A Safer Naper
April – Online Personal Safety

Today, being online is a part of life. We all go online daily to make purchases, keep up with friends and family, see what's going on in the world, and more! But not everything online is what it seems, and criminals routinely use the anonymity of the internet to prey on unsuspecting victims. This month, the Naperville Police Department aims to make our community "A Safer Naper" by reminding everyone of the importance of online personal safety.

SECTION 1: General Internet Safety

General internet safety rules to help you avoid getting into trouble online (and offline).

- **Keep Personal Information Professional and Limited:** You wouldn't stand on a street corner giving out your personal information to the strangers who walk by you, right? Then why would you do that online where millions of strangers can see what you posted?
- **Keep Your Privacy Settings On:** Both web browsers and mobile operating systems have settings available to protect your privacy online. These settings are sometimes hard to find because companies want your personal information for their marketing value. Make sure you enable these privacy safeguards and keep them enabled.
- **Practice Safe Browsing:** The Internet has hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge to click, you don't even give the hackers a chance.
- **Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection:** When you go online using a public Wi-Fi connection, you have no direct control over its security. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before inputting information such as your bank account number. To further improve your Internet browsing safety, use a secure VPN (virtual private network) connection. VPN enables you to have a secure connection between your device and an Internet server so that no one can monitor or access the data that you're exchanging.
- **Be Careful What You Download:** A goal of cybercriminals is to trick you into downloading malware programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Don't download apps that look suspicious or come from a site you don't trust.
- **Choose Strong Passwords:** Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. Select strong passwords that are hard for cybercriminals to decipher. Password manager software can help you to manage multiple passwords so that you don't forget them.
- **Make Online Purchases From Secure Sites:** Cybercriminals are eager to get their hands on the credit card or bank account information you provide when making an online purchase. Only supply this information to sites that provide secure, encrypted connections. You can identify secure sites by looking for an address that starts with https: (the S stands for secure) rather than simply http: They may also be marked by a padlock icon next to the address bar.

- **Be Careful What You Post:** The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made or get rid of that embarrassing selfie you took at a party. Don't put anything online that you wouldn't want your mom or a prospective employer to see.
- **Be Careful Who You Meet Online:** People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to cozy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.
- **Keep Your Antivirus Program Up To Date:** Internet security software cannot protect against every threat, but it will detect and remove most malware … as long as it's up to date. Be sure to stay current with updates for your operating system and any applications you use. They provide a vital layer of security.

SECTION 2: Sextortion

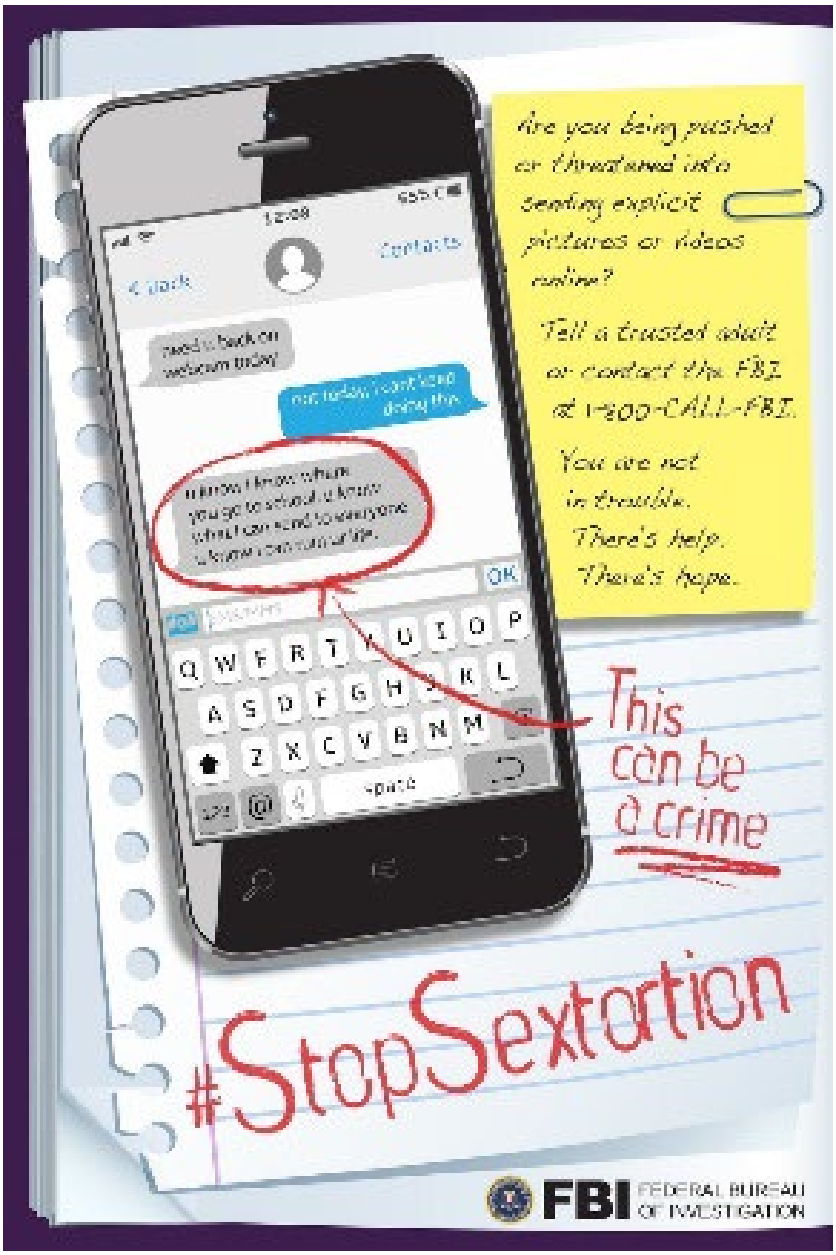
In early February 2025, the Naperville Police Department arrested a subject following a lengthy investigation into the online exploitation of a Naperville teen. The young man reported to Naperville Police that he had sent explicit photos of himself online to someone purporting to be a 16-year-old female. Police allege it was actually a 39-year-old man from Texas who then threatened to release the photos publicly unless the teen sent the suspect electronic payments.

“This is called sextortion, and it’s a growing problem in our society that every family should be aware of,” said Naperville Police Chief Jason Arres. The offenders of these crimes are not just targeting juveniles, however. In Naperville, 27 incidents of sextortion have been reported to the Naperville Police Department in the last two years, and more than half of the victims were adults.

What is sextortion?
Sextortion refers to someone threatening to share or distribute intimate images unless the victim takes a certain action. The perpetrator might demand that the victim share more images, send money or both to stop the perpetrator from sharing images more widely. The perpetrator may be stranger to the victim, but in some cases the victim and offender are acquainted.

How do I protect myself and my friends?
- Awareness and sensible safety practices online, along with a willingness to ask for help, can put an end to this exploitation.
- Be selective about what you share online. If your social media accounts are open to everyone, a predator may be able to figure out a lot of information about you.
- Be wary of anyone you encounter for the first time online. Block or ignore messages from strangers.
- Be aware that people can pretend to be anything or anyone online. Videos and photos are not proof that people are who they claim to be. Images can be altered or stolen. In some cases, predators have even taken over the social media accounts of their victims.

- Be suspicious if you meet someone on one game or app and this person asks you to start talking on a different platform.
- Be in the know. Any content you create online—whether it is a text message, photo, or video—can be made public. And nothing actually "disappears" online. Once you send something, you don't have any control over where it goes next.
- Be willing to ask for help. If you are getting messages or requests online that don't seem right, block the sender, report the behavior to the site administrator, or go to an adult. If you have been victimized online, tell someone.
- Never send anyone a picture or video of yourself that could be considered inappropriate or embarrassing. Ask yourself, would I send this to my grandma?



Resources:

https://www.childhelp.org/subs-online-harm/
https://www.missingkids.org/theissues/sextortion
https://www.onlinesafeonlinesmart.com/
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion
https://parents.thorn.org/guides/sextortion/

Sextortion video - Good for all ages (cat video)

https://www.youtube.com/watch?v=9yQ3fdttbUk

Image Removal (for victim use)

For kids: https://tidstart.ncmec.org/case/create?lang=en-us
For adults: https://stopncii.org/