The latest digital trend growing in popularity for our children are apps on their phone or tablet that look like one thing but are secretly hiding another purpose. They first became particularly popular in 2016. However, children are becoming more and more familiar with 'secret' photo hiding apps, where an app which looks relatively ordinary is actually a hidden gateway to private photos and videos. These apps allow their users to hide images, videos and notes within the app which is also passcode protected. One of the most common types of hidden app used is a 'fake calculator' app however many others are also available.

What parents need to know about HIDDEN PHOTO APPS

MAY HIDE 'SEXTING'

The most common use for the apps is to hide 'sexting' images which young people may be sending or receiving. This problem is growing rapidly amongst students, and from an increasingly early age. Not only is sexting dangerous, but it is illegal when it involves a minor even if both the sender and receiver are underage. By storing and sending these images, young people should be aware that they are committing a crime.

PRIVACY RISK

If you are aware that your children are using the app, you should read the small-print in the usage policy/terms and conditions to ensure the developers do not have access to any of the images stored on the device. If the photos are linked to a cloud storage, then the images stored are also in danger of being released if the application is compromised/hacked.

ENCOURAGE IMPULSIVE BEHAVIOUR

Young people tend to act more impulsively if they believe that their behaviour will go unnoticed and remain secret, so often they will produce content for these apps thinking that it will be safe. Let's face it, how many adults read all the small print in the terms and conditions, so why would we expect our children to.

BYPASS PARENTAL CONTROLS

Although these apps are not specifically 'targeting' their advertisements towards children, they can generally be used by anyone over the age of 4. This means that these apps will not be blocked automatically by parental controls. Whilst online platforms, such as Apple, have removed these apps on numerous occasions from their app store, due to their popularity and potential profitability for creators, they continue to be produced and find their way into the stores or available for download.

FAKE/DECOY PASSWORDS

Some of the most secure apps that are available offer the ability to set-up a decoy feature as an added layer of security. This allows the user to provide a fake password which, when used, directs people to a decoy folder containing content of the user's choice or just stock photos. The real password provides access to the secret folder within the app.

National Online Safety®
#WakeUpWednesday

Safety Tips For Parents

TRY TO REMAIN VIGILANT

There is a natural human instinct to believe that what we see on screen is real and accurate. If you are concerned that your child might be using secret apps, you may want to look at their phone. The search feature on a device can be used to type keywords such as 'secret', 'hidden' and 'photo vault'. On iOS, this can be done by swiping down on the home screen to open a search bar. If the app appears and says 'Open' then the app is installed. If it says 'Get' then it is not installed. On an android device, you can go to the apps menu and use the search bar at the top of the screen.

QUESTION THE AUTHENTICITY OF DUPLICATE APPS

You should be aware that almost every mobile device will have pre-installed apps, such as notes and calculator, so the first major warning sign would be to look for duplicates of these apps. By default, the pre-installed apps are almost always displayed on the first page of the home screen.

Default iOS Calculator

Examples of Hidden Calculator Apps

DISCUSS THE DANGERS OF 'SEXTING'

Ensure your child is aware of the dangers of sexting, and how it is illegal to keep or distribute images of minors. Try to talk to your children in a positive way a nd encourage them to take control of their online persona and what they are posting to others. Remind them that they always have a choice and that they can say no to anything that makes them feel even the slightest bit uncomfortable.

LOOK OUT FOR IN-BUILT 'HIDDEN' FEATURES

iPhones have the option to lock notes within the default Notes app. Users can paste images into a note file and lock it using Touch/Face ID and a password. In addition, iOS allows their users to move images to a Hidden folder in the photos app. When an image is moved to the hidden folder, it is removed from the 'All Photos' folder. To find this folder, open the 'Photos' app, scroll down and click 'Hidden'. Users may also create folders to try and hide the app on their home screen or on a second or third page. If you see a folder on your child's device, ensure you check each page for hidden apps.

CONTROL APP USAGE

If your child's iOS device is linked to your Apple ID account, you are able to set a password for downloading apps which only you know. This will mean every-time your child tries to download an app, they will need your password to do so. If you do not have access to your child's Apple ID, you can delete the app without a passcode. This will delete any images stored on the app and will not be recoverable, even if the app is redownloaded.

Meet our expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

SOURCES: https://www.businessinsider.my/apple-pulls-private-photos-calculator-from-app-store-2018-4/, https://smartsocial.com/private-photo-calculator-app/, https://offspring.lifehacker.com/is-your-teen-hiding-sexting-photos-in-a-fake-calculator-1829529749

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

THE DEEP WEB & THE DARK WEB

What is it?

'The Deep & The Dark Web'

While the deep web and the dark web are not the same thing, they do overlap significantly. The Deep Web refers to pages that are not indexed, which means that most search engines (Google, Bing etc) won't return them to you after a search. The dark web is part of the World Wide Web that is only accessible by installing and using special software. It is the unregulated part of the internet; no organisation, business, or government oversees it or can apply rules. This is why the dark web is commonly associated with illegal practices.

Know the Risks

Unmonitored access

Children and young people often dive into the Dark Web using their devices, unmonitored, unregulated, and unnoticed. Whilst children may access and use the Dark Web and/or the Deep Web, a child's curiosity may result in the access and viewing of very inappropriate, unacceptable, and illegal sites, forums, and communities.

Inappropriate content

Children can access sites with indecent images, sites selling drugs and/or weapons; however, this is also the case for the Surface Web. The possibility of users infecting their devices with malware is higher when visiting the Dark Web also.

Online predators

Online child predators are more likely to interact and groom children on the Surface Web than the Dark Web. However, once contact is made, interaction can continue within the Dark Web.

Safety Tips

Question their motives

If you believe your child may be using TOR or accessing the Deep or Dark Web or asks if they can download the software, ask them why they are using them rather than using the surface web. Children should be able to access everything they need via normal web browsers.

Check devices

Check all devices for the TOR (or I2P / Freenet) software and delete any unknown browsers. Monitor your child's online purchases. If you know that your child has been using TOR to access the Dark Web, watch for any unusual mail or packages delivered to your home.

Talk about the dangers

Ask your children what they already know, and then openly speak about the Dark Web. Part of the attraction to the Dark Web may be the mystique and curiosity associated with it so it's important to educate your child about the dangers and how it can be misused by criminals.

How they Work

TOR Software

The most common software used is called TOR (The Onion Router). TOR is a web browser that keeps your identity a secret by hiding your IP address. This means that users largely cannot be tracked while browsing the dark web. Most dark web users use a search engine such as DuckDuckGo, which protects users' privacy. TOR can bypass school internet filters.

Three Web levels

The surface web is the internet we are familiar with; we use it to run businesses and connect with family, friends, and customers. Deep websites emphasise protecting users' privacy. People who need to keep their identities private use this to share sensitive information. The dark web is focused on illegal activities and services. However, unless you carry out unlawful acts, it is not illegal to use the dark web or TOR.

Our Expert

Jonathan Taylor

Jonathan Taylor is an online safety, social media and online grooming expert who previously worked as a Covert Internet Investigator with the Metropolitan Police for over 10 years. He has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, apps and platforms.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

HACKING

What are they?

'Hacking'

Hacking is the unauthorised attempt to exploit a computer system or network. There are different types of hackers who are usually categorised under 'hats'. White hat hackers are known as ethical hackers and have no intent to cause harm, but rather will penetrate a system to identify weaknesses. Black hat hackers or Crackers are those who intentionally hack to gain unauthorised access to harm or steal sensitive information. Grey hat hackers act more for fun and exploit security weaknesses in computer systems to raise awareness of issues for recognition, political awareness, or financial reward.

Know the Risks

It's Illegal

Hacking is often portrayed in the media as dark, dangerous and cool. However, young people attempting to hack are often unaware that they are actually breaking the law. It is a criminal offence to access or modify data stored on a computer system without permission which is often punishable by law and could lead to a criminal record.

Theft of Personal Data

Cyber criminals collect information in a variety of ways and will try to entice children to an attractive website through offers of free media or products. They will often hide malware in downloadable content which can take over your computer, steal personal data and pass it on to third parties. This can lead to financial and reputational damage, embarrassment, blackmail or even identity theft.

Inappropriate Content

If a child is using an unsecure network, free WiFi or hasn't implemented any necessary security measures, they could leave themselves open to being hijacked by other users. This could leave them open to being sent or exposed to inappropriate images or videos, especially via social media platforms or communication apps.

18+

Safety Tips

Talk about the risks

Encourage discussion with children about what hacking is and what the consequences of being hacked are, as well as those risks if they were to become involved in hacking themselves. Discuss the legalities and the dangers of not keeping accounts and passwords secure.

Be security aware

Talk to children about being security aware. Advise them to seek your help when filling out online forms and make sure they know what to keep private when filling in online profiles such as their date of birth, phone numbers and addresses. Make sure children know the risks of connecting to open/free Wi-Fi.

Tighten protection

Make sure that you have implemented necessary security measures across all devices and apps your child uses. Use passwords that are made-up of at least 8 characters consisting of symbols, numbers, uppercase and lowercase letters. Create different passwords for different accounts and use two-factor authentication where possible. Turn off browser pop-ups and location services in apps when not in use and make sure your anti-virus software is up to date.

Further Guidance

Provide support

Try to make sure that child know that they can feel comfortable talking to you. If a child's account has been hacked and they have suffered embarrassment or loss of private information, they may become withdrawn, secretive or emotional so it's important that they know that you will be there to help and can offer them support and advice to help rectify the situation.

Change security controls

If you suspect that a child's account has been hacked or compromised, disable it, change passwords for other accounts that may be linked to it and use a password manager to increase the level of security. If you believe a device has been hacked, update and run your anti-virus software. You might also need to wipe the device and re-install everything.

Seek further help

If you notice that a child is starting to show a deep interest in hacking activities or mentions the dark web or TOR browsers, have a conversation with them about the laws they may be breaking and the possible dangerous consequences. Seek advice from local organisations who may have more specialist knowledge and can provide further guidance.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Online Relationships Series

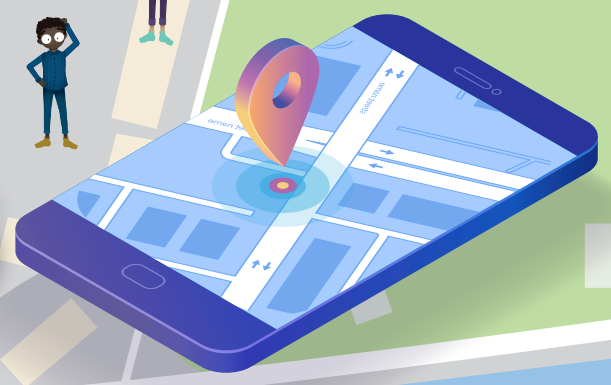
NOS Online Relationships

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

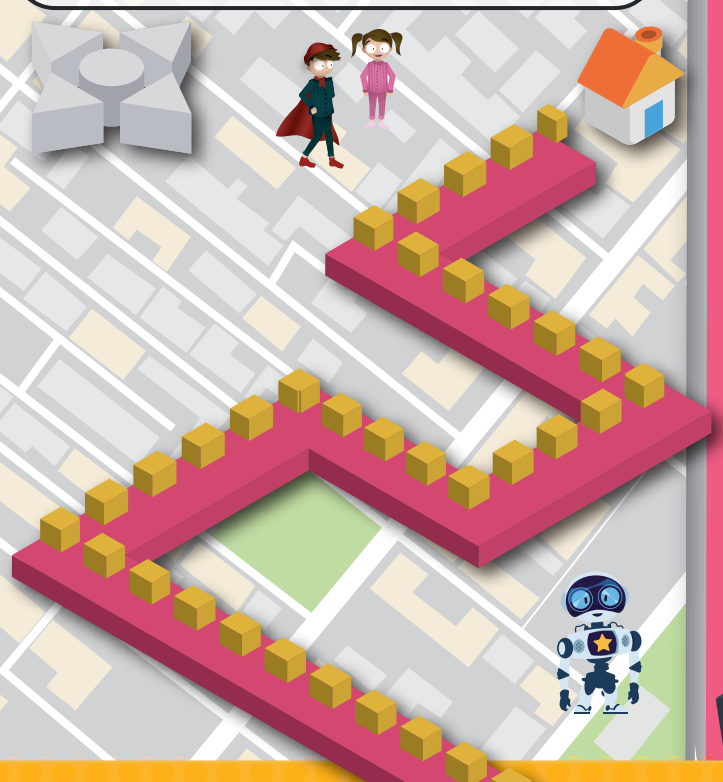
LOCATION TRACKING



What is it?

'Location Tracking'

Location tracking has always been a fundamental part of the way mobile phones work, the most basic element of which is the ability to triangulate a device's position in relation to a mobile network's radio masts. As smartphones became popular, Global Positioning System (GPS), Wireless networking (Wi-Fi), and Bluetooth Low Energy (BLE) technologies complemented this, any one or combination of which can now feed highly accurate location data via any app on that device.



How Does it Work?

Based on consent

In the UK, data protection laws require that access to a person's personal data (including their location) is based on consent. In principle, the same protection applies to children even when parents use location tracking to keep tabs on them although this is a grey area for under-16s.

Location sharing apps

As well as being built into Google's Android and Apple's iOS software, location sharing is often a feature of popular apps, for example Snapchat's Snap Maps, specifically designed to appeal to children, or WhatsApp Live Location. These usually require the user to turn the feature on.

Wi-Fi surveillance

Although location tracking is associated with GPS, in urban areas Wi-Fi is more important. Tech companies have built up highly accurate pictures of the location of Wi-Fi networks in towns and cities. As a smartphone moves within range of these networks, it's possible to accurately calculate that device's location.

Know the Risks

Non-consensual monitoring

Whilst location tracking has many benefits, a number of apps have recently emerged that allow location data to be sent to third parties. This inevitably raises the risk of location tracking via apps being used, without consent, to keep tabs on someone's whereabouts.

Frequently visited locations

A function of mobile operating systems is to document location history, which can provide someone with access to all past locations a child may have visited since location permission was granted. Anyone with access to a child's phone could establish where they go and when an build up a pattern of where they are likely to be at any particular time of the day.

Stalking apps

Whilst these apps are often illegal, gathering evidence for prosecutions can be difficult. Stalking apps are designed to monitor someone's smartphone communication and location without their knowledge or consent and could be used as part of harassment or stalking activity.

Safety Tips

Disable when not in use

It's possible to turn off or limit location sharing on mobile devices, but this will also disable other features such as street navigation. It may be better to explore which apps are using location sharing and in what ways and that young people know to turn if off when the app is not in use.

Discuss the risks

Young people are often unaware that location sharing is powerful and open to abuse. Talk to them about how it can be misused and discuss the importance of keeping their data private. Tell them to never provide others with unauthorised access to their phone and to always keep it locked when not in use.

Talk about location monitoring

Remind children that smartphones are a powerful technology that can monitor and record everywhere a person goes as well as all their communication. Talk about the law and about what they can and can't do to others and that monitoring someone else's location without their consent is a huge invasion of their privacy.

Our Expert

John Dunn

John E Dunn is a hugely accomplished cybersecurity expert who has edited and written for numerous computer and technology magazines since the early 1990s, most recently Which Computing, The Register, Computerworld and Naked Security. He is the co-founder of Techworld and has featured on BBC TV/radio as well as CBC Canada.

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

Online Grooming is when someone befriends and builds an emotional relationship with a child and communicates with them through the internet with the intent to commit a sexual offence. This type of victimisation can take place across any platform; from social media and messaging apps to online gaming and live streaming. Often it involves young people being tricked, forced or pressured into doing something they wouldn't normally do (coercion) and often the groomer's goal is to meet the victim in a controlled setting to sexually or physically abuse them. In some cases children may be abducted or have long-lasting psychological damage.

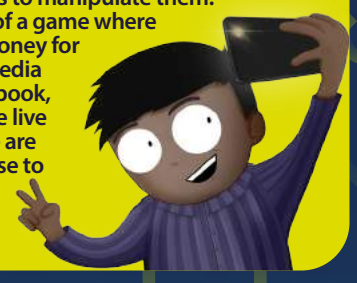
What parents need to know about ONLINE GROOMING

CHILDREN ARE MOST VULNERABLE

Unsurprisingly children are often most at risk as they are easy to target and unlikely to question the person who is engaging in conversation with them. Groomers will use psychological tricks and methods to try and isolate them from their families and friends and will often choose to target more vulnerable children who may be easier to manipulate. Predators will stalk apps and websites that are popular with young people and will use a 'scattergun' approach to find victims, contacting hundreds online to increase their chances of success.

LIVE STREAMING CONCERNS

Predators may use live video to target children in real-time using tricks, dares or built-in gifts to manipulate them. Grooming often takes the form of a game where children receive 'likes' or even money for performing sexual acts. Social media channels, such as YouTube, Facebook, Instagram and Snapchat, all have live streaming capabilities, but there are many apps which children can use to live stream, including Omegle, Live.me, BIGO Live, YouNow and many more



ANYONE CAN BE A PREDATOR

The internet has made the ability to interact with strangers online easy. Many sites and apps are reliant on individual users entering their own information when signing up. However individuals can remain anonymous if they choose to enter inaccurate information and many online predator cases are due to groomers using impersonation techniques. However, often the greater threat comes from adults who 'hide in plain sight', choosing to befriend young children without hiding their real identity.

CAN BE DIFFICULT TO DETECT

Unfortunately, most children find the 'grooming' process (before any meeting) an enjoyable one as the predator will compliment, encourage, and flatter them to gain their trust, friendship and curiosity – 'a wolf in sheep's clothing' scenario. This often means children fail to disclose or report what is happening. If the groomer is also previously known to the child, their family and their friends, then this can make detection even harder.

FROM OPEN TO CLOSED MESSAGING

Online predators may contact their victims using any number of ways including social media, forums, chat rooms, gaming communities or live streaming apps. Sometimes there is little need to develop a 'friendship /rapport stage', as the victim has already shared personal information online and is communicating openly with others. Children may also be prepared to add other online users they don't know so well to gain 'online credibility' through increasing their friends list. Predators will often seize this opportunity to slowly build a relationship and then move their conversation with the child to a more secure and private area, such as through direct messaging.

EMOTIONAL ATTACHMENTS

Online predators will use emotive language and aim to form close, trusted bonds with their victims through showering them with compliments and making them feel good about themselves. Often victims will refer to them as their 'boyfriends' or 'girlfriends' and it can be difficult to convince some young people that they have been groomed, often leading to lasting psychological effects.

National Online Safety®
#WakeUpWednesday

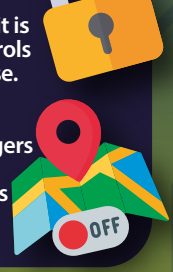
Safety Tips for Parents & Carers

IT'S GOOD TO TALK

It's unlikely that you can stop your child using the internet, nor can you constantly monitor their online activities, but you can talk to your child on a regular basis about what they do online. By talking openly with them about online relationships, they can quickly ascertain the kind of behaviour which is appropriate or inappropriate. Ask them whether they have any online friends or if they play online games with people they haven't met. This could then open up conversations about the subject of grooming.

CHECK PRIVACY SETTINGS

In order to give your child a safer online experience, it is important to check privacy settings or parental controls on the networks, devices, apps, and websites they use. Disable location sharing if you can. If you use location-sharing apps to check where your child is, remember that these could always be used by strangers to follow your child without their knowledge. Ensure that you check options so that location information is never shared with anyone except those they have permission to share with.



MONITOR SOCIAL MEDIA & LIVE-STREAMING USE

It's important to be aware of what your child is sharing on social media and with whom. Create your own profile and become "friends" with them or follow them so that you can monitor their activity. Similarly, always check on them if they are live streaming and implement privacy controls. Choose a generic screen name and profile picture that hides their identity. You may also feel more comfortable being present each time they live stream.

STICK TO 'TRUE FRIENDS'

Make it clear to your child that they should not accept friend requests from people they don't know and to verify friend requests with people who they do know. Encourage them to only interact and engage with 'true friends' i.e. those friends who don't ask personal questions such as close family and friends. Remind them to never agree to chat privately with a stranger or someone they don't really know and to never divulge personal information, such as mobile phone numbers, addresses, passwords or the name of their school.

DISCUSS HEALTHY RELATIONSHIPS

Talk to your child about what a healthy relationship looks like and how to detect someone who might not be who they claim to be. Explain that groomers will pay your child compliments and engage in conversations about personal information, such as hobbies and relationships. They may admire how well they play an online game or how they look in a photo. Groomers will also try and isolate a child from people close to them, such as parents and friends, in order to make their relationship feel special and unique.

BE SUPPORTIVE

Show your child that you will support them and make sure they understand they can come to you with any concerns they may have. They need to know they can talk to you if someone does something they are uncomfortable with, whether that is inappropriate comments, images, requests or sexual comments.

Meet our expert

Jonathan Taylor is an online safety expert and former Covert Internet Investigator for the Metropolitan Police. He is a specialist in online grooming and exploitation and has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, social media apps and platforms.

LOOK OUT FOR WARNING SIGNS

Child safety experts have identified key grooming patterns and advise parents to look out for:

- Secretive online behaviour.
- Late night internet or smartphone usage.
- Meeting new friends in unusual places.
- Becoming clingy, develop sleeping or eating problems or even bedwetting.
- Lack of interest in extra-curricular activities.
- Having new items, such as clothes or phones, unexplainably.
- Seem withdrawn, anxious, depressed or aggressive.
- Having older boyfriends or girlfriends.

Personal data is a strange commodity. Cyber thieves can buy huge quantities of personal data on the black market for very little, yet your own personal data is hugely valuable to you. If your personal data falls into the wrong hands, it could lead to identity theft, bank fraud or something even more sinister such as stalking. The severity of that threat is multiplied when it comes to the personal data of children, when threats such as internet grooming begin to emerge. The bad news is that children aren't always great at safeguarding sensitive information, which is why they need parents' help and guidance. That's why we've created this guide to show you how you can protect your own and your family's personal data.

What parents need to know about PROTECTING PERSONAL DATA

EVERY DETAIL IS KEY

Which info should you be wary of sharing online? Aside from the obvious, such as full names, date of birth and address, think of the type of information you're asked for when answering security questions for services such as online banking. The name of your first school, your mother's maiden name, the names of your pets, your favourite band. Data thieves will harvest as much of this information as possible, so don't make it easy for them by publishing it anywhere online.

SOCIAL MEDIA VISIBILITY

Social media sites, such as Facebook, encourage us to share sensitive information in order to build our online profiles. Many people are lulled into thinking that only their friends can see such information, but that's rarely the case. Such information can easily be shared with 'friends of friends' or even anyone searching for you online because privacy settings are opaque. Keep social media profiles to the bare minimum. If you wouldn't be comfortable hanging a sign with that information on your front door, don't enter it into social media sites.

DANGEROUS GAMES

Online games are a particular risk for children. Many of the most popular games – such as Fortnite, Minecraft or Roblox – have voice or text chat facilities, allowing them to talk to fellow gamers. Or, sometimes, people pretending to be fellow gamers. It's very easy for children to be seduced into divulging personal data such as their address, birthday or school. It's critical parents both educate children on the dangers on online chat in games and take safeguards to protect children.

IMPOSTERS AND PHISHING ATTACKS

Even if you're scrupulous about keeping your data private on social media, it's easy to be lulled into handing it over to imposters. There are two golden rules for you and your children to follow: 1. Never divulge personal information to phone callers, unless you can be absolutely certain you know who they are. 2. Never click on links or open attachments in emails or social media, unless you're 100% certain they are genuine. So-called phishing emails are growing ever-more sophisticated, with fraudsters able to replicate the exact look of bank emails and even include details such as account numbers and IDs.

THE RISKS OF PASSWORD SHARING

Password sharing – using the same password for multiple sites – is one of the easiest ways to lose control of your personal data. Hacking of major websites, including usernames and passwords, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, you're handing data thieves an easy route into your inbox, where they will doubtless find all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them reset the password on multiple other accounts. Don't share passwords; use password managers to create strong, unique passwords for every site.

National Online Safety®
#WakeUpWednesday

Safety Tips for Parents & Carers

LOOK OUT FOR LEAKS

Many security software packages have features that look for personal data leaks or prevent people from entering it into risky sites in the first place. For example, Bullguard Premium monitors dangerous sites for usage of data such as your email address, debit card numbers, passport number and more, and then sends you email alerts and details of how to take remedial action if it spots them being used. Such software also issues warnings if it sees personal data being entered into unprotected, high-risk sites.

KEEP DATA GUARDED

Don't give the thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email address such as davesmith1976@gmail.com – an immediate clue that you were born in that year. If you have a less common name than Dave Smith, thieves could immediately start using that information to cross reference against public records or other database breaches, allowing them to start building a profile of information about you. Likewise, don't use your date of birth in a password. If that's hacked, you've handed the thieves another big clue.

DON'T OVERSHARE ON SOCIAL MEDIA

The biggest threat to your child's privacy is you. Parents often overshare personal information on social media: full names, names of schools, children's birthdays, names of their friends. All of this can be easily gleaned to build profiles that could be used to groom your child in online games or in real life. Exercise extreme caution with social media posts concerning your children.

BE WARY OF SHARED NETWORKS/SYSTEMS

Avoid entering any personal data into a web browser when you're using public Wi-Fi (in a coffee shop or airport, for example) or when using shared computers. Shared Wi-Fi connections are much easier to eavesdrop on than your home network, especially if they are not password protected or the password is shared freely with customers. Don't do online shopping, banking or enter any logins/passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very easy for a browser to save logins that could be used by others.

PLAY SAFE IN ONLINE GAMES

Children must be taught to treat strangers in online games with the same caution as they would treat strangers in the street. Don't allow children to use their real name as their username in games to prevent imposters conning kids into thinking they are real-life friends, and only allow them to add friends in the game that they know in real life. Regularly ask to monitor your child's friends list in such games and ask them to identify who the players are. With younger children in particular, ask them to only use voice chat in family rooms, so that you can hear conversations.

Meet our expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as *The Sunday Times, Which?, PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *BBC Newsnight, Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues over the years.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about... PHISHING

What is it?

'Phishing'

Phishing is a form of cyber-attack where victims are targeted in the form of spoof emails, phone calls or texts. These are commonly carried out by an attacker posing as someone else to influence individuals into giving out sensitive data such as payment details and passwords. Phishing usually takes place via email, where the attacker manipulates a message to make it appear to be from someone else, therefore deceiving the victim into doing as they say. Hackers try to deceive you into downloading malicious code and will aim to extract small pieces of information at a time.

Know the Risks

Loss of personal data

If a young person has been the victim of a successful phishing attempt, hackers may gain access to their personal data and destroy/corrupt it. Some hackers may ask for a ransom in order to get files back, whilst others may simply destroy it or even publish it on the dark web.

Targeted phishing

If a hacker can trick children with a phishing attack, the chances are that they'll be back for more. They may begin asking for 'harmless' information, then move on to sensitive information such as passwords and entry codes. Many phishing attacks start with the attacker offering to help the victim with a common problem to build enough trust to ask for information such as passwords.

Hidden entry

If an attacker manages to successfully execute a phishing attack on a victim, they have essentially found a 'way in', or backdoor into their online security. Even if they do not notice any changes, the hacker may be monitoring/controlling their computer without their knowledge.

Safety Tips

Backup your files

Always create a backup of your files to an external hard drive or USB before any potential damage or destruction. If you regularly perform backups, you may only have to backup any files recently added/updated since the last backup.

Disconnect the device

If you think a child has been a target of a phishing attempt, firstly disconnect the device from the network by switching off the Wi-Fi in settings or unplugging the ethernet cable. Alternatively find the router and unplug it. This will prevent any malware from accessing any internet services.

Scan your system

Always perform regular and full malware scans; this will check for any potentially harmful programs installed on your computer. Scans are most effective when the antivirus is up to date so it's crucial to keep on top of the latest security downloads.

Check official websites

If you're unsure about a message you receive, don't click any links or follow any instructions. Check the official websites online and don't give out any personal information that you don't need to. Even if the message seems like it's from someone you know, if anything seems suspicious, or matches any of the criteria above, simply do not open it...

Look out for...

Suspicious URLs

Sometimes links and attachments aren't always what they appear to be and could send you to a site completely different to what was expected. Hovering over a hyperlink will display the actual website. Some links are shortened, so the actual website address is hidden behind a generic link, such as goo.gl/7fh28. Never click shortened URLs.

Odd sense of urgency

Cyber criminals will put fear in their victim's mind in an attempt to push them into giving away personal information. They may act as if they're trying to help create a false sense of 'trust' or pressure users into giving information 'before it's too late'.

'Too good to be true'

If you receive an email saying you've 'Won a new phone' or a 'Holiday Abroad', it is likely to be a phishing email. Hackers engineer emails and trick targets into believing they've won something, as it puts a false sense of trust towards the hacker.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

REMOTE ACCESS & REMOTE DATA DELETION

What are they?

'Remote Access'

Remote access, as the term suggests, refers to the ability to access a computer, such as a home computer or a machine that's connected to a school's network, from a remote location. Remote access can be set up using a local area network (LAN), a wide area network (WAN) or a virtual private network (VPN), and once established, it gives you full control over the device you're 'remoting' to. You can then run any applications and even open files on the machine.

'Remote Data Deletion'

Remote data deletion is related; this is a security feature that allows a network administrator, for example, to send a command that deletes data on a computing device. It is primarily used to erase data on a device, such as mobile phone or laptop, that has been lost or stolen so that if the device falls into the wrong hands, the data won't be compromised.

Know the Risks

Cyber-scams

Some popular scams employ remote access tools in order to infect your PC with malware and obtain financial details. These typically appear in the form of phone calls, where a company warns you that your computer has a security problem and promises to remote-in and fix it.

Privacy concerns

If your child is using remote access software and is also allowing others to access their computer, it could mean that they're potentially providing the remote user with access to sensitive information, such personal images or videos or even financial details.

Permanent loss

Remote deletion is a great way to ensure that if your device is lost or stolen, that the data cannot be compromised by others. However, if the data isn't backed up elsewhere and a remote wipe is completed, this can lead to permanent data loss which is irrecoverable.

Hacking risk

While many, typically paid-for remote access tools will encrypt remote sessions between the local and remote devices, some services don't offer such protections. This could leave any information passed over the service open to hacking and the theft of personal and private information.

Safety Tips

Protect your devices

Always protect your devices with the most up to date security software. While both Windows and macOS have built-in protections against malware threats, it's recommended that you implement additional measures, from firewalls to two-factor authentication (2FA).

Avoid public WiFi

If you or your child are using remote access software, it's always best to avoid using a public Wi-Fi hotspot. These are often open networks that are typically unsecure by nature, and prime locations for cybercriminals to gain access to your devices.

Read the small print

When you or your child are installing remote access software, it's important you know what you're downloading so that you know that your data will remain safe. You must make sure the service offers built-in encryption, complies with regulations (such as GDPR), and that it's fully compatible with the PC and mobile devices that will be connecting to it.

Backup data

You're never going to be warned prior to unexpected data loss, which is why it's critical to back up any important data - particularly if data ever needs to be wiped remotely. While this data can be backed up in the cloud, it's always advisable to have a physical copy too.

Conversation Tips

Talk about privacy

Remote access has long been a target for cybercriminals, and even if they don't feel at risk, it's important your child is aware of the security issues and knows how to maintain strong online privacy, be it through the use of strong passwords or multi-factor authentication. Always ensure they know never to let an unauthorised third-party gain remote access to their system.

Understand their usage

Always ensure you know what your child is downloading or how they are using their devices. If they're using remote access tools, it's important you're confident that it's secure. Talk to children about potentially using a reputable VPN to offer extra security and making their computers less vulnerable to hackers.

Our Expert

Carly Page

Carly Page is an experienced and highly respected freelance technology journalist, editor and consultant. Previously the editor of tech tabloid The INQUIRER, Carly now works as the news editor for Computer Shopper and IT Pro and writes for a number of publications including Forbes, TechRadar, Tes, The Metro, uSwitch and WIRED.

What parents need to know about SEXTING

18+

Sexting involves sending, receiving or forwarding explicit messages, images, or videos of a sexual nature. Although mobile phones are the most common vehicle for sexting, the term can also apply to sending sexually explicit messages through any digital media such as email, instant messaging, and/or social media sites. They can be sent to or from a friend, boyfriend, girlfriend, or someone your child has met online. Sexting is often described as the new flirting for children, but it is illegal for anyone under the age of 18. Some of the main platforms it occurs on are Snapchat, Tinder, WhatsApp, Facebook Messenger, Instagram and Kik.

IT IS ILLEGAL

Sexting is illegal if you share, make, take, or distribute an indecent image or video of a child under the age of 18. It is an offence under the Protection of Children Act (1978), the Criminal Justice Act (1988), and under section 67 of the Serious Crime Act (2015). Sexting or 'youth produced sexual imagery' between children is still illegal, even if they are in a relationship and any images are shared consensually.

PERCEIVED AS 'BANTER'

Many young people under 18 see sexting as 'banter' and an easy way to show someone that they like and trust them. Whilst it is a criminal offence, the reasons for taking and sharing can be very innocent and all part of growing up, understanding their own sexuality, and establishing a relationship. However, whilst most images and videos are taken and shared willingly, there can be unintentional consequences, embarrassment, humiliation, and emotional hurt.

FEELINGS OF REGRET

Although some children willingly exchange messages, images, or videos, many may regret sharing them after they've been sent. Once it's out there, there's no going back and your child may feel ashamed, vulnerable, or anxious about the imagery resurfacing later, especially if a relationship or friendship has broken down.

NO CONTROL

Once a photo or video is out there, there's no way of knowing how many people have saved it, tagged it, or shared it. Children like to show off to their peers and, suddenly, an image has gone beyond its intended recipient to classmates, friends, and even strangers. Once an image or video has been shared online, there's nothing to stop it being archived and repeatedly shared.

ONLINE BLACKMAIL OR BULLYING

Sexting can also expose young adults to the risk of being exploited by paedophiles or sexual predators, who then use images to extort additional photos, sexual favours, and sometimes money from victims. Your child may also feel pressured into sexting so they don't come across as boring, or think it's a way to show someone they care for them. They may feel under pressure to give in to repeated requests or feel obliged to share sexual messages and imagery which could then be used against them as a form of bullying or intimidation.

National Online Safety®
#WakeUpWednesday

Safety tips for parents

THINK ABOUT LANGUAGE USE

Teenagers often prefer to use the word 'nudes' to 'sexting'. One reason for this is the normalising of this behaviour; another is that most children always feel a sense of embarrassment when discussing any issue with the word 'sex' in it. Sexting an image could also be described as an 'inappropriate selfie'. Using this term with your child might make the discussion less embarrassing.

BLOCK & PARENTAL CONTROLS

Show your child how to use the block button on their devices and favourite apps to stop people sending them unwanted messages. You can also set up parental controls with your internet service provider or on your child's phone to stop them from accessing harmful content.

EXPLAIN THE REPERCUSSIONS

Let your child know that once they have sent a message, they are no longer in control of it and the messages, images and videos that they may intend to share with one individual may end up where the whole world can have access to them. Even if they completely trust someone, other people using their phone might accidentally see it. And, later in life, it may affect their online reputation, especially if universities, employers or future partners access the imagery.

TALK TO YOUR CHILD

Encourage open dialogue about appropriate information to share with others, both online and offline. Show that you understand that sexting can be about finding out about nudity, bodies and exploring their sexuality, but explain why it's important to think twice before sharing something. Show that you are approachable and understanding and discuss what a healthy and trusting relationship with a partner looks like.

DISCUSS THE LEGALITIES

Children and young people may not realise that what they are doing is illegal. Ensure that your child understands that when they are aged under 18, it is against the law for anyone to take or have a sexual photo of them – even it is a selfie and even when the activity is consensual.

LEARN HOW TO RESPOND

If an image has already been shared, either your child or you should speak to the person that the image was shared with and ask them to delete it. You can also use the report button on a website where the image was posted. Speak to your child's school as they may be able to confiscate phones if they know that they have sexual imagery stored. If you believe the child was forced into sending the message, report this to the police. You or your child can also report the content to a child protection advisor at the CEOP.

Meet our expert

Jonathan Taylor is an online safety expert and former Covert Internet Investigator for the Metropolitan Police. He is a specialist in online grooming and exploitation and has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, social media apps and platforms.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, ghints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about... WEBCAMS

What are they?

'Webcams'

Most commonly found embedded in laptop screens and smartphones, webcams are tiny video/still cameras designed to let you participate in video calls on services such as Skype and Zoom. They have become hugely popular since the start of the coronavirus pandemic, allowing homeworkers to chat with remote colleagues and helping friends and families stay in touch. However, there are many security and privacy risks associated with webcams that owners should be aware of.

Know the Risks

Hackers

Webcams are a prime target for hackers as they give attackers a highly intrusive eye into the victim's home. There have been several high-profile breaches where integrated laptop webcams or dedicated webcams have been targeted.

Malware

Malware often targets webcams, secretly giving hackers access to your computer's webcam without any visible signs that the camera is switched on. Such malware can arrive in email attachments or by clicking on rogue links on websites, and it can often install itself in the background without the user being alerted.

Access to strangers

Children can be naïve to the dangers of allowing strangers to access the computer's webcam. They may click through warning messages that grant access to the camera or they may willingly share the camera with people they meet online who are pretending to be children.

Blackmail

Webcams can be used for blackmail, even when the webcam itself hasn't been hacked. Fraudsters will claim to have webcam footage or stills of the victim whilst naked or accessing pornography and threaten to post such footage on social media or send it to employers if the victim fails to pay up. The fraudsters normally don't have any footage at all, but the threat is often enough.

Look out for...

The indicator light

It can be difficult to tell if your webcam has been compromised or is secretly capturing footage. If the little indicator light (normally green) next to the webcam is lit when you don't expect it to be, this could be a sign.

Camera permissions

Check the camera permissions on your computer to ensure no rogue or unnecessary apps have been granted access to the camera. Switch off any apps that don't need access to the camera. If you never use the webcam, you can bar all access to the webcam. Better still, cover it when not in use.

Unexpected saved folders

Another telltale sign of a webcam compromise is folders containing videos or photos taken by your webcam appearing on your computer. Malware will often save videos/photos on your machine before attempting to upload them to the hackers, who will then use them for blackmail purposes. Check your Photos and Videos folders occasionally for any unexpected files.

User Safety Tips

Explain the dangers to children

Talk to your children about the dangers of talking with strangers via webcam and tell them not to accept any video chat requests from people they don't know in real life. Keep computers in family rooms, so that children can't covertly use the webcam in their bedrooms.

Refuse & report

Do not pay anyone claiming to have captured embarrassing webcam footage of you. It's highly likely they don't have footage in the first place, and even if they do, paying them may encourage them to demand more money. Report the matter to the police and keep a record of any evidence you can.

Unplug webcams & update firewalls

Unplug external (USB) webcams when they're not in use. Make sure your computer is running up-to-date security software and that the firewall is switched on. This can thwart attempts to access your webcam remotely.

Our Expert

Barry Collins

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as The Sunday Times, Which?, PC Pro and Computeractive. He's appeared regularly as a technology pundit on television and radio, including on BBC Newsnight, Radio 5 Live and the ITV News at Ten. He has two children and has written regularly about internet safety issues over the years.