Spotlight on online scams

Online scams involve deceiving and manipulating individuals with the purpose of gaining something of value, such as sensitive personal information or money. They can occur on websites, within games, on social media and in direct messages (DMs).

Potential risks

Account theft
Scammers may ask users to enter their personal data on false websites or talk to a user with the intention of stealing their personal information. If a scammer is successful, the personal information they have stolen may allow the scammer to access a young person's social media or online game account.

Too good to be true
Scammers may suggest deals or trades (for example for a valuable in-game item at a fraction of its price) or even offer high-paid jobs, all of which seem hard to turn down. These scenarios constitute scams which are often designed to take a user's money or personal details.

Fake giveaways
Scammers often promote fake giveaways on social media or in online games that promise large payouts of real money, in-game currency, or premium membership plans for free or for a small donation. Users are often instructed to complete a small task to receive their reward, like 'verifying' their account or completing a survey.

Fake relationships
Scammers may attempt to engage in a form of blackmail called 'sextortion' in which they threaten to publicly share sexual images of someone. These scammers acquire these sexual images by impersonating someone on social media or in an online game and feign romantic interest in the victim. Once the scammer receives the images, they will often threaten to share them unless the victim sends them money.

Practical advice

Lock accounts down
Whenever possible, always enable multi-factor authentication or 2-factor authentication. This means that scammers who successfully gain your child's login details will need to provide additional details or even devices to access the account.

Trust your instincts, not the deal
Speak to children to make sure they know they can speak to you if they find an offer that seems too good to be true. You should encourage them to check reviews or warnings, look at the profile of the person offering a deal on social media, and talk to an adult that they trust. Finally, ensure they know that if something feels wrong, it probably is.

Don't fall for fake giveaways
If a giveaway asks for personal information, account login details or even in-game items, then your child should avoid engaging with it. Reputable giveaways will never ask for these details in exchange for rewards.

Don't give in
Scammers engaging in sextortion often try to isolate the victim to make them feel powerless. However, professional support for young people is always available. You can learn more about sextortion to appropriately support your child and ensure that they know they can always come to you for help, no matter the problem.

For more information

Hwb®

Llywodraeth Cymru
Welsh Government