Cyber Byte

January 2025.

Online recruitment, anonymity and encryption – just how easily are cyber criminals targeting our Children and Young People.

Encrypted messaging services on social media allows criminals to create chat groups online, with restricted access typically limited only to verified members. These platforms are often exploited by organised criminal groups to facilitate illegal activities, with minimal risk of detection by authorities or to the criminal organisers themselves.

Young people are highly active on a wide range of social media and gaming platforms. Criminals take advantage of this, with minimal effort, to target a large and often unassuming audience, using phrases such as "easy money" or "quick cash" to disguise illegal activities.

As a result, our children and young people may perceive these interactions as harmless or low risk, making them more likely to engage with these online criminals.

Carefully controlled language used by criminals, including slang terms, emojis, symbols and coded phrases are used to communicate in ways that are both appealing to minors and difficult for outsiders to understand. This makes the criminal messaging more appealing, whilst obscuring the true nature of criminal intent.

For example, everyday language will be replaced with drug related terms or symbols, such as snowflakes to stand for cocaine or a leaf to signify marijuana.

Terms like “job opportunity” or “business” are also used to make illegal activities sound legitimate, removing warning signals for our young people to recognise the potential dangers, such as exploitation.

Criminals will often adopt communication styles similar to social media influencers, where illegal tasks can also be posted as “challenges” or “missions,” making them more appealing and appearing less intimidating. This approach, known as “gamification,” resonates directly with a younger audience familiar to online gaming.

By introducing these activities as part of a game or competition, criminals aim to dilute the risk and encourage participation.

In some cases, criminals may offer rewards for completing specific tasks, enhancing the appeal, fostering a sense of accomplishment among young participants.

Associated messages can also be automated to self-destruct, in effect deleting conversation histories. This feature makes it challenging to check communications, because as soon as messages are received, they will quickly delete without creating a lasting digital footprint.

Emotional manipulation and grooming techniques feature very often. These are used in fostering trust, loyalty, and a sense of belonging. This type of approach appeals particularly to those seeking validation, protection, or wanting to feel part of a community.

By capitalising on these emotional needs, criminal networks effectively blur the lines between friendship and exploitation, making it difficult for our young people to recognise the dangers of their involvement.

The following link Staying safe online | Childline provides excellent guidance, including tips for staying safe whilst gaming and awareness to the signs of grooming.

Our partners have also created guidance on Chatrooms - Get Safe Online. This is another great resource and raises awareness of risk in chat rooms and how to protect yourself from unwanted online encounters.

This link for 11-18s | CEOP Education but not limited to that age demographic, will provide further excellent guidance and support. CEOP, one of our trusted partners, provides online safety guidance and support if you or someone you know has experienced inappropriate interaction online.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

This Cyber Byte was sent out for your information by

Police Scotland Cybercrime Harm Prevention Team

All information correct at time of distribution.