Safer Internet Day 2022 | Tuesday 8 February

Together for a better internet

www.saferinternetday.org

European Commission | INHOPE insafe

PARENTS GUIDE TO BEING CYBER SMART

This Guide provides information to parents and care-givers of children of all ages to help them ensure their children are safe online. Children especially, unlike older generations, have developed an ease and familiarity of use with Internet technologies that makes them 'digital natives' or tech savvy. While these digital skills are beneficial, there are significant risks that come with them. Digital literacy is crucial as technology continues to advance. Children remain vulnerable to online risks and it is crucial for parents and care-givers to empower and support their children to have safer and more positive experiences online.

THIS PUBLICATION IS PROUDLY SPONSORED BY THE AFP IN COLLABORATION WITH THE PNG SAFER INTERNET COMMITTEE (PNGSIC)

1. SOCIAL MEDIA

What is social media?

Social media refers to computer or mobile based technology that facilitates the sharing of ideas, thoughts, and information through virtual networks and communities. It is internet – based and gives users quick, electronic communication of content, such as personal information, documents, videos, and photos.

The entire experience of social media aims to get people more connected, however, as a parent you may feel completely disconnected when it comes to your own kids' online activities.

ADVANTAGES

1. **Education opportunities and access**
   Social networking sites and interest from students has advanced a range of internet-based and digital tools to provide distance education and online learning opportunities.
2. **Global connectivity**
   The internet removes geographical barriers, offering the chance to connect with others and share information in seconds with others all over the world, sharing experiences and perspectives.
3. **Online marketing**
   For businesses, the internet and social media platforms offer a mechanism to grow audience, expand sales, and collect data to help refine products. It offers instant feedback and expanding the reach of product or services.
4. **Access to information**
   All Information is accessed at the touch of a button.
5. **Platform for artists**
   Artists share their work with millions, while maintaining creative control for themselves.

DISADVANTAGES

1. **Privacy breaches**
   Sharing your online location, inappropriate content, or too much with the public has irreversible effects. Online hackers can gain access to your personal data. These groups rely on digital illiteracy.

2. **Hacking technology is also advancing**
   Popular social media quizzes, like the ones that pop up in Face book feeds, may look harmless and fun — but taking them can leave you vulnerable to identity theft or fraud. Hackers and scammers are behind many of these social media quizzes. They collect, use and profit from the personal information you share. Many of the social media quizzes ask the same questions your financial organizations use for security purposes to verify your identity when you need to change your password or access your account without a password. Once you take these quizzes, you can't take back the information you provide.

3. **Conversations can be misinterpreted**
   Conveying tone using text-based communication platforms such as social media can be challenging and has the potential to lead to miscommunication. Communication style can be altered with prolonged use.

2. HOW CAN I PROTECT MY CHILD'S PRIVACY ONLINE?

There are two kinds of online privacy; 1) Personal Privacy – refers to your child's online reputation. It allows children to control when, how and how much information is revealed about them on the internet; and 2) Consumer Privacy – also known as customer privacy refers to the data companies can collect about your child during an online interaction or transaction. Both are important and a few simple steps can help parents and children keep their private information private when using internet.

Use privacy settings and review them frequently

All social media platforms offer privacy settings. The companies usually keep them off by default. You can adjust and enable the ones you want. Sit down with your kids and go over their privacy settings. The safest privacy setting to use on Facebook is "Only Me", which means you're the only one who can view it and Facebook is not allowed to share it. Also, check your app settings on Facebook to see what you've agreed to share with each app.

When your child gets a new device or signs up for a new website or application, establish your privacy preferences. Follow directions during initial set up. Although it might not be practical to read through every Terms of Service contract, it's a good idea to remind kids to be aware of what information they are agreeing to share before they start using applications, websites, or devices.

HOW CAN PARENTS MONITOR THE PRIVACY OF THEIR CHILDREN WHEN THEY ARE SURFING ONLINE?

Use two-factor authentication

This allows you to authorise only certain devices to access an account. It increases your security and prevents others from logging into your account even if they have your password.

Deleting old accounts and updating your passwords

Hackers can get to you through your defunct social media profiles. To find old accounts, Google your name; you'll be surprised at what you find. If you can find it, anyone else can, too. Don't forget to update your passwords.

Children must be aware of information shared online

Teach children the definitions of address, phone number, birth date and other personal information. It's important they understand the basics of good online behavior and the impact and potential repercussions of posting or commenting online

Restrictions protect your children

Legal restrictions help to protect your child's consumer privacy and ensure they are using age-appropriate websites and applications.

3. WHAT IS CYBER BULLYING?

Cyber bullying is bullying in digital spaces over digital devices like cell phones, computers, and tablets. It can occur through SMS, email, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. It includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behavior.

Examples of cyber bullying can include sending mean texts to someone; pranking someone's cell phone; hacking into someone's gaming or social networking profile; being rude or mean to someone online; spreading secrets or rumors about people online; pretending to be someone else to spread hurtful messages online; sharing private images of someone to other audiences.

Cyber bullying can escalate quickly and involve a lot more people than face-to-face bullying. Cyber bullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it.

Effects of cyber bullying

Online bullying can feel as if you are personally being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can be long term and affect a person in many ways, such as mentally — feeling upset, embarrassed, stupid, even angry; emotionally — feeling ashamed or losing interest in the things you love; or physically — tired (loss of sleep) or experiencing symptoms like stomachaches and headaches. The feeling of being laughed at or harassed by others can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyber bullying can lead to people taking their own lives. If you think you're being bullied, the first step is to seek help from someone you trust like parents, a close family member, another trusted adult, or a professional counselor.

If the bullying is happening on a social platform, block the bully and formally report their behavior on the platform itself. Social media companies are obligated to keep their users safe.

Collect evidence –text messages and screen shots of social media posts –to show what's been going on. For bullying to stop, it needs to be identified and reporting it is key. If you are in immediate danger, contact the police or emergency services.

Tips for internet safety and preventing cyber bullying.

- Know your technology. If your children are allowed to carry cell phones, or work with other technologies, learn how to use them yourself. They can teach you about the technological devices or application they have in their possessions. Take an interest in your children's online world.
- Set reasonable limits. Help your children learn to make responsible decisions about using technology by establishing guidelines and controls when necessary. Investigate all features of the technology they use. Cell phones with internet access should have the same guidelines and safety measures as those for household computers.
- Know your children's online friends. Help children learn the difference between a real friend and a friendly stranger. Monitor their virtual friendships. Instruct them never to meet online friends- only friends in person.
- Talk with your kids if you suspect they are being bullied. Changes in your child's behavior and attitudes can signal that they are being bullied at school or online. Victimized children are more likely to have difficulty sleeping, headaches, nervousness, stomach aches, and make excuses to avoid going to school.
- Help kids understand the difference between tattling and reporting. Tattling is when you tell something to get someone in trouble. Reporting is getting someone help to keep them safe. We must help children speak up when they are being victimized or witness someone else being victimized.
- Show your children you love them and will protect them. Children who are bullied are at risk of mental health problems, such as depression, anxiety, diminished self-esteem, and social withdrawal.

4. USAGE OF PHONES – HANDSETS SAFETY FEATURES; APPLICATIONS

Smartphones provide access to emails, online games, music, applications and social networking sites. They can also be used to take and send photos and videos. Other devices such as tablets, gaming devices and other media players can also connect children to the online world. Decide whether you are happy for your child to have a mobile phone or device that links to the internet. Always consider your Child's age and maturity and what it will mean for them to use it safely. Some risk-taking activities children may be engaging in online:

Sexting

Electronic device must not be used to send or forward sexually explicit text or photos. This is called 'sexting.' Once an image is sent, there is no control over what happens to it or who else sees it. It could be online forever. Sending nude or sexual photos of themselves or others under 18 can be classed as possessing and distributing pornography. This can cause serious harm and have serious consequences.

Games and applications

Games and applications can be great educational tools that build skills and a sense of achievement, as well as being lots of fun. However, it is important for parents to know the content of the games and applications being used. Some applications are labelled, 'educational' but are not much more repetitive activities. The best applications are those giving children a chance to experiment and try out their own ideas, e.g., creating drawings or music.

Advertising and product information

Many applications contain advertising, and it can be hard for young children to tell the difference.

Application purchasing

Real purchases can be made from inside the application which normally cost a lot to purchase a new application online. Simulated gambling is particularly risky for children as exposure at a young age can make it more likely they will gamble when older.

Violence and problem game use

Games with graphic violent or sexual content are linked to emotional problems, particularly in younger children. Children exposed to violent media may think it is OK to be aggressive, be insensitive to others being hurt, or become scared of their world. Lead by example and do not play violent games in front of children. Children are quick to spot double standards. You may need to be firm when limiting violent games as some children like these the most.

5. GENDER EQUALITY, DISABILITY AND SOCIAL INCLUSION

Social media has an important role in awareness and advocacy on gender and disability issues.

The internet can be used to link people to health and support services in response to requests for help and support. Ensuring that devices and internet data are equitably accessible helps to share information and knowledge in inclusive ways for the benefit of all users, including young people.

Online safety for children and adolescents is directly affected by gender beliefs and attitudes in the broader community. The internet also creates new vulnerabilities, particularly for girls and children with disabilities. The experiences and uses of online technology are not same for girls and boys, and the level of interaction and interest in being online also changes across different age groups. These interactions, interests and time spent online also affect parents differently, and the ability of parents to be supportive.

The internet is sometimes used as a platform to spread images of girls and boys in abusive and harmful situations. Online content and activities can reinforce harmful and abusive behaviors in real life situations. Intentionally exposing young people to this content is a form of virtual gender-based violence, whether it is used to make direct threats of physical and/or sexual violence or to encourage others to harm children. Helping children stay informed about online safety involves open discussion about the potential harm of internet use so that they are confident to report abusive behavior.

Parental fears about the online safety of their daughters are understandable but can also become barriers for supporting girls to access the internet as a useful educational and social tool and means of communication, and to encourage their aspirations to pursue education and careers in science, technology, engineering and math (STEM) fields. Supporting girls to use the internet with confidence helps to ensure online safety while enjoying the positive benefits of ICT.

The Lukautim Pikinini Act (2015) explicitly elaborates on measures to ensure the protection and privacy of each child. It stresses the importance of parental/guardian consent when using or sharing a child's image or information. It also prohibits employers and organisations to use children for exhibition and exposure without parental consent. Parents' awareness of their obligations under the Lukautim Pikinini legislation will help them to support the online safety of their children.

Disability and Social Inclusion

Children and young people with disabilities can be held back from using online technology due to fears of cyber bullying or internet safety. Parents may feel they do not know enough to keep their children safe. They may think not being online is the safest option. It is important to consider benefits children with disabilities can gain from being connected. A disability inclusive approach means not only protecting the person but helping them exercise their rights to communication safely and without discrimination. They must be protected from cyber harm just like anyone else.

6. CYBER SAFETY AT WORK AND AT HOME

Think twice before clicking on links or opening attachments

Even if an email looks like it is from someone you know. Do not reply to the email because the sender's identity might have been compromised.

Verify requests for private information

Verify the identity of the requester when requested to provide private information– even if it appears to be somebody you know. Con artists are clever in how they collect information to steal information and identities. Regularly check your financial statements and credit reports.

Protect your passwords

Never reveal your passwords to anyone. Make your password long, strong, unique and use multi-factor authentication (MFA) wherever possible. Use different password for different accounts and do not let websites and applications remember your passwords.

Keep your device, browser and applications up to date

At home, consider an automatic software updater and periodically restart your devices to ensure that updates are fully installed.

Back up critical files

Store backups in physically separate location from the originals and periodically test them. For critical work files, use storage options that are approved. For personal files, save a backup on a separate drive (cloud or encrypted USB) to securely store it.

GENERAL CYBER SMART TIPS

- Contact site administrator to have bullying content removed
- Report bullying to the school if it is coming from another student and report any serious threat to local police
- Get support for a young person if they are very upset
- Set up parental controls for phone usage and internet access for children under 18
- Disable in-application purchases so phone bills are controlled
- Advise children not to give away personal details to people they know or trust offline
- Turn off the phone's location settings when using it
- Create a family media agreement with tech-free zones such as cars, bedrooms, and meals.
- Teach your child how to filter information online and navigate fact from fiction
- Delete sensitive information when it is no longer needed
- Never provide personal or financial information to an unsolicited email, SMS, phone calls or websites even if they appear to be legitimate
- Do not open links or download anything from an unauthorized site
- Learn to spot signs of a secure site. Secured sites have URLs that start with https:// and should have a padlock icon in the browser frame
- Report any suspicious activities to relevant authorities.