Cyber Security At Home

Connect safely for kids and teens

Bank of Ireland UK

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.

1

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

A I get a strange text message telling me I have unread social media notifications and to click a link to see what people are saying about me.

? Phishing

B I get a random email telling me I have won 12 months free access to my favourite online game! All I have to do is click on the link to claim the prize.

? Vishing

C I get a phone call from someone I don't know telling me they need my parents' credit card number to pay for an upgrade to a game or one of my chat apps.

? Smishing

2

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

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

B I want everyone to see everything about me.

3

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

A The year I was born.

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

C I don't need to lock it.

4

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

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

B 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.

5

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

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

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

6

I need to think up a new password for an online account so I use:

- **A** Something I have used before.
- **B** My pet's name, or my favourite sports team.
- **C** A long password made up of 3 or 4 random words or a sentence that I will remember but others would not be able to guess.

7

Identity theft is when:

- **A** Someone steals information about me online and then pretends to be me.
- **B** Someone I know who asks to connect to one of my playlists.

8

When my phone tells me that a software update is waiting, I:

- **A** Download it as soon I am connected to my home Wi-Fi.
- **B** Ignore it.
- **C** Keep telling it to 'remind me later'.

9

I'm playing an online game and I get a pop-up message from an online Help Desk asking for my password to fix something in the game, so I:

- **A** Tell them the password straight away .
- **B** Tell my parent or carer.

10

Someone you don't know and trust wants to connect with you on social media. Do you:

- **A** Connect straight away and tell them all about yourself.
- **B** Reject or ignore the invitation.

Answers:

1. A = Smishing, B = Phishing, C = Vishing
2. a
3. b
4. b
5. a
6. c
7. a
8. a
9. b
10. b

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.

Personal info – try not to overshare info about yourself online, and never share your address, phone number, date of birth or passwords.

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.

bankofirelanduk.com/help-and-support/security-and-fraud/

UK37-1429N (09/24)