Fact Sheet

NORTHERN TERRITORY CONSUMER AFFAIRS

SEXTORTION SCAMS

Sexual extortion or 'sextortion' scams are a type of cybercrime where a criminal threatens to expose a victim's explicit images, videos, or intimate information unless they comply with specific demands. These demands usually include a demand for payment, sometimes in the form of money, payment cards or cryptocurrencies. There may also be a demand for more explicit sexual content. The demand for money may be repeated again and again. Sextortion is a very nasty and highly criminal type of extortion.

How these scams work

The extortionist often contacts victims through social media, dating apps, email, or other online platforms. They may pretend to have a romantic interest in you, but the account and personal information they share are fictitious. The extortionist engages in conversation to build trust and a connection with the victim. Eventually, they will persuade the victim to share explicit photos, videos or other compromising material. They will often share explicit images or videos of themselves with the victim, which have been created using artificial intelligence or other images they have sourced online. Once the extortionist has obtained material from the victim, they threaten to share it with the victim's contacts, family, friends, and schoolmates or publicly online unless the victim meets their demands. Extorters rely on the victim's fear of embarrassment and shame to manipulate them.

The extortionist will often try to create a sense of isolation and urgency with their victim to ensure payment is made before the victim seeks outside help and support. If the victim complies with these initial demands, the extortionist will often return and continue to extort them for more money or content.

The Australian eSafety Commissioner reports that sextortion complaints have more than doubled in recent years. The Australian Federal Police suspect's cases involving Australian kids are about ten times higher than those reported. According to the Australian Federal Police, 90% of sextortion victims are young males, many under the age of 18.

The law

Sextortion is considered a serious crime in Australia. All States and Territories have criminal offences for revenge pornography, as well as for extortion and blackmail. There are also Federal offences for using a carriage service to menace, harass and cause offence. The mental anguish of sextortion is considered grave by Australian courts, and sentences reflect this.

How to protect yourself

Take the time to gain a better understanding of online safety and computer security. The more you know, the better you can protect yourself and your devices.

Protect your personal information online. Your personal information is a financial commodity, and extortionists can use it for a whole range of criminal activities. Be cautious when sharing information online. Limit the personal information you share on social media and online platforms. Avoid sharing intimate photos or videos.

Adjust your privacy settings on your social media accounts so that you share information only with those closest to you. The stronger your privacy settings are, the harder it is for an extortionist to access your information.

Use strong, unique passphrases, not passwords. A long phrase, instead of a simple password, is much more complex to access for hackers. Enable two-factor authentication whenever possible.

Take care and try to recognise and avoid phishing attempts by being very wary of all unsolicited messages, friend requests, or emails, especially those asking for personal information or containing links. Remember to never click on a link. Simply clicking on a link can infect your device with malicious software.

If you do need to click on any internet links, ensure they are from trusted sources. Hover over the link to see the actual URL.

Never share your personal information in response to unsolicited requests. Consider limiting how much personal information you share at all. Personal information includes all sensitive information, including passwords, access to your phone or digital device, bank details, intimate photos and videos.

Stay updated about scams and internet and personal information security. Scammers continue to evolve, and it is important to know when a new type of scam becomes common.

Securing all your devices is critical. Always use security software and ensure its installed and set for automatic updates of antivirus and anti-malware software. Ensure your devices' operating systems and apps are updated regularly. Never download an app from an unknown source. Always use Google Play or the Apple Store.

Avoid using public Wi-Fi for any sensitive activities, and try to avoid using them unless you need to. Use a VPN for an added layer of security.

Carefully consider how much personal or sensitive information you share, even if its people you think you can trust. Use secure and encrypted communication platforms for sensitive conversations. If you wish to share intimate content, consider using platforms that do not allow others to download and save the content.

What to do if you're being extorted

It is essential to know it's not your fault. Even if you share intimate content with the extortionist, anyone can experience sextortion.

On a positive note, extortionists usually give up when they realise you won't pay. But suppose they do share your intimate image or video online. In that case, you can report it to the eSafety Commissioner, and they will help remove it.

Stop. Don't rush to act. Extortionists create a sense of urgency and play on your emotions. Cease all contact and do not pay the blackmailer. Keep a record of all communications and threats so that the Police are able to investigate.

Reach out to a trusted family member or friend for help. If you're 25 or younger, you can call or chat online with Kids Helpline. If you're 18 or older, you can call, text or chat with Lifeline.

Contact your bank immediately if you have shared financial information or transferred money. Help others by reporting your experience to Scamwatch.

Victims aged 18 or under should contact the Australian Centre to Counter Child Exploitation (ACCCE). If you're 18 years or older, report it to any platforms or services where the extortionist contacted you. If your intimate image or video is shared, or if the platform doesn't help, you can report it to the eSafety Commissioner.

You should report the extortion to the Northern Territory Police. They will investigate the incident and reduce the chance of it happening to others.

You can also consider seeking legal advice, especially if you suspect someone of sextortion. Darwin Community Legal Services (DCLS) offers a range of free legal and support services.

Lastly, consider speaking to a mental health specialist if you are experiencing stress or anxiety due to your experience. The impact of sextortion is far beyond the monetary loss. Many victims need time and support to recover fully.