# Cyber Security At Home

Sonnect safely for kids and teens



# Are you a cyber defender?

Take our quick digital safety quiz for kids and teens.

### Ready Set Go!

Answers are upside down at the bottom of this page.

### Match the word which describes each of these potentially unsafe situations:





Α

Α

Α

## I should always check my privacy settings on my social media accounts because:

l can control who can see my posts and my profile information - after all, l really don't want strangers knowing all about me.



I want everyone to see everything about me.

#### On my mobile phone, the passcode I use to unlock it should be:



4

The year I was born.



At least 6 random characters, a pattern or if possible my finger print / face ID.



l don't need to lock it.

#### If I connect to public Wi-Fi, for example in a café, I like to:

Look up some new games and use my parent/parents' or carer's credit card to buy the best ones. В

Browse some of the new games available but wait until I am connected to my home Wi-Fi to buy them or use my mobile data.



When I want to download a new app, I go to:

Either the Apple App Store (if I have an iPhone or iPad) or Google Play Store (if I have an Android phone or tablet)



Click on a link I saw on a pop-up ad on my phone to download it directly



0. b	r 6	.5
d .e	5 q	4'
е.8	3 q	3.
е.7	<u>к</u>	5.
о. <u>с</u>	9 BnintsiV = C, gnintsinf9 = B, gnintsim2 = A	٦.
Answers:		

## Top tips for kids and teens



**PINs & Passcodes** – use them, but don't share them (except with your parent or carer) and use one that can't easily be guessed (don't use your date of birth!)



**Photos** – think before you share. 'Public' accounts mean that anyone can see them, and they often show your location. Do you want everyone to know where you are?



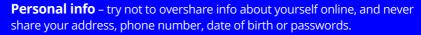
**Apps** – use official app stores only. Never download an app by clicking on a link in a text, on an ad or on social media as it could be fake.



**Privacy** – check your privacy settings on social media and control who can see what you post.



**Connections** - make sure you know and trust any new friend or follower requests.





**Public Wi-Fi** – it's okay to browse sites or play games but you can never be too sure who else is connected, so don't log into online accounts on public Wi-Fi. They could pick up your private info. And don't forget to disconnect when you're finished.



**Passwords** – make them long (a sentence or four random words) and never use the same one twice.



**Links & attachments** – they can be unsafe, especially in emails and texts if you're not expecting them or if they are from a stranger. Think before you click on them.



**Software updates** - updating your software and apps helps protect your devices from cyber criminals on your phone or tablet. Download the latest versions as soon as they become available.



**Screenshot** – take screenshots of posts or messages that you feel are unkind and upsetting towards you, and tell a trusted adult.



**Remember** - anything that you post can be shared or forwarded - think before you post.

#### bankofireland.com/security

The information included in this brochure is intended only as guidance to increase awareness of information security and online fraud and, while Bank of Ireland has made every effort to ensure the accuracy of this content, no responsibility is accepted by, nor liability assumed by or on behalf of, Bank of Ireland.

Bank of Ireland is regulated by the Central Bank of Ireland.