Internet and E-Safety Risks

Contents

Internet and E-Safety Risks

General Safety Concerns

With the ever-increasing development and accessibility of technology, our children are being introduced and exposed to it very early in life. Whilst the benefits of the technology in children's learning is very much beneficial in preparing them for life outside education, there are risks. This document will describe several issues and risks but also assist in addressing them. See some of the topics below;

- Online gaming
- Cyberflashing & AirDrop
- Coerced Online Sexual Child Abuse
- Livestreaming
- Misinformation
- Online bullying

Online gaming

Online gaming is hugely popular with children and young people. Annual research conducted by OFCOM shows that gaming is still one of the top activities enjoyed online by 5–16 year olds, with many of them gaming on mobile phones, games consoles, tablets or computers.

Cyberflashing

'Cyberflashing' is where somebody digitally sends sexual images or pornography to an unsuspecting person. Due to the nature of channels used to send these images, the victim will not know they have been cyberflashed until they have actively opened the notification or gone into the app.

AirDrop is a file and image sharing app, bespoke for Apple devices, which enables users to drop content for nearby devices to accept or reject. Cyberflashing most commonly occurs using Apple AirDrop, as strangers can send images to a victim's phone without having their details saved. Cyberflashing can also occur through file sharing apps and social media, especially if the perpetrator has the victim's details.

Coerced Online Sexual Child Abuse

Children can be groomed, coerced, or encouraged into sexual activities online. This is known as self-generated child sexual abuse content, or first person produced images and videos. It's where sexual images or videos of children are captured via a webcam or camera-enabled device. There is no physical presence of the abuser, and the child is often in their own bedroom or bathroom. Whilst these images can be the product of grooming, blackmail, and coercion, they could have also been originally voluntarily produced by the child, but then shared with others without the child's full knowledge or consent. Any child with unsupervised access to the internet is potentially at risk.

Livestreaming

Livestreaming is when an individual or a group of people broadcast themselves or others to an audience online in real-time. Many social media platforms offer a livestreaming feature that is available to anyone but often used by gamers, celebrities, or influencers to communicate with a chosen audience. Livestreaming can be an enjoyable way to share content with followers but can also present risks around privacy and coercion as well as potential harm towards those watching.

Misinformation

Misinformation or 'Fake news' is online content that can mislead or provide false information towards a particular topic. Stories can often be fabricated to cause panic or concern and heavily rely on users to critically determine what is trustworthy or not.

Internet and E-Safety Risks

Online Bullying

Cyberbullying, or online bullying, is when someone uses the internet to bully someone else. The Cambridge dictionary defines cyberbullying as 'Someone who uses the internet to harm or frighten another person, especially by sending them unpleasant messages

Source(s): https://saferinternet.org.uk/

Smart Technology

Smart technology is now very common in household environments. They are all connected to the Internet and should be considered regarding Esafety. Some examples are below;

- Smart TV's
- Smart Speakers
- Smart Home control systems - Nest
- Smart Plugs
- Wi-Fi enabled camera's – baby monitors.
- Smart appliances

Smart TV's

Our home network is only as strong as its weakest link and with dozens of items connected to your router there are plenty of areas for a hacker to attack. If your TV isn't secure, it could allow a hacker access to your router and if that's compromised than anything else on your network could be at risk.

The TV isn't exactly devoid of personal data though. App and wi-fi login data, as well as card details in some cases if you've rented a film or signed up for an app through your TV, are at risk if your TV is insecure.

Hackers can hijack a TV to display their own content and they can do far worse than force you to watch Keeping up with the Kardashians over and over. They could put up fake versions of app login screens to trick you into entering your card details and steal your information.

Smart Speakers

Are Smart Speakers Safe?

Smart speakers provide incredible convenience, but some features may leave you open to cyberthreats and unwanted data sharing. Being aware of the known concerns with smart speaker privacy and security can help you stay safe. Once you understand the risks, you'll be able to take precautions against weaknesses in your devices, network, and behavioral usage.

Smart Speaker Privacy Issues

The privacy of smart speakers is a worry for many users, especially when it concerns how their conversations are handled. Generally, a speaker from the big three manufacturers — Amazon, Google, and Apple — is safe to use. But an "always-on" microphone does come with some risks and ethical concerns.

Accidental Smart Speaker Recordings

Smart speaker microphones are always listening by design. This is how they are able to hear your requests at any given moment and passive listening is always on (unless the mic is muted). Recording

only happens if the wake phrase is used (like “OK Google” or “Alexa.”) The device records to capture and process your command. However, accidental recordings are possible. For example, other words can be misheard as activation phrases, like using “OK booboo” instead of “OK Google.”

Smart Speaker Recording Storage and Human Reviewing

Recordings are the only audio stored, and they are always stored locally on the device. However, they are also shipped off to the corresponding cloud servers for processing. Depending on your privacy settings, you may find that your recordings are being used in several ways.

Many users never actually change default settings — leaving the manufacturer to decide. This stored audio is usually used for voice service improvement, and only a minor percentage of these recordings are reviewed by humans to develop their voice recognition further AI. Other uses for voice data may include building advertising profiles on users.

Policies around recordings and their usage have been shifting due to the increase in smart speaker popularity. However, privacy is still a concern, even for the three main smart speaker manufacturers (Amazon, Google, and Apple).

Smart Home Control Systems

Smart homes use devices which can connect to the internet and contain small computers enabling them to be remotely controlled. These devices might be as small as a coffee maker or as large as your entire heating system.

What makes them different from your traditional TV remote is that they use internet protocol to link up, and they're all connected through a hub. That might be your home network router, or your smartphone.

Unlike the TV remote, these devices can collect and store information on your usage, habits, and preferences — either on the device or on the network. All that data makes your smart home a potential privacy risk, and every device you add to the network adds a new privacy concern.

Wi-Fi Enabled Cameras/Baby Monitors

Any product that is connected to the internet without proper security could in theory be hacked by someone with malicious intent, including a baby monitor. The likelihood of it happening is thankfully still relatively low, but there are disturbing stories of baby monitors being hacked by strangers who are then able to project their voice through the monitor's speaker.

Additionally, footage from hacked baby monitors has ended up on rogue websites, enabling strangers to watch it.

Smartphone Concerns

Cyberbullying

A growing issue, cyberbullying is the harassment of individuals through electronic channels such as mobiles, online forums, gaming chat rooms and social media. Examples of cyberbullying could include hostile text messages, the spreading of rumours, or the sharing of embarrassing photos. As cyberbullying takes place online, it’s a challenge for parents and or teachers to become aware of this issue unless a child speaks up about it.

Internet and E-Safety Risks

Unprotected Use of Social Networking

Stranger danger isn't just an issue offline. Predators can easily hide their identities online while asking probing questions about a child's friends, family and interests.

Access to Unsuitable Content

The internet is home to many things, including inappropriate and adult content. Studies have shown that 1 in 10 children between the age of 8 and 11 who go online have seen something nasty or worrying. Even playing age-inappropriate games can expose children to swearing or images of violence.

Eye Strain from Mobile Phone Usage

Too much screen time can lead to burning, itchy or tired eyes in children. While children can better adapt to the high-energy, short-wavelength blue light that devices emit, too much exposure can lead to long term problems. These long-term side effects can include headaches, fatigue, blurred vision as well as head and neck ache.

Decreased Attention Span

Mobile phones, televisions and other devices are rewriting how our brains work – for adults and children alike. It has been proven that children with prolonged access to screens can develop a decreased attention span. This is unsurprising, given that modern technology means their brains are being trained to continually expect and receive new information.

Link - https://www.premier-education.com/news/the-parents-guide-to-mobile-phone-health-safety-for-kids/

Internet and E-Safety Risks

Social Media

Did You Know?

- For context, as of Dec 2022, total worldwide population is around 8 billion
- The internet has 5.473 billion users – as of June 2022
- There are 4.62 billion active social media users
- On average, Gen Z and millennials have 8.5 social media accounts per user
- The average daily time spent on social is 147 minutes a day
- 71% of small-to-mid-sized businesses use social media
- $1268.7bn is expected to be spent on social media advertising in 2023.

The facts: 13–17-year-olds are on social media

- 71% of all teens are using more than one social networking site
- 41% of all teens use Facebook
- 20% of all teens use Instagram
- 11% of all teens use Snapchat
- 6% of all teens use Twitter

Data Types Collected by Social Media Companies

- **Personally identifiable information**: your first and last name, age, and email address. This may also include any information you share about your job, employment/education history, relationship status, religious views, political views, health data, and your interests. This type of information is subject to special protections under the **Privacy Act 1988**.
- **Location**: where you live, the places you like to go, and the businesses and people you're near to. Your current location is also tracked (if you've got Location turned on) and this includes the location of a photo or the date a file was created.
- **Texts and calls**: this may include contacts in your address book, call logs, and your SMS log history.
- **Your social interactions**: what you post, content you consume, the people you interact with, accounts you follow, hashtags, Facebook groups you joined, and any pages you're connected to and how you interact with them across all platforms.
- **Device information**: the name of your mobile operator or Internet Service Provider (ISP), language, time zone, mobile phone number, IP address, connection speed, and, in some cases, information about other devices that are nearby or on your network.
- **Financial information**: this includes your credit or debit card number and other card or payment information, as well as your billing, shipping, and contact details.

Social Media Tracking

- Interesting Fact – **Instagram shares 79% of a user's data with third parties**.
    - Browsing history
    - Current location
    - Contacts
    - Financial information – if you've purchased through the app

Link - https://xiphcyber.com/articles/social-media-tracking
Social Media Interesting Facts - https://sproutsocial.com/insights/social-media-statistics/

Internet and E-Safety Risks

Protection & Monitoring in Education

Schools in the UK are required to meet digital and technology standards, as directed by the UK government. Does Jersey follow the same? Emailed Education…

Protection in Education Environments

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

Digital and Technology Standards in Schools and Colleges

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges