At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about

ONLINE FINANCIAL SCAMS & EXPLOITATION

To date, nearly 43 million UK internet users have encountered a financial scam online; roughly 20% of those victims wound up at least £1,000 out of pocket as a result. The number of con artists plying their trade in the digital world has grown in recent years (a worrying trend which, unfortunately, appears likely to continue), and their methods have become increasingly creative. It can, therefore, be difficult to recognise an online financial scam – let alone to safeguard our children against them – but it's not impossible. Our guide offers a few pointers on what to look out for.

WHAT ARE THE RISKS?

PHISHING SCAMS

Scammers often use deception to obtain personal and financial information from their target. They might pose as legitimate organisations, such as pretending to be HMRC and threatening legal action for unpaid tax unless the victim provides their National Insurance number. Their efforts have been getting more convincing recently, so be mindful of any unexpected or unusual emails.

IDENTITY THEFT

Criminals can manipulate someone into providing personal data, then use it to assume their identity online and commit fraud, make unauthorised purchases or engage in other illegal activities. Identity theft can be accomplished by tricking victims into downloading malware that scans their device for information; by figuring out passwords to social media accounts; or through phishing scams.

FRAUDULENT INVESTMENTS

Fraudsters might lure victims into offering their hard-earned cash for a "one-of-a-kind investment opportunity" promising high returns or quick profits – such as the many cryptocurrency scams currently circulating online. Some unscrupulous influencers have even used their status to tempt their followers into paying for courses which promise to help them become rich and more attractive.

DECEPTIVE ADVERTISING

Many online sellers use false or misleading advertising to persuade consumers to spend money or supply personal information. Certain websites, for instance, have become notorious for using attractive images to advertise their products, promising to deliver an item for a fraction of its usual price – only for a cheaper-looking, poor-quality reproduction to arrive in the post instead.

SOCIAL MEDIA SCAMS

Scammers use social media to manipulate or deceive victims, often by posing as a popular influencer and exploiting their audience – such as posting a link to a 'giveaway' which actually siphons money or personal data to whoever is behind this false identity. This type of scammer commonly impersonates influencers with a younger fan-base, as children tend to make more naive targets.

Advice for Parents & Carers

EDUCATE YOUR CHILD

Talk to your child about the risks of online financial scams and encourage open communication about their digital activities. Make sure they know the kind of ruses that are out there, and what to look out for when encountering a potential scam. Foster their critical thinking skills – and emphasise that if something they see on the internet seems too good to be true, then it probably is.

USE PARENTAL CONTROLS

Almost all devices that children typically use to access the internet have built-in safeguards like parental controls and monitoring tools. Stay aware of the options available to you, and make use of them to shield your child from possible exploitation as best as you can. This, combined with common sense and critical thinking, should go a long way towards keeping them safe.

STAY INFORMED

Try to keep your knowledge of current and emerging scams in the digital world up-to-date, so you can help your child stay safe. New methods of exploitation are developing all the time, but thankfully it's not all doom and gloom. There are plenty of sources – such as Ofcom – that keep a record of online scammers' methods, plus lists of which sites or schemes to be wary of.

PRIORITISE PRIVACY

Teach your child to value their own privacy: that is, to respect the value of their personal data and be cautious about sharing it online. It's especially important that children know to safeguard their financial details and other sensitive data – and never to provide that information to anyone online, unless they're absolutely certain that it's safe, secure and for a legitimate reason.

REPORT SUSPICIOUS ACTIVITY

Encourage your child to report any suspicious or potentially harmful online encounters to you or another trusted adult. Make it clear that that they will never get in trouble for telling you about what's happened. Fraudsters often attempt to play on children's fear of getting into trouble, so cancelling out that notion robs internet scammers of one of their greatest weapons.

Meet Our Expert

Ross Savage has a proven track record in countering financial crime, having spent 13 years with UK law enforcement – specialising in money laundering investigations and asset recovery from organised criminal groups. He now holds senior visiting expert positions at various organisations and delivers customised training and consultancy to government and private-sector clients worldwide.

National Online Safety®
#WakeUpWednesday

Source: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages | https://www.bbb.org/article/scams/26628-2021-bbb-scamtracker-risk-report
https://www.ofcom.org.uk/news-centre/2023/scale-and-impact-of-online-fraud-revealed | https://www.local.gov.uk/about/news/younger-people-scammed
https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 16.08.2023