E-Safety for Parents Fundamentals

You don't know what you don't know!

Hannah Wright

STEM and CyberFirst Ambassador
Founder and CEO of CirKits Ltd®

Topics

- **Basic E-Safety:**
  - Scams and viruses, what they are and how to prevent them
- **Parental Controls for Devices:**
  - Tools available on Apple and Android
- **Parental Controls for Gaming Consoles:**
  - Tools available for Xbox, PlayStation and Switch
- **Awareness of Games and Social Media:**
  - Multiplayer games such as Fortnite, COD and ROBLOX including microtransactions and DLCs (Downloadable Content)
  - Social media such as TikTok, Facebook and Snapchat, in app, pop up adverts
- **GLOSSARY**

Expectations for these workshops

- Structure of each topic is – What it is, Examples, Advice, Links

- Information is advisory to help you prepare
- Communication, communication, communication!
- Relaxed session, from one parent to another!
- **You don't know what you don't know! – Its okay to ask!**

Basic E-Safety - What is a Scam?

A Scam is when someone tricks you online to take your money or information.

These scams can be:

- ✓ **Fake ads** for free games or gifts or vouchers
- ✓ **Messages or emails** asking for personal details
- ✓ **Fake contests** with big prizes but hidden fees

Your personal information is the most valuable asset you have online.
Scammers can use this data to either sell to other scammers or use it to steal money from you.

Basic E-Safety – Examples of Scams

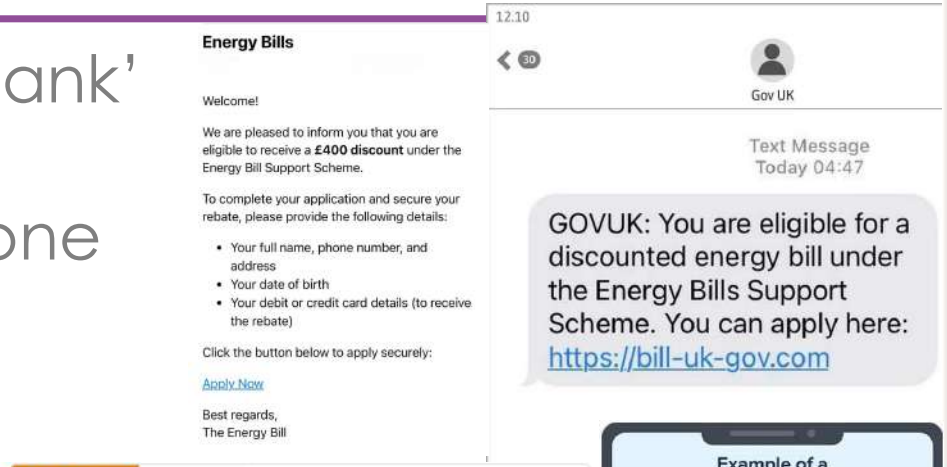
Email scams from a ‘bank’

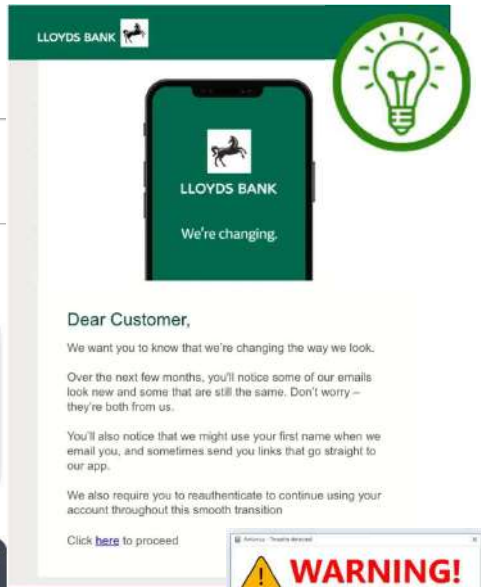
Messages on your phone

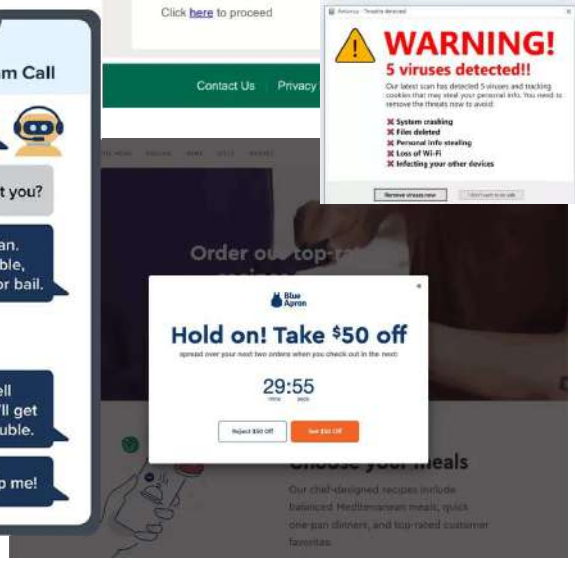
Fake pop-up adverts

Fake products

AI scam – new scam







Reinwood Infant & Nursery School, Parental Workshop, © CirKits Ltd, 2025

Basic E-Safety – How to prevent Scams

It is very difficult to stop every scammer from contacting you as your information is already online.

But there are a few measures that can help:

- ✓ **Look for spelling mistakes in ads and hover over the "click here" links and you can see the address it will take you to.**
- ✓ **No bank will ask for your account details. If unsure, ring up the bank branch using the number on their website. For example, https://www.barclays.co.uk/**
- ✓ **If it is too good to be true, it probably is!**
- ✓ **Click on the X straight away and block or ignore**
- ✓ **Never share passwords outside your household**

Basic E-Safety – Useful links

https://stopthinkfraud.campaign.gov.uk/

https://www.gov.uk/report-suspicious-emails-websites-phishing

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/prevent-personal-fraud/

https://www.moneysavingexpert.com/shopping/stop-scams/

https://www.youtube.com/watch?v=yazlGC_Os5Q

https://www.youtube.com/watch?v=R12_y2BhKbE

https://www.youtube.com/watch?v=U7tbJVSInvo

https://www.ceopeducation.co.uk/parents/articles/parents-guide-to-cyber-security/

Basic E-Safety - What is a Virus?

A computer virus or a bug is a type of malicious software designed to spread from one device to another by attaching itself to files or programs.

These viruses can be:

- ✓ **Corrupt your data**
- ✓ **Steal information**
- ✓ **Make your computer unusable**

There are a variety of different viruses that can infect your device and from many sources. Criminals create viruses for financial gain, vandalism, demonstrate security gaps or for fun!

Basic E-Safety – Examples of Viruses

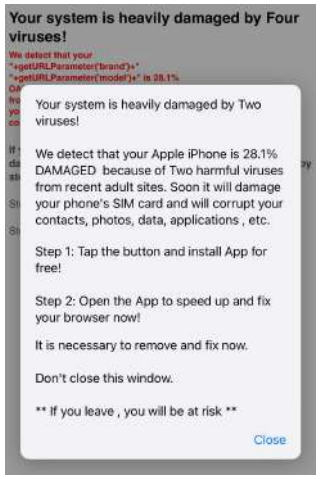
Worms – Copy themselves hundreds of times harming your computer

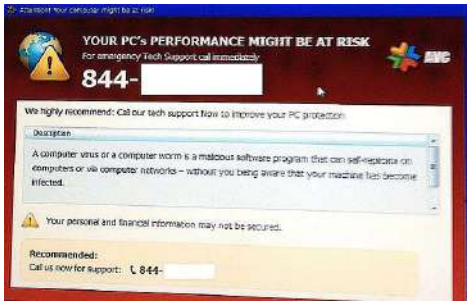
Trojans – pretend to be a trusted file but then infect your computer

Ransomware – corrupt your files and then ask for money to fix them

Spyware – collects information from your computer and send it to someone else

Scareware – tricks you to buying their software because you 'need' it





Basic E-Safety – How to prevent Viruses

To prevent viruses online using your laptop or computer, you can:

- ✓ **Install and run anti-virus software and make sure it is updated regularly**
- ✓ **Don't open any attachments you are not expecting**
- ✓ **Make sure your anti-virus software also has malware (malicious software) prevention too for added security**
- ✓ **iPhones and Android phones do not need anti-virus apps because iOS has very tight security features and Google Play has built-in security features in their store.**
- ✓ **If you are downloading apps NOT from these stores, you will need to download anti-virus apps to keep safe**

Basic E-Safety – Useful links

https://support.google.com/google-ads/answer/2375413?hl=en

https://www.ncsc.gov.uk/collection/using-online-services-safely/defending-online-accounts-from-malware

https://www.itgovernance.co.uk/blog/how-to-prevent-malware-attacks-8-tips-for-2023

https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it

https://www.youtube.com/watch?v=6mMZFoXbKqI

https://www.youtube.com/watch?v=EHqXMxY4_Nk

If you are wanting to download anti-virus software, go to the genuine website of that company. For example, https://www.mcafee.com/, https://uk.norton.com/

TIP: the s in https means it is a secure website, be careful with websites with only http

Parental Controls Introduction

Parental controls are tools designed to help Parents manage and restrict children's access to content and activities online.

A good perspective when explaining parental controls for a child (especially a teenager) is that you are not 'policing' their activities or restricting their freedom but creating a responsible environment for them to be free and explore safely. You are supporting healthy online habits.

A great example is **"Online Stranger Danger!"** to explain the safety measures when you're out and about, this should be the same as online.

There are many safety measures for Parents but the main take-away is regular open and honest conversations with your child about their online experience, potential risks and responsible behaviour.

Parental Controls for Devices

When we talk about devices in the home, these are:

- ✓ **Smartphones – iOS and Android**
- ✓ **Tablets – iOS and Android**
- ✓ **Laptops and PCs**
- ✓ **Gaming Consoles – XBOX, PlayStation and Switch**

We will be focusing on Smartphones and Tablets for this section as they are similar systems in layout and accessibility.

Links will be added for Laptops and PCs for more information and Gaming Consoles will be looked at later.

Parental Controls for Devices on iOS and Android

Google Family Link: Allows you to manage app permissions, and control screen time, approve or disapprove apps before they are installed and monitor your child's device usage.

Apple's Screen Time: This feature lets you set age-related restrictions for content, app purchases, privacy settings, restrict explicit content, purchases, and changes to privacy settings.

Kids Mode: On Android devices, you can switch the phone to Kids Mode, which restricts the phone to only the apps they are allowed to have access to.

Content & Privacy Restrictions on iOS: These settings allow you to control access to the device's microphone, location services, and Bluetooth connections and prevent apps from sharing your child's data.

Parental Controls for Devices on iOS and Android

To maintain trust and a safe environment to navigate online:

- ✓ **Open and honest communication with your child.**
- ✓ **When they are on their tablets or phones, 'spot check' to see what they are doing in a supportive way.**
- ✓ **Check the settings menu first on your device first before downloading safety apps. A lot of the safety features can be turned on through the settings menu without the need for another app.**
  An example is Kids Mode for Android is in the settings menu.
- ✓ **If you need to install safety apps on your phone and your children's devices, make sure you install from Google Play (Android) or App Store (iOS and Apple), so you know they are from a secure location.**
- ✓ **Don't install third party apps unless they are from a trusted source.**

Parental Controls for Devices on iOS and Android

https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/

https://safety.google/families/

https://www.staysafeonline.org/articles/parental-controls

https://www.internetmatters.org/

https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online

https://www.youtube.com/watch?v=6Z_lPERv4xY– how to use Google Family Link App

https://www.youtube.com/watch?v=JB8SXTC2c5s – how to set up iPhone parental controls

You can search for questions if you are unsure for specific devices on https://support.apple.com/ and https://support.google.com/.

Parental Controls for Gaming Consoles

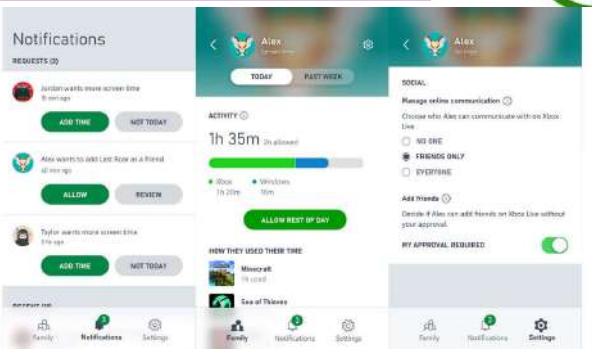
Keeping children safe while playing console games is as important as when they use handheld devices. It's important to note that consoles also offer built-in settings that can help you manage and control gameplay to create an enjoyable and safe gaming experience.

The consoles we will be discussing are primarily:

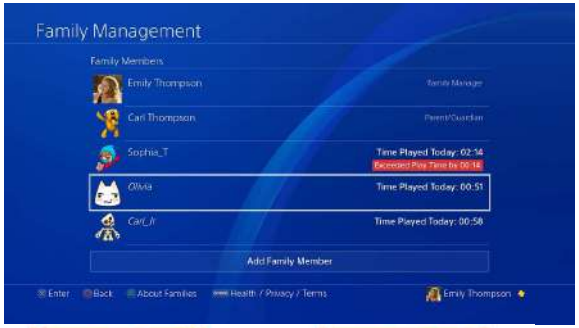
- ✓ **Microsoft Xbox One**
- ✓ **Sony PlayStation 4 (PS4)**
- ✓ **Nintendo Switch**

Parental Controls for Gaming Consoles

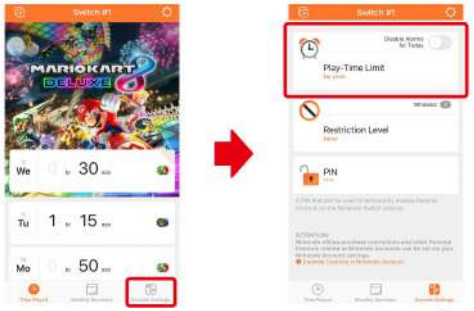
Xbox One: Set up a family group and manage child accounts using Xbox Family Settings app and Xbox Live account through the console settings, where they can restrict content, limit Xbox Live access, and set daily or weekly screen time limits and limit who they speak to online.



PlayStation 4: Provides robust parental controls that allow parents to manage and restrict their children's gaming activities using PlayStation Network account. These controls include time limits, content access, spending limits, and who they can speak to when playing online.



Nintendo Switch: Offers various parental control options that can be managed with the free Nintendo Switch Parental Controls App. These controls allow parents to restrict or monitor their children's activities, including setting time limits and controlling access to content based on age ratings



Parental Controls for Gaming Consoles

To maintain trust and a safe environment to navigate online:

- ✓ **Open and honest communication with your child.**
- ✓ **Make sure the console is in an environment where there is a lot of foot traffic making it easy to do 'spot checks' and take an interest in their online activities.**
  - ✓ **For the Xbox, use the Xbox Family Settings app.**
  - ✓ **For the PlayStation, go to Settings>Parental Controls>Family Management on console**
  - ✓ **For Nintendo Switch, use the Nintendo Switch Parental Controls app or the controls from the console**
- ✓ **You can set a passcode to your console to prevent unauthorised changes to the parental controls**

Parental Controls for Gaming Consoles

https://www.youtube.com/watch?v=03bAayBtcb0 – parental controls for the Nintendo Switch
https://www.youtube.com/watch?v=BVXJAX68LMs – Parental Controls app

https://www.youtube.com/watch?v=XIPKQdVy3kg - parental controls for the Xbox
https://www.youtube.com/watch?v=kN36zubUojA – Xbox Family Settings app

https://www.youtube.com/watch?v=Z-Mi2Ej72Fk – parental controls for the PS4

https://parentzone.org.uk/article/setting-up-gaming-consoles

https://www.internetmatters.org/parental-controls/gaming-consoles/

https://www.ofcom.org.uk/cy/online-safety/protecting-children/parental-controls-for-games-consoles

https://www.xbox.com/en-GB
https://www.playstation.com/en-gb/
https://www.nintendo.com/en-gb/

Awareness of Games and Social Media

Gaming and social media can be fantastic tools for connecting with others. However, some games, social media, and ads have raised concerns about their suitability and safety for children.

Such concerns include:

- ✓ **Violence and adult themes or offensive language**
- ✓ **Cyber bullying and exposure to harmful behaviours**
- ✓ **In-app purchases and financial risks**
- ✓ **Scams that include malware disguised as game mods and hackers**
- ✓ **Impact on self esteem, mental health and addiction**

This happens on many apps, games and devices. You need to be aware of the dangers and continue to have open conversations with children about safety.

Awareness of Games and Social Media

This is a large topic. Due to the feedback from the Internet Safety Day presentation and feedback from teachers and students, our focus is:

Multiplayer games:

- ✓ **ROBLOX** – exposes children to adult content as it is not rigorously checked or moderated for age rated games, in-game purchases called "Robux", microtransactions, cyberbullying, user generated content makes it difficult to regulate harmful material or behaviour.

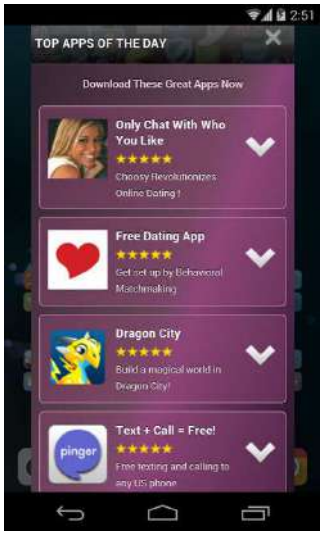
- ✓ **Call of Duty** – 18 rated game due to mature language, realistic violence, microtransactions and adult themes. These include mutilated corpses and drugs. Children connecting with strangers leading to inappropriate language, cyberbullying, toxic behaviours such as aggressive addicted habits.

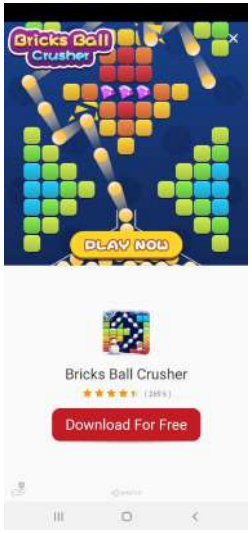
Awareness of Games and Social Media

Social Media:

- ✓ **TikTok** – exposes children to adult themes such as sexual material, collects data without user permission, adverts, TikTok shop, cyberbullying, addictive with shorter videos leading to 'doom scrolling' (constant flicking through videos), online predators and abusive.
- ✓ **Snapchat** – Exposure to unfiltered and inappropriate content, difficult to monitor with disappearing messages, pressure to constantly share and maintain 'Snapstreaks' and location sharing that can be exploited
- ✓ **YouTube –** Autoplay feature that can lead to unchecked screentime and over exposure to inappropriate videos, frequent ads before, during and after the videos that can lead to financial burden of purchasing YouTube Premium. Over hyper-stimulating videos with unrealistic acting, influencers and quick-cut editing.

Awareness of Games and Social Media





Other concerns:

- ✓ **In-app purchases** – the app advertised as free, will ask for payment later
- ✓ **Pop-up ads** – ads that pop up with a game demo can collect your data, frustrating gameplay to watch more ads, ads itself can be inappropriate

Awareness of Games and Social Media

To maintain trust and a safe environment to navigate online:

- ✓ **Open and honest communication with your child.**
- ✓ **Check each game that your children are playing for the age rating and the type of game app they have installed.**
  - ✓ **On a console, uninstall or return any games that are inappropriate. If this is not possible, install parental controls and make sure they are not on their own when playing on the games to create a safe environment.**
  - ✓ **On a tablet or phone, install parental controls and go through the apps and delete games that are inappropriate straight away. Blame it on updates!**
- ✓ **You can easily monitor game and app updates and DLCs (downloadable content) by checking the descriptions, such as security fixes or new features. Parental controls help you decide if they are necessary. Many DLCs are expensive and not always needed for gameplay.**

Awareness of Games and Social Media

https://www.nspcc.org.uk/keeping-children-safe/online-safety/access-to-technology-for-different-ages/

https://saferinternet.org.uk/guide-and-resource/parents-and-carers

https://www.ncsc.gov.uk/section/advice-guidance/you-your-family

https://www.bbc.co.uk/teach/topics/cp440njz78zt

https://saferinternet.org.uk/guide-and-resource/social-media-guides

https://learning.nspcc.org.uk/online-safety/online-safety-for-schools

https://www.youtube.com/watch?v=pWzhE8fUi7E – ROBLOX information

GLOSSARY

Microtransactions	Small payments made within a game or app to buy virtual items, such as in-game currency, upgrades, or cosmetic items.
In-app purchases	Any purchase made within an app, often for additional features, content, or virtual goods.
DLC (Downloadable Content)	Additional content for a game that can be downloaded after the initial purchase, often adding new levels, characters, or game modes.
Updates	Changes made to software or games to fix bugs, improve performance, or add new features.
Demos	A trial version of a game or software that allows users to test it before purchasing
Cyber bullying	Using technology to harass, threaten, or embarrass someone.
E-Safety	Measures to protect users from online risks, such as cyberbullying, scams, and inappropriate content.
Game Mods	Modifications made by players to change or enhance a game, often adding new content or features.
Hackers	Individuals who gain unauthorised access to computer systems or networks, often to exploit or harm them.
User generated content	Content created and shared by users, such as videos, posts, or game levels.
AI (Artificial Intelligence)	Technology that enables machines to perform tasks that typically require human intelligence, such as learning, problem-solving, or decision-making.

And finally…. Now you know!

Having open, regular and honest chats with your child helps to create a safe environment for them to voice their concerns and for you to voice yours.

https://www.ceopeducation.co.uk/
Thinkuknow by NCA-CEOP: Offers guidance for parents and children on online safety

https://www.nspcc.org.uk/keeping-children-safe/online-safety/
NSPCC: Offers comprehensive guides and tools to help parents manage online safety issues

https://saferinternet.org.uk/
UK Safer Internet Centre: Provides tips, advice, and resources to help keep children safe online

https://saferinternet.org.uk/report-harmful-content
UK Safer Internet Centre Reporting Tool: Allows users to report harmful content found online.

Hannah Wright

STEM and CyberFirst Ambassador
Founder and CEO of CirKits Ltd®