*This is the fourth of a series of documents created by St. Andrew's parishioner Kelly Bourne, a retired computer security professional.*

**Cyber-safety Article #4 - Sextortion**

Sextortion is threatening to release explicit images or video unless the victim pays the criminal. Sextortion can be initiated on any site, app, messaging platform, or game where people meet and communicate. The number of cases of sextortion are rising rapidly. The National Center for Missing & Exploited Children (NCMEC) received reports of 26,718 cases in 2023, compared to 10,731 in 2022. Authorities believe that sextortion is vastly underreported because victims are too embarrassed to tell anyone about it. Surprisingly, this crime heavily targets boys aged 13 to 17. USA Today reported that at least 30 suicides of teenage boys have been attributed to sextortion since 2021.

The first contact may come from someone claiming to be of the opposite gender who expresses a desire to develop a relationship. Eventually the criminal will suggest an exchange of intimate images. The image sent by the criminal will be of another person that was copied off the Internet.

In some cases, the criminal may claim to already have explicit photos of the victim. It's unlikely that he has authentic images. If he has anything, it's more likely that the criminal copied the victim's photos off the Internet and use artificial intelligence to transform them into nude images.

Sometimes the criminal will include pictures of the outside of the victim's home to make the threat more credible. It's extremely doubtful that the criminal has been anywhere near the victim's home. Photos from the street of almost every home in America are available on Google Street View so it's more likely that he used those readily available photos.

If the victim pays, then demands from the scammer probably aren't over. The criminal will almost certainly continue to demand more and more money from the victim. In the worst-case outcomes, teenagers have committed suicide because they see no way out of their situation.

One extremely dangerous aspect of sextortion attacks is how quickly they can escalate. The criminals know that they can't extort large amounts of money from each victim, so they push a victim into paying off as quickly as possible then move onto the next victim. In one case a teenager committed suicide a mere six hours after the first threat was received.

Anyone threatened by sextortion needs to realize they are victims of a crime, and it must be reported. The FBI has staff dedicated to assisting crime victims, including sextortion. Victims can call 1-800-CALL-FBI or report online at tips.fbi.gov. The victim should also contact the administrator of the site where contact was initially made.

Parents and guardians of teens need to initiate conversations about this type of crime before their child is exposed to it. Kids will certainly be embarrassed to talk about this topic with an adult. They may claim that they're too smart to be tricked by this scam. They might insinuate that an adult doesn't understand social media. Don't let those excuses deter you! Educating them about sextortion can prevent immeasurable pain and could possibly can save their lives.

Adults should emphasize the following points during discussions with their children:

- Social media accounts are extremely attractive to predators because so many potential victims use it.
- If a new online friend tries to get too friendly too fast, it should raise a red flag.
- These criminals are professional liars and will use flattery and love bombing to build a relationship.
- This isn't your fault and you're not the only one this has happened to. You can survive this attack.
- Everyone should be extremely selective about what they share online. It's unfortunate, but anything you share can be used against you by criminals.
- Online encounters with strangers should be treated with extreme caution. Never assume that a stranger is telling you the truth about their age, gender, interests or where they live. Predators often steal photos off the Internet or take over someone's account and pretend to be that person.
- Predators frequently suggest that conversations be moved from the initial social media site to platforms like WhatsApp or Telegram. The new platform has fewer security features, making it hard to track where communications are coming from.
- Never send explicit images of yourself to anyone. Never. Content put online or sent to someone is out of your control forever. Some sites claim that images will disappear after a few seconds, but those limits are easily worked around.
- Web cameras can be hacked. When not being used it your camera should be turned off and physically covered. Using a Post-it to cover a lens might seem low tech, but it works.
- Attachments can contain malware so be extremely cautious when opening one. Never open anything from a stranger. Open attachments from someone you know only if you're expecting it or have confirmed with them that it's actually from them.
- If you're threatened, tell someone you trust. You should confide in a parent, family friend, school counselor, pastor, youth minister, teacher or older sibling. They can help you handle this.
- Paying what he demands won't make the problem go away. These criminals will continue to demand more money, images or videos.
- Some criminals offer to give something in exchange for explicit photos. They might offer money, gift cards, cryptocurrency, game cheat codes, movies, nude photos of themselves or games. Don't fall for this trick.

Steps that teens should take if they're contacted by sextortion criminals are:

- Ask for help from a trusted adult or law enforcement. Never send money or images.
- Report the incident to both the authorities and the platform it occurred on. Save the predator's name or account and all messages with him. These might help the platform administrators and legal authorities catch and prosecute him.
- Block the predator on the platform so he can't continue to contact you.
- Giving money or more images to the predator won't end it. You'll continue to be harassed and requested to pay more money.

- Kelly Bourne