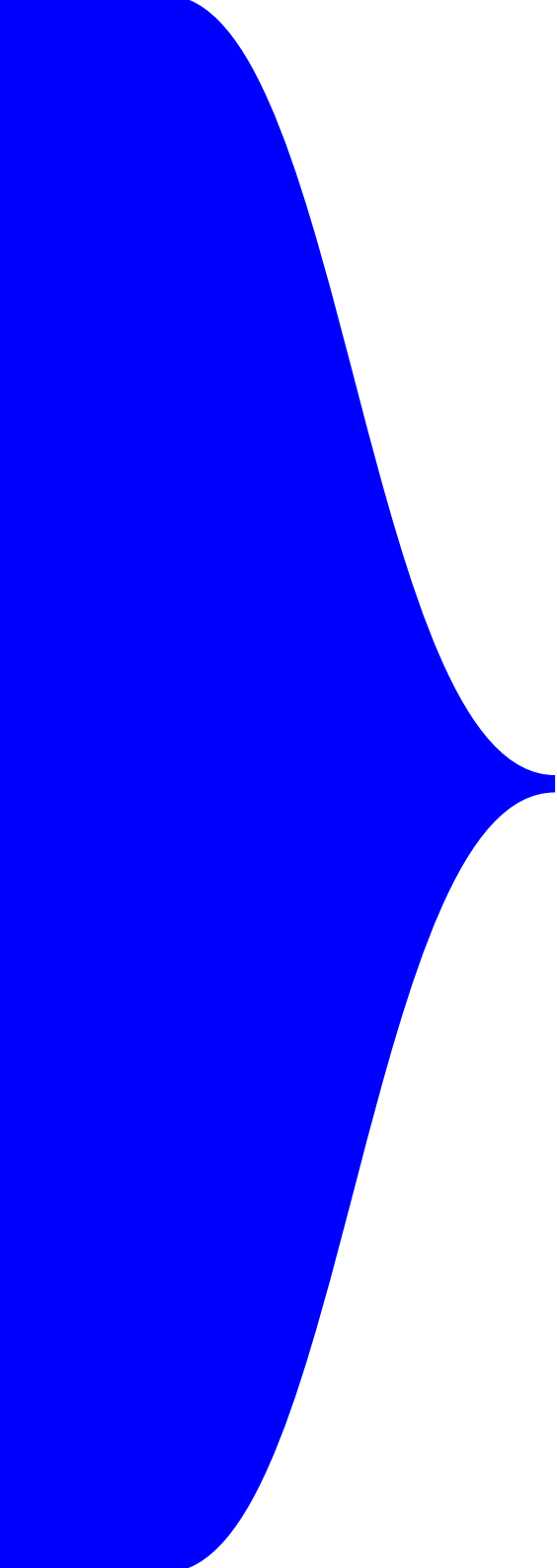
Begin

Cyber security at home

Helping to protect you and your family online

Bank of Ireland UK



Contents

Introduction

It can be hard to know where to start when it comes to protecting your home and your family from today's cyber threats.

Being connected is a part of our daily lives, whether it's talking to friends and family through apps or on social media, playing games, downloading music, looking up facts for a school project, sharing photos, shopping, or banking online. We all need to protect our important information so, to make things easier, we have created this guide to help you and your family enjoy the benefits of technology in a safe way.

The guide includes recommendations on practical steps you can take to help you interact confidently with technology and contribute towards your digital wellbeing. It is divided into three main sections:

- Common tactics used by cyber criminals
- Securing your home network
- Guidance for parents and carers

By securing our home networks and personal devices, and teaching both young and old family members about the importance of using devices responsibly and safely, we can help safeguard our families from scams and control unwanted content.

Stay safe.

Common tactics used by cyber criminals

Being connected in today's digital world can sometimes be risky. Read about the most common tactics cyber criminals use to get your personal information so that you know what to look out for:

What cyber criminals want

- To steal money
- To steal confidential information
- To cause disruption

What they might look for

- Passwords
- Your identity
- Your banking details

How they tempt us

- **Curiosity:** You've won!
- **Urgency:** Deadline 24 hours
- **Threat:** Account suspended
- **Fear:** I have your password

What to look out for – phishing emails and smishing texts

Cyber criminals send emails and texts containing links that may take you to a fake website, or attachments that once opened download malicious software to your device. They can look very realistic and may even contain real information about you or your personal interests. When it comes to phishing, remember, no topic is off limits. Sometimes the emails or texts might also contain a phone number that you think is legitimate but is in fact fraudulent, designed to trick you into sharing confidential information over the phone.

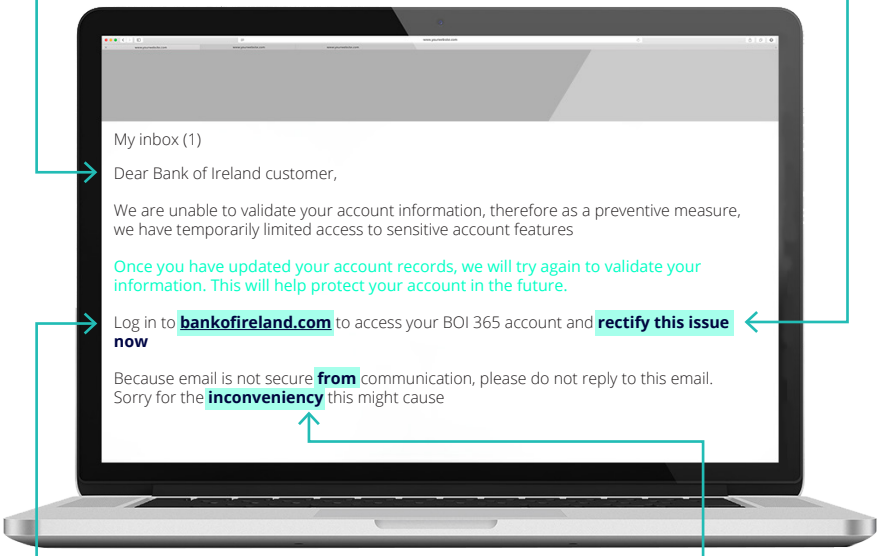
Phishing example

Unexpected emails

Unusual email sender address

Generic or unusual greeting

Urgent requests
Be cautious of any urgent requests e.g. "update details" or threats to "close your account". Verify first, using trusted contact details (eg use the phone number on the company's official website, or those provided on the back of your bank card etc), being careful not to use phone numbers quoted in the email as they could be fraudulent.



Unknown links or attachments
Hover over the link to see where it is bringing you. If in doubt, go directly to the website instead (do not click on the link).

Poorly written and/or badly displayed emails
Includes poor syntax and grammar, unusual signatory or no contact information.

Smishing examples

"Your account has been suspended"

Your registered phone number has expired and therefore we suspended your outgoing payments. Confirm your registered number at **https://neverclick/on-links**

"You've won a prize"

You have been selected to win 1000 pounds in the Lottery! (second round!) Click here **https://neverclick/on-links** to win! Hurry, access is limited.

"Your package couldn't be delivered"

Dear Customer, your item is out for delivery today. If you will not be home, call 078 XXX XXXX to agree alternative delivery arrangements.

"You have a tax refund"

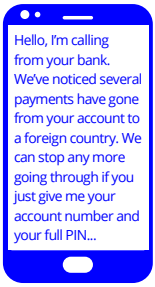
Your refund is now available. Refund amount GBP: 1479.15. Please check **https://neverclick/on-links**

DO NOT CLICK LINKS OR OPEN ATTACHMENTS YOU ARE NOT 100% CERTAIN ABOUT

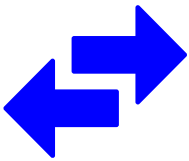
What to look out for – vishing calls

Unexpected calls from someone claiming to be your bank, credit card company or other trusted company (eg IT company, Revenue) who:

requests your full banking details or other confidential information

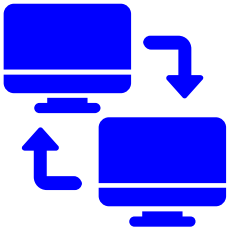


claims that your bank account has been compromised



asks you to transfer money out of your account

offers assistance after you have interacted with your bank or another company on social media



asks to take remote control of your computer so that they can 'fix' or upgrade it

THESE ARE JUST SOME EXAMPLES OF HOW YOU COULD GET TRICKED INTO GIVING AWAY YOUR INFORMATION. BE VIGILANT – DON'T GIVE AWAY PERSONAL OR BANKING INFORMATION. HANG UP THE PHONE, AND DON'T CALL BACK ANY NUMBER THE CALLER MAY HAVE GIVEN YOU

What you need to know

Here are some other ways cyber criminals might try to access your personal information or trick you into doing something for their gain:

Social media

What to look out for

Cyber criminals could try to use what you post on social media to steal your identity and access your accounts, or they might contact you pretending to be someone you trust.

What you can do

Check your privacy and security settings and control who sees your profile and what you post.

Limit how much personal information you share and only connect with people you know or trust.

Be suspicious of strange requests, even if it seems to come from a friend who claims that they need some money urgently or they need your bank account details.

Public Wi-Fi

What to look out for

When you access public Wi-Fi you can never be sure who has set up the network and you don't know who else is connected to it. Cyber criminals can intercept public Wi-Fi without you knowing and see everything you are doing online, including when you enter your payment details.

What you can do

Avoid using public Wi-Fi to check your bank accounts, make a payment or shop online. Use 3G/4G instead or wait to use a secure trusted Wi-Fi connection.

Money mules

What to look out for

Typically young people and students are targeted either by someone they know or through online advertisements or social media posts and recruited as money mules to allow their account to be used to receive (unknowingly) stolen money. Then they must either transfer it to another account, usually overseas, and keep some of the cash for themselves as 'payment', or withdraw the cash and pass it on to the money mule recruiter.

What you can do

Beware of requests to make quick and easy money. Do not allow someone to transfer money into your account for onward transfer to an account designated by them, in return for cash payment. By allowing your bank account to be used in this way, you are acting fraudulently and, if you are caught, the consequences can be serious.

Remember, if you are a Bank of Ireland customer, we will never:

- send you a link to the login page of our online banking channels
- ask you for your full 6-digit PIN (we only ever ask you to confirm 3 random digits of your PIN)
- ask you to transfer money out of your account to protect you from fraud
- ask you to click a link in an email with an urgent warning about suspicious activity on your account. (We may sometimes send you a text to verify a transaction on your account but we will never ask you to provide confidential information or click a link to verify a transaction)
- call you to ask you to make a payment to another account
- ask you to tell us any 'one-time password' or code that you have received from us by text

Always monitor your bank accounts regularly to check for any unauthorised activity.

Report suspicious emails or texts to **365security@boi.com**.

For more information on fraudster tactics and the latest fraud alerts, visit Security Zone at **bankofirelanduk.com/security**.

This guidance is standard practice across the global financial services industry.

Securing your digital home

Advances in technology create greater opportunities for us to stay connected – whether at home or on the move. With this convenience though comes greater risk from online fraud and cyber attack, so it's important that you take steps to help secure your home network, smart home appliances and mobile devices.

Secure your home network

Why is it important?

The first step to a cyber secure home is to secure your home network. This will help protect your information, including bank account information, user names, passwords, photos etc. from unauthorised access.

What can I do?

Go to your home broadband provider's website to search for further guidance on the following:

- **Check whether the provider uses a WPS** (Wi-Fi Protected Set Up) feature. This enables a Wi-Fi connection to your hub without needing to know the network name or password, which may allow someone to connect to your network without permission.
- **Change the Wi-Fi password to a strong password** only you know and change the wireless network name (or SSID) to something unique. (You will then need to reconnect all your devices connected to it). Default user names and passwords for Wi-Fi networks are generally known and can be shared by hackers, so it is safer to change them.
- **Most home Wi-Fi providers now enable encryption** (such as WPA2) on their Wi-Fi networks by default. This means that the Wi-Fi signal is scrambled so that unauthorised computers and devices cannot read or understand the information you are sharing across your Wi-Fi network. Check your service provider's website for more information about how the network that you use at home is protected.

Secure your smart home appliances

Why is it important?

Check what appliances in your household are connected to each other and the internet through your home network eg. TVs, games consoles, speakers, heating systems, refrigerators etc. Sometimes you can communicate with these web-enabled smart appliances through your mobile phone as they are connected to your home network.

What can I do?

- **Change the default username and / or password** that comes with all smart appliances, making sure they are protected with a strong PIN or password. Check the product or service provider's website to help you. Default manufacturer passwords are generally known or easily guessed, which makes it easier for a cyber criminal to target you and steal your valuable information.
- **Where you have installed an app on your phone to manage a connected product or appliance, make sure your mobile device is suitably protected.** That way, if your mobile device is lost or stolen, it is protected from unauthorised access.

Secure your mobile devices

Why is it important?

Your phone or tablet holds a lot of information about you, such as your contacts, your emails and text messages, your music and all your apps, so it's important that you protect it.

What can I do?

- **Lock your mobile device** with a long passcode (at least six digits), and/or biometric protection (fingerprint/face ID) where possible.
- **Install the latest version of operating software** as soon as it becomes available and enable automatic updates where possible.
- **Before disposing of your mobile device, reset it to factory settings.**

Use strong passwords for online accounts

Why is it important?

Passwords provide a layer of protection when accessing your email accounts and websites or apps that you have registered with.

Do

Create a long password - use three or four random words or a sentence - that is easy for you to remember but harder for a cyber criminal to guess.

Use different passwords for different accounts so that if one is guessed, the rest of your accounts won't be at risk.

Consider using a 'password manager'. It frees you from having to remember multiple complex passwords as you only need to remember the master password.

Use stronger (two factor) authentication where it is offered by online services - often a security code texted to your mobile phone. It is used in addition to your password to make sure that you are who you say you are when logging on.

Don't

Don't use words that can be linked to you personally, like your pet's name, date of birth, or a well-known phrase.

Don't share your usernames or passwords.

Don't allow websites to 'remember your password'.

Don't use single dictionary words or common themes, like sports or seasons.

If you think that one of your online accounts has been hacked, such as your email account, change the password for that account as soon as possible. Consider changing your password for other accounts too.

TIP: VISIT THE WEBSITE WWW.HAVEIBEENPWNED.COM AND TYPE IN YOUR EMAIL ADDRESS TO CHECK IF IT HAS BEEN COMPROMISED IN A DATA BREACH

Use anti-virus and/or anti-malware software

Why is it important?

Anti-virus software offers general protection for your laptop, desktop or Android mobile device, guarding it against a variety of known viruses and weaknesses. Anti-malware is a more specialised layer of defence. Without this protection, cyber criminals may be able to steal your personal information or prevent you from accessing your files. Using both anti-virus and anti-malware tools together can help to maximise your protection.

What can I do?

- **Install a reputable anti-virus and/or anti-malware software product:** there are many to choose from nowadays. Make sure you go to the product provider's official website to download and install the software, following their instructions.

Make regular back-ups

Why is it important?

Making a back up of the information that is important to you (like your contact list, text threads, photos, videos, music, documents etc) helps prevent you from losing it completely, for example through malware, theft or physical damage.

What can I do?

Options for backing up your information include:

- **Cloud storage services** (there are many to choose from such as Google Drive, iCloud, OneDrive, Dropbox)
- **Saving to external and portable hard drives**
- **Saving to a USB device that you own**

Remember to label any portable back-ups that you create!

Guidance for parents and carers

As a parent or carer, it can be tricky keeping track of your child's digital life and knowing that you are doing everything you can to keep them as safe as possible online. Read our practical guidance below to help get you started.

Talk to your family about cyber security

Talking openly, positively and regularly with your child is the first step to teaching them safe online habits and why it is so important. This could include discovering the internet, games and apps together and talking about what is suitable, what boundaries you have and why.

You can also ask them who they are chatting to or playing a game with online, and encourage them to come to you when they are worried about negative online behaviour, like cyberbullying. Talking to other parents may also help with your own decision making.

Use parental control tools & restrictions for a safer online experience

Why is it important?

Parental control tools and restrictions help you to manage what your child can access online.

What can I do?

- **Parental control software products** offer protection for home computers (eg. Windows, Mac). They can include:
  - filtering and blocking unsuitable websites and pop-ups
  - setting time restrictions on accessing websites
  - filtering age-appropriate content

  There are several good products available - choose the right one for you and follow the provider's instructions to set it up.
- **Turn on Google SafeSearch.** This helps to protect children from coming across inappropriate content and images when using the Google search engine on their phone, tablet or computer.
- **Enabling 'Restrictions' in iPhone and iPad 'Settings'** allows you to manage access, including:
  - blocking access to apps, system apps (like Safari and Camera) and In-App Purchases
  - preventing apps from being installed or deleted
  - placing age restrictions on films and apps and restricting explicit content in music and podcasts
- **Enabling 'Parental controls' in Android device 'Settings'** allows you to:
  - set age limits for apps, games and films
  - restrict explicit music content

  You can also set up a separate 'Restricted Profile' for your child on Android tablets in Settings. This is handy if you want to share your own device with your child.
- **Parental control apps** are also available which can help to:
  - block apps and filter web content
  - track location and manage time restrictions, etc

  There are several good products to choose from eg Google Family Link on the Google Play Store for Android or the Apple App Store for iPhones and iPads. Download the parental control app that suits your needs and follow the instructions provided. Many applications also offer in-app restriction settings, or restricted mode, (eg YouTube).
- **'Screen Pinning' or 'Guided Access'** on mobile devices temporarily restricts younger children to one app, for example if you have lent them your phone for a short while to play a game. They are unable to switch to another app without your PIN code or fingerprint. You can turn this function on in 'Settings'.

Keep up to date with apps and social media safety

Why is it important?

Kids love apps. There are new apps available all the time so it's important that you keep up to date with the latest ones and what your kids want to use them for. Social media, photo and video sharing apps are especially popular. You can help to keep your kids safe and safeguard their identity by teaching them how to protect their privacy and what they need to be aware of.

What can I do?

BEFORE YOU BEGIN

- **Apply restrictions and parental controls** (see page 12 and 13).
- **Talk to your child** about the apps they want to download.
- **Read the app provider's recommended safety precautions** and about the app's features designed for online safety.

Then, talk to your child about:

APP SAFETY

- **Only download apps from official app stores** (such as the Apple App Store and Google Play Store) and not from links received in texts, emails or on social media.
- **Review and restrict app permissions.** For example, consider if an app really needs to know your location, or access your contacts, photos, microphone, or other features.

PRIVACY FIRST

- **Check privacy settings.** Often the default setting means that photos or videos can be seen by anyone. Manage who can see your posts and who can send posts to you.
- **Avoid sharing any 'personally identifiable information'** like your phone number or home address on apps.
- **Respect the privacy of others.** If someone you know is in a photo you post, make sure they have agreed that you can share it.

TRUST YOUR CONNECTIONS

- **Only connect with people you actually know or trust.** Fraudsters or dishonest people can set up fake profiles to try and connect with you for dishonest reasons.
- **You can usually block, delete or report other users** if you have a negative experience.
- **It's not safe to meet up with someone you have only met online;** stranger danger rules apply here too. Tell a parent or guardian or another trusted adult if you have any concerns.

PUBLIC SHARING

- **Be aware that friends could publish photos of you** using a 'public' account which means anyone could see them, or they could be posted through other social media accounts which may have different privacy settings.
- **Be careful when sharing information about you.** Sharing too much can increase the chance of someone stealing your identity, unwanted contact or even cyberbullying.
- **When you share photos, others might be able to see your location.** Think about if you really want people to know where your photos were taken; you can turn this off in location settings.
- **Information you post can live forever**, even if you remove it later.

TIP: IN SOCIAL NETWORKS ENCOURAGE A TRUSTED EXTENDED FAMILY MEMBER (E.G. OLDER COUSIN) TO BE INCLUDED IN THE SAME SOCIAL MEDIA GROUPS AS YOUR CHILD.

Commonly used apps - what you need to know

Let's look at some of the most commonly used photo and video sharing apps and what you need to know. Of course there are many more, so make sure you know what apps are trending now and what they are about.

Snapchat

Be cautious when sharing photos and location

- While photos and videos 'disappear' moments after they are posted on Snapchat, the Snap and Chats (photos, videos or texts) don't always disappear because the recipient can take a screenshot of it and share it further (you will receive a notification to tell you if someone has taken a screenshot).
- Snapchat Stories last for 24 hours and can be viewed more than once by anyone connected to your profile.
- SnapMap allows your location to be shared (enabling "Ghost Mode" turns this off).

Instagram

Understand the default settings and other features

- The default 'Public' setting means that photos or videos can be seen by anyone.
- Photos and videos can be shared publicly (to everyone), privately (to approved followers only) or directly (to max. 15 people). Even if your posts are private, your profile is public (your photo, username and bio).
- Group messages can be shared through the Direct Messaging feature.

YouTube

Talk about what type of content is and is not appropriate to watch

- You, as a parent or carer, are best placed to monitor and talk about what your child watches on YouTube.
- YouTube Restricted Mode filters search results to help prevent them displaying age-restricted or inappropriate video content.
- Restricted Mode can be locked to prevent your child changing the setting back to unrestricted, but this is not currently a feature in the app.

TikTok

Restrict in-app purchases and understand privacy features

- Accounts are public by default, meaning anyone can see your videos, send you direct messages, and use your location information. Once a profile has been set to private your profile photo, username, and bio will still be visible to all TikTok users.
- TikTok Coins are an in-app currency paid for with real money. Both iTunes and Android devices offer the ability to restrict these purchases. Enable iTunes "Ask to Buy" feature or set up purchase approval within your Android family group.
- TikTok offers a Digital Wellbeing feature designed to protect children under 13. It allows parents to limit time spent on the app and restrict inappropriate videos.

Twitter

Think before you post

- Most tweets are public, which is the default setting.
- Tweets appear immediately and can spread quickly by being re-tweeted by others.
- Sometimes content can be inappropriate and include location information.

ALWAYS CHECK IN YOUR SETTINGS WHO CAN SEE WHAT YOU SHARE AND WHO CAN CONTACT YOU THROUGH AN APP. CHECK OTHER SECURITY CONTROLS AND FEATURES WITH THE APP PROVIDER.

Play online games safely

Why is it important?

Knowing what games kids are accessing online and how appropriate they are can be a challenge. Help your child understand the dangers and learn how to play safely on their gaming consoles.

What can I do?

- **Ask your child questions** about the games, what they like about them and who they are connecting with. Perhaps you can even play the game with them!
- **Know what games your child is playing** and make sure you feel the games are age appropriate for your child. You can check the age rating for games on the PEGI website. Search **pegi.info**
- **Learn about and set up parental controls** by visiting the game console's official website. This will help prevent your child from accessing inappropriate games.
- **Advise your child not to share personal details** like their password, phone number or home address. Not using real photos or real full names helps to protect their privacy, and make sure they understand that people can hide behind fake profiles.
- **Block unwanted players or strangers.** You can find out how to do this from the console's official website. Make sure your child knows how to do this too.
- **Secure your device** with the latest version of the gaming software and use strong passwords.

Use trusted websites and be careful of pop-up advertisements

Why is it important?

Fake websites and some online advertising can contain malware or viruses designed to steal your personal information, or to trick you into paying for a product that looks genuine but is fake.

What can I do?

- **Don't click on links or advertisements to go to a website.** Instead type the official website address into your browser so that you can be certain you are on the legitimate website.
- **Stick with websites that you know and trust** when shopping online.
- **Look for 'https' and the padlock icon** at the start of the web address when entering personal information (like registering on a site or making a purchase). Bear in mind that cyber criminals use fake https sites too, so you need to take the full look and feel of the site into account, even where the connection is secure.
- **Consider installing suitable ad blockers or pop-up blockers.**

Know how to recognise and respond to cyberbullying

Why is it important?

Just like in the physical world, bullying can happen online too, but it is often harder to spot, and harder to escape. It can happen through instant message or text message, email, photos or videos, phone calls or social media.

What can I do?

- **Encourage your child to come to you** if they have any worries about cyberbullying or negative online experiences. Listen to and support them.
- **Report cyberbullying** to your child's teacher if it is school-related.
- **Know the signs of cyberbullying** – including depression, low self-esteem and poor exam results.
- **If affected, tell your child to:**
  - screenshot anything a cyberbully sends them for evidence
  - not to reply to any cyberbullying messages
  - block the cyberbully from contacting them
  - change passwords and contact details
  - report the abuse to social networking providers and mobile operators
- **Further support can be sought from professional counsellors or services like Childline.**

Family topics for discussion

Sharing personal information

Understand that it can be used by fraudsters for identity theft, manipulation, blackmail or bullying.

Protect mobile devices

Use a strong passcode and/or biometric protection.

Advertisements

Be aware of random ads popping up on screen – and don't click on them.

Strong passwords

Combine 4 random words or use a sentence, and don't use the same password more than once. Consider using a password manager app.

Phishing, Smishing and Vishing

Know how to identify and avoid these scams.

Social media for kids

Use privacy settings, know how to use it safely and age-appropriately, ensuring that parents or carers maintain ultimate control.

Software updates

Update devices as soon as the latest software version is available to allow any bugs to be fixed.

Anti-virus/anti-malware software

Install it on laptops, desktops and android devices and keep it up to date to help prevent malware.

Online gaming safety

Agree boundaries, know the age ratings and ask questions about the games and who they are playing with.

Public Wi-Fi

Understand the risks around using public Wi-Fi when accessing private information.

Talk about apps

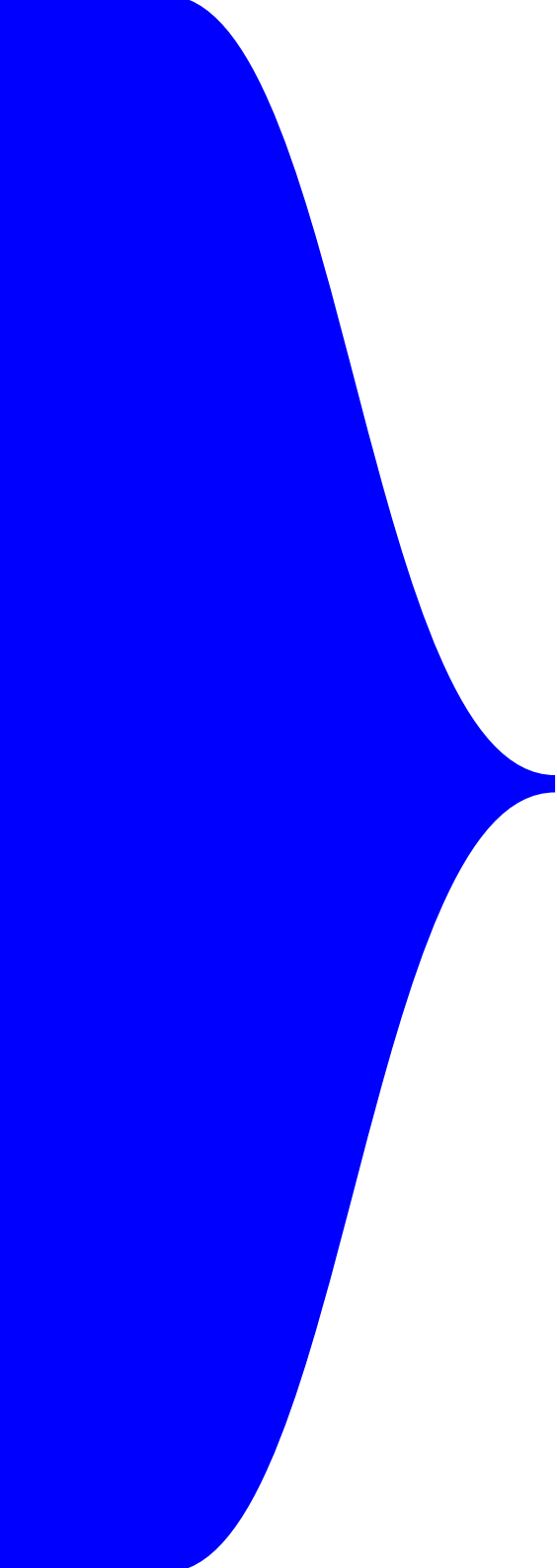
Keep up to date with trending apps, what's good about them and what the risks are.

Cyberbullying

Know the signs, how to respond, and where to get help.

Parent and carer checklist

1	I know what tactics cyber criminals use to steal information and money and how to spot them	☐
2	I have taken the necessary steps to secure technology in my home (network, appliances, devices)	☐
3	I have set up restrictions and parental controls (e.g. on the device itself, through a parental control app or through parental control software)	☐
4	I know what apps my child is using and what they are used for	☐
5	I will keep up to date with popular apps as they emerge	☐
6	I have talked to my child about safe online habits and why it is important	☐
7	I understand or will learn how to use privacy settings on social media and will guide my child in doing the same	☐
8	As a family, we are careful about sharing photos and too much personal information on social media	☐
9	I encourage my child to tell me or another trusted adult if they have experienced negative or unusual behaviour online	☐



Notes

Bank of Ireland UK

UK37-1522N.1 (09/24)