co-funded by the
Erasmus+ Programme
of the European Union

INTERNET SAFETY CHECKLIST

According to Norton Security Centre, playing it safe online can help prevent you — and your family — from being exposed to unwanted information, materials, or risks on the internet that might harm your devices, personal information, or your family. It's smart to teach specially children computer safety so that they don't fall victim to some common dangers that we previously mentioned.

Here is an Internet Safety Checklist based on advice from Norton Security Centre:

1.**Use strong, unique passwords**: Ensure all accounts have strong, unique passwords to protect against unauthorized access.

2.**Keep software up to date**: Regularly update operating systems, browsers, and security software to protect against vulnerabilities.

3.**Use security software**: Install reputable antivirus and anti-malware software to protect against viruses and other threats.

4.**Be cautious of phishing scams**: Be wary of emails, messages, or websites that ask for personal information or contain suspicious links.

5.**Enable two-factor authentication**: Enable two-factor authentication on accounts that offer it for an extra layer of security.

6.**Use secure networks**: Avoid using public Wi-Fi for sensitive activities and use a virtual private network (VPN) when necessary.

7.**Monitor children's online activities**: Keep an eye on children's online activities and educate them about safe internet practices.

8.**Back up important data**: Regularly back up important data to protect against data loss due to malware or hardware failure.

9.**Limit sharing personal information**: Be cautious about sharing personal information online and only do so on secure, reputable websites.

10.**Educate yourself and your family**: Stay informed about the latest online threats and educate your family about safe internet practices.

Co-funded by the
Erasmus+ Programme
of the European Union

REFERENCES

Internet safety tips and checklist to help families stay safer online. Norton Security Center. Retrieved from: https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html

How to protect your privacy online. Norton Security Center (2021) https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

Internet Safety: Avoiding Spam and Phishing. GCFGlobal (2021) Retrieved from: https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/

Parental controls. Internet matters (2021) https://www.internetmatters.org/parental-controls/

The 5 cyber safety tips every parent should know. Norton Security Center. Retrieved from: https://us.norton.com/internetsecurity-kids-safety-5-cybersafety-tips-every-parent-should-know.html

What are web threats? Kaspersky (2021) Retrieved from: https://thebossmagazine.com/internet-safety-tips/

What is a digital footprint? netsafe (2021) https://www.netsafe.org.nz/digital-footprint/

What is Online Safety? National Online Safety (2021) Retrieved from: https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety

The dangers of sharing personal information on social media.

Patel, D., May 2020, PennToday. Retrieved from: https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

STEGNER, Ben. (2017) The complete guide to parental controls. MUO: Technology explained. Retrieved from: https://www.makeuseof.com/tag/guide-parental-controls/

Staying safe online: guidelines for parents and teens

https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

How to protect your private information online. UK Norton Security Centre https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html

Co-funded by the Erasmus+ Programme of the European Union