Phishing – helping your child avoid online fraud

As online scam artists get more sophisticated, even tech savvy young people might find themselves vulnerable to some of their schemes. Here's some information and tips to help your children (and you) stay clued up.

What is phishing?

Phishing means trying to get access to personal information (usernames, passwords, bank details etc) using fake emails, websites, posts or other tricks.

How can your child avoid it?

The consequences of getting taken in by phishing can be serious, so it's important to know how to detect it. Make sure your children are aware of these tips to stop them falling for online scams.

1. **Check the URL.** Often, the URL on a phishing site will intentionally have missing letters or be spelled incorrectly. Make sure your kids know it wouldn't be a good idea to enter your information on f*aec*book.com, for example.
2. **Don't fall for requests to confirm your details.** Most legitimate online services won't ask for your password or bank details by email. If your child is asked for personal information in an unusual way, such as an email or pop-up, it should be a red flag.
3. **Be wary of 'free' stuff.** You usually can't trust offers that sound too good to be true, like winning free gadgets or making loads of money at the click of a button. That might sound obvious, but sometimes these offers can seem realistic, so make sure your children know to check with you before entering online competitions or taking advantage of 'investment opportunities'.
4. **Don't let curiosity get the better of you.** Have you ever seen a friend share a link that offers you a chance to see everyone who's looked at your profile? Or an unexpected raunchy video? Sometimes, posts that seem unusual or out of character mean a person's account has been compromised. Clicking on these links could cause problems for your child, so if it doesn't seem like something their friend would share, they should avoid the temptation.
5. **Watch out for pop-ups.** Pop-ups (windows that show up suddenly on your screen) can be used for phishing or to download harmful software onto your device. Your child shouldn't enter personal information into a pop-up window and should also be careful about clicking on them – especially on a mobile device, where smaller screens might make them more difficult to avoid.
6. **Get a second opinion.** It's not always easy to tell what's real online. Let your child know that if they're ever unsure about something they see, you'll help them figure it out.