COM GROUPS

Early Threat Identification Notice for Safeguarding Professionals

October 2025

This notice is for safeguarding professionals only. It is not designed to be shared with children, young people, parents or carers. Should this threat evolve, the NCA will issue further guidance.

Please be aware this notice contains sensitive and distressing information, which is shared strictly for awareness and safeguarding purposes. Engaging with information of this nature can have a psychological impact. Please follow your organisation's wellbeing processes if support is required.

The National Crime Agency (NCA), National Police Chiefs' Council (NPCC) and Counter Terrorism Policing (CTP) are notifying children's safeguarding professionals of harmful online groups called 'Com groups', who may target children and young people.

What are Com groups?

Com groups are online networks of individuals who carry out serious, high-harm offences including child sexual abuse, serious violence, cybercrime (referred to as cyber Com), and extremism. Com groups are dynamic and often overlap across these threats, although not every case will involve all. Within these groups, offenders may compete against one another to cause the highest harm to gain status and notoriety. Offenders may do so by creating and sharing harmful and extreme content, for example, child sexual abuse material (CSAM), or by coercing victims, often under 18-year-olds, to commit harmful acts towards themselves or others, such as inflicting injuries.

Com group offenders may use grooming and extortion tactics to coerce a victim, with the aim of obtaining intimate images to humiliate, degrade or control them. In extreme cases, victims have been coerced into self-harm or attempting suicide; including the ingestion of toxic/harmful materials, or burning themselves. Victims may also be forced to record or livestream these acts, which are then shared within the groups to increase the status and notoriety of the perpetrator.

Relevance to your role

This notice is in the interest of awareness raising and early identification, to prepare safeguarding professionals should a concern arise. Should this threat evolve, the NCA will issue further guidance.

It is possible you may come across children and young people who are involved with, or a victim of, Com group offending. Based on the cases identified, a large proportion of individuals enacting Com group offending are males under 18 years old. These groups can target individuals of all ages and genders, however, females under 18 years old are being disproportionately targeted by offenders to groom, extort, commit child sexual abuse, and coerce self-injury and suicidality.

What are we asking you to do?

- Develop your understanding of the threat by familiarising yourself with the information in this notice
- Share this notice with safeguarding practitioners in your area, for awareness purposes
- Not to share with children and young people, to avoid increasing their exploration of, or engagement in, Com groups
- Look out for indicators of a young person's involvement, interest or victimisation, taking a safeguarding-first approach to ensure an effective response
- Follow your local safeguarding policies and procedures to manage concerns about a child, young person, or another person who may be at risk of harm
- Report concerns to the police, calling 999 if a child or young person is in immediate danger

What to look out for

No single behaviour is proof of links to a Com group. While some behaviours may indicate involvement or victimisation, others are less specific and may suggest a different type of online risk (e.g. bullying). Look out for the signs listed below that may indicate a child or young person is a victim, or involved in Com group offending. Please be aware, behavioural indicators may be seen in both victims and offenders.

Possible victim indicators

- Self-harm, such as skin lacerations depicting numbers, symbols, initials, usernames or group names (known as 'cutsigns' or 'fansigns')
- Numbers, letters or symbols written in blood, knowns as 'blood signs'
- Reluctance or fear of consequences associated with disengaging from an online group
- Unexplained injuries to siblings or pets

- Possession of extremist symbols (e.g. swastikas, occult symbols)

Possible offender indicators

- Promoting an online network, or encouraging others to join
- Possession of extreme content on their device, including child sexual abuse material, bestiality, the infliction of injuries or suicide and terrorist material
- Banners, symbols, or extremist flags in the home environment
- Fascination or fixation with violence, weapons or acquiring firearms
- Showing an interest in violence or extreme themes
- Unexplained injuries to siblings or pets

Possible cyber Com specific indicators

- An intense interest in cyber activities. This may include:
    - A known history of hacking, swatting (making false emergency calls), Distributed Denial of Service (DDoS), or online fraud (use of compromised credit cards)
    - An advanced understanding of and skills in digital technologies, hardware, and software
- Unexplained wealth – where the individual is in possession of items with a value that is disproportionately high to family or individual income
- Interest and advanced understanding of cryptocurrency

Other victim/offender behaviours to monitor*

- Unwilling to share electronic devices, passwords or accounts
- Increased secrecy around online activity
- Spending significant amounts of time online
- Strong emotional response (e.g. distress, anger or withdrawal) linked to online interactions
- Reluctance to engage with frontline professionals
- Obsession with new online friends
- Displaying social isolation offline

*The behaviours listed above may be typical of adolescent development, as many young people spend time online, value privacy and independence from adult monitoring. However, they may also be associated with involvement in or exposure to online risks (including but not limited to Com groups). Therefore, the context, patterns of behaviour over time, and any sudden or significant changes should be considered.

Who is at risk of victimisation?

There is no single set of characteristics that define someone as at risk from Com group offending. However, offenders looking to groom, extort, commit child sexual abuse, and coerce self-injury and suicidality often deliberately seek out vulnerabilities. This includes targeting individuals engaging with forums or online communities around:

- Body image concerns

- Discrimination on the basis of ethnicity, race and/or religion
- Gender identity exploration
- Mental health disorders
- Neurodiversity
- Self-harm and suicidality
- Sexual orientation exploration
- Substance misuse
- Those who have experienced sexual or physical abuse

Whilst these online environments, if effectively moderated, may be helpful and protective for individuals seeking support and guidance, the ease by which offenders are able to infiltrate and exploit these vulnerabilities may compromise their protective value – if not effectively moderated.

The harm caused by these groups can extend beyond the individual directly targeted. Victims may be manipulated or coerced into harming family members, often under threat, blackmail or psychological pressure. This can include being forced to physically or sexually abuse siblings or other children, or to injure or kill pets.

Who are the offenders?

Based on the cases identified, a large proportion of individuals enacting Com group offending are males under 18 years old. Engagement and the sharing of extreme content in Com groups may appeal more to young people who:

- Are socially rejected or isolated offline
- Are seeking belonging and community
- Spend significant amounts of time online
- Are often unsupervised online for extended periods
- Are seeking approval and notoriety from others online

The offender and victim dynamic is complex and not always clearly defined. Some individuals who perpetrate harm may themselves be victims who have been coerced or forced through threats, blackmail or psychological control. Others who offend may not have experienced victimisation themselves but still require safeguarding to prevent further harm and address vulnerabilities.

What should I do if I identify a concern?

- Follow your local safeguarding and child protection policies and procedures to manage concerns about any child, young person, or another person who may be at risk of harm.
- Report your concern to the police, calling 999 if a person is in immediate danger. Where possible, provide the following: the online platform(s), any online usernames and group names.
- Recognise that all children or young people involved, whether they are a victim or potential perpetrator, need safeguarding to ensure their safety and wellbeing, and to enable access to appropriate support.
- Encourage the child or young person to report to the platform(s) directly. Advise them not to delete anything that could be useful in an investigation, such as messages, images, videos, usernames, and URL links.
- Wellbeing support must be prioritised to manage the emotional and psychological impact of Com group involvement or victimisation on any child or young person involved. This may include referral to specialist services, such as CAMHS.

If you have specific concerns that a child or young person has been drawn into cyber criminality (including cyber Com groups), please visit Cyber Choices where you can send your concern or referral to your local regional team.

Your wellbeing and safety

Professionals should be aware that during an interaction with a child or young person involved with or a victim of Com groups, you may be exposed to distressing behaviour, disclosures or material. Any wellbeing concerns that you have about yourself, or colleagues should be discussed with your line manager or through your organisation's supervision and wellbeing processes.

As often seen in cases of grooming and coercion, victims of Com group offending may not recognise or identify themselves as a victim. This may present as reluctance to engage with professional support and in extreme cases, seeking to disrupt safeguarding attempts by targeting frontline professionals through 'doxing' (publishing personal information), 'swatting' (making false emergency calls) or in rare cases, live-streaming safeguarding visits. For more information on what doxing is, protecting against it and what to do if you're concerned, visit What is Doxing? A Guide for Professionals, Parents and Carers | SWGfL.

Our priority always remains to provide timely and accurate information on the threat to support informed decision making and effective action. Our understanding of the scale and nature of this threat is still developing; therefore, should this threat evolve, the NCA will issue further guidance across varying audiences.

Feedback

Scan the QR code below to share your feedback on this notice.