

Resource Sheet – Cyberschool.ie

We hope you all enjoyed your Cyber Safety Workshop. The following will help you stay safe whilst online. We hope to see you all again next year.

1. Antivirus Software

- Ensure your Antivirus Software is up to date – If you use Windows O/S explore Window Defender, it's free. Within your organisation, this maybe different. Please check and understand the procedure for work laptops.
- With personal machines, if you are using paid antivirus, you can remove via the control panel and also search online for the removal tool to clear register files.

2. System Updates.

- Configure O/S to install updates automatically. Patches and New Features – Google if you don't know-how.

Windows Update



Updates available

Last checked: Today, 09:38

2021-09 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)

Status: Pending download

Download

[View optional updates](#)

3. Scams and Social Engineering

- Social engineering scams may build the trust of their target, using their alleged position to persuade people to drop their guard and provide confidential information to gain access to data.
- Avoid falling foul of phishing attacks, Avoid Typosquatting, Make Secure Online Payments, Have a Strong Password, Back up Data to the Cloud.

 <p>Avoid falling foul of phishing attacks</p> <p>Do not click on suspicious links, banners, provide your password or download software from an untrusted source (emails, messages). <u>E.g. BOI Scam</u></p>	 <p>Avoid Typo squatting</p> <p>Use correct URL</p>	 <p>Device Health</p> <p>Make Secure Online Payments</p> <p>Check for 'https' or use a secure payment provider <u>e.g. PayPal</u></p>
 <p>Spam Filters</p> <p>Provided by Email provider.</p>	 <p>Passwords</p> <p>Use 2-step authentication. Don't use one password for all apps.</p>	 <p>Back up Data to the Cloud</p> <p>Avoid being held at ransom</p>

4. To understand any of the above area it simple. Just head to Youtube and find a 3 to 4 minute clip to educate yourself.
5. Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised
 - a. <https://haveibeenpwned.com>
6. **Browse Yourself** – Stick your details into a browser and see what you can find!
 - a. Name
 - b. Email Address
 - c. Phone Number
7. **Irish Law** - Harassment, Harmful Communications and Related Offences Act 2020
 - a. <http://www.irishstatutebook.ie/eli/2020/act/32/enacted/en/print>
8. **Understanding Settings (Apps)!**
 - a. After the presentation, you now understand the importance of the Apps setting. Google these for individual Apps, use YouTube to aid you to know how to stay protected.
9. **Reclaim your Data.** Discover where your personal data is and manage your digital footprint. You decide where you want to keep your data and where you don't. <https://saymine.com/>
10. **Understand your organisation AUP** – Acceptable Usage Policy.
11. **Video Resource** – This allows you to understand specific areas and initiate discussions with your students.
 - a. <http://computingatschools.ie/cyber-safety-resources/>
 - b. Password cas2020

Educate Students

School's aim...(keep students and teachers safe)

Education students to

- Increase awareness, class lessons and discussions
- Grow Empathy
- Grow Resilience
- Facilitate Internet Safety Day- Let Students drive discussions and engineer chosen activities. Most effective when message comes from their peers.
- Recognise that sharing intimate content is illegal for minors <17
- Encourage students to Report concerns
- Encourage critical thinking (evaluate ideas to form healthy judgements)

WHEN DISUCSSING CYBER SAFETY (IN CLASS)

Suggestions:

- Become aware of any related issues in your class before starting
- Assess students' emotional state before and after discussions
- Inform students that disclosures indicating underage sexual activity, will be reported to the Designated Liaison Person
- Provide opportunities for students to come to you outside of class
- Inform the principal of any major concerns or findings from class discussions

WHEN DISCUSSING CYBER SAFETY (IN CLASS)

Suggestions:

- Be comfortable approaching the subjects. Learn from students
- Use resource videos as a lead into areas and allow open discussions
- Facilitate students to develop their own strategies for raising awareness (Posters, campaigns, videos)

Understanding Internet Safety for Children

Threats to children's internet safety include invasions of privacy, cyberbullying, sexting and harassment. Options to protect your children include parental controls, apps and tracking software.

But the most effective way to keep your kids safe is to talk with them about online risks, how to avoid them and how they can come to you when something goes wrong.

NAME OR LOGO

Understanding Discussing Internet Safety with Your Teen

Teaching your children about the online risks they may face and how to avoid or report threats is one of the most important steps you can take to ensure their safety online.

But first, you have to understand those risks for yourself. This means keeping up-to-date on the latest technologies, apps and social media trends. It can be challenging, but it better prepares you to talk to your kids about what to expect online.

NAME OR LOGO

Understanding

Online Dangers to Discuss with Your Kids

- Dangerous or inappropriate websites
- Malware and how it can be downloaded onto computers and phones
- Cyberbullying
- Online frauds and scams – Understand Privacy Setting
- Sexual predators – Stranger Danger

You'll also need to keep an open dialog with your kids. Let them know you are looking out for their safety and be sure to listen to their questions and concerns.

NAME OR LOGO

Understanding

How to Set Rules

- Setting clearly defined rules and explaining the reason for each rule and the hazard it protects against can help your child understand potential risks .
- Be consistent

NAME OR LOGO

Understanding

Common Rules

- Never give out personal information YAPPY
- Do not post photos on public site
- Do not chat with strangers online
- Do not respond to insulting, hurtful or bullying messages
- Never agree to meet someone you befriended online
- Understanding what is appropriate and not.
- Being able to talk – Has your Child a Cyber Buddy?

NAME OR LOGO

Understanding

How to Teach Your Kids to Use Their Smartphones Responsibly

- Set rules.
- Set up password protection.
- Update the operating system.
- Tell your child not to download new apps without your approval.
- Talk about location services.

NAME OR LOGO

Remember We Are Here To Help!
Together We Get Better!