



PARTNERS IN CRIME PREVENTION

SEPTEMBER/OCTOBER 2023

INSIDE THIS ISSUE

CYBERSECURITY- 1
TEACH YOUR
CHILDREN TO BE
CYBERSECURE

CYBERSECURITY- 2
TALKING TO YOUR
CHILDREN ABOUT
BEING
CYBERSECURE

CYBERSECURITY- 3
TEACH BASIC
CYBERSECURITY
PRACTICES

CYBERSECURITY- 4
MOBILE SECURITY

CYBERSECURITY- 5
FENTANYL

CYBERSECURITY- 6
RESOURCES

CYBERSECURITY— TEACH YOUR CHILDREN TO BE CYBERSECURE

Computers, smartphones, and the internet have become integral to our lives. We use the internet to look up facts, make dinner reservations, message family and friends and much, much more. As our children mature, they too learn to use the internet with a computer and a smartphone. And they often start using the internet much sooner than many adults.

On average, children ages 8-18 spend 7 hours and 38 minutes per day online, or almost half of their waking hours. And children are often enthusiastic in exploring and searching on the internet and communicating with their friends. As children use the internet more, they become susceptible to similar security issues as their parents.

Some common online issues children face include:

- **Cyber-Predators**– who search online for other people in order to use, control, or harm them.
- **Cyber-Bullying**– when someone posts mean-spirited messages about a person, often anonymously.

- **Identity Theft**– Cybercriminals love getting a child's social security number and other personal information since the victim often discovers the theft many years later causing havoc to them as young adults starting out in life.

And as parents, we might see other risks for our children:

- **Inappropriate conduct.** The online world can feel anonymous. Children sometimes forget that they are still accountable for their actions.
- **Inappropriate contact.** Some people online have bad intentions, including bullies, predators, hackers, and scammers.
- **Inappropriate content.** Children could find pornography, violence, or hate speech online.

To avoid risks and to use and enjoy the benefits of the internet as children then as adults, you can help them by educating your children on the various online threats and how they can prevent harm to themselves and their family.



Adam Fortney- Sheriff
Snohomish County
Sheriff's Office

3000 Rockefeller
 M/S 606
 Everett, WA 98201
 425-388-3393
<http://sheriff.snoco.org>

CYBERBULLY- ING-

Bullying or harassment can happen online in an email, a text message, an online game, or in comments on a social networking site.

Talk to your child about bullying. Discourage them from being a bully. Remind them that bullying makes them look bad and could bring punishment from authorities.

Ask your child to let you know if an online message/image makes them feel threatened. If you fear for your child's safety, contact police.

Check your child's profile page for mean-spirited comments. If their profile has been changed without their permission, contact the social media page's provider to have the comment/profile taken down. Block cyberbullies from the friend's list.

Encourage your child to tell cyberbullies to stop if they see someone else being bullied.

CYBERSECURITY- TALKING TO YOUR CHILDREN ABOUT BEING CYBERSECURE

Talking to your children about being secure online is important in their online development so that they use the internet in a safe and secure way as adults.

Start early in explaining safe practices online. Be supportive and positive as you talk to them. If they run into trouble online, you want them to feel they can come to you for help. Initiate conversations about online security, For example, pointing out news stories about internet scams or cyberbullying, can show that these are real world problems and help start a conversation about how to stay away from those situations or what to do to get out of a situation.

You may want to closely supervise younger children as they are first introduced to computers and the internet. That may mean that you choose what websites that your children visit and not letting them leave the sites on their own. It also means using filtering or monitoring tools, to help you know where your child is going.

As your child becomes more proficient in using the internet, and you are more comfortable that they will seek appropriate web sites, you may want to allow them to explore on their own. You still need to supervise them closely to en-

sure that they go to web sites that are appropriate in terms of their educational or entertainment value.

Children between ages 8 to 12, the "tween" years, will be more proficient in exploring on their own. It still is important to know where they are going and to talk to them about the pitfalls of the internet. Also, it may be a good idea to put a limit on how much time your child spends on the internet and to only allow computer use in a common area of your house.

As your child enters the teen years, they become more proficient, and will start to form their own opinions about internet use. Plus, they will have more access to the internet through more devices such as cell phones and friend's computers. A strict regime of monitoring may not be realistic as your child gets older.



CYBERSECURITY– TEACH BASIC CYBERSECURITY PRACTICES

As your child ages you should build their knowledge and understanding of online security and its importance. Below are some subjects that children should understand. You will not introduce all of these subjects to your child when they are young, but they should understand them by the time they reach their teen years.

- **Online words/pictures have consequences**– Write words or post pictures as if their audience is in front of them. Mean words, bad language, disrespectful talk can have real world consequences.
- **Only post information they are comfortable with others seeing**– Anything that they post may be seen by more people than their intended audience such as employers, college admissions officers, coaches, teachers, or police.
- **Once its posted it can't be taken back**– Once its posted, its posted. Even if the information is deleted from the site, other copies might be on other servers or personal computers.
- **Credibility**– Not everything on the internet is true. Also not everyone using the internet are who they seem to be. And some people pass around misinformation, disinformation, and fake media online.
- **No sex talk**– This can attract sexual predators. Encourage your teen to ignore or block someone that they find creepy or try to solicit them.
- **Encourage trusting their gut**– Encourage your child to tell you if they feel threatened by someone or are made uncomfortable online.
- **Don't impersonate**– Let them know that it is wrong to create web sites, pages, or posts that seem to come from someone else.
- **Create a safe screen name**– A good screen name won't reveal how old they are, where they live, or their gender.
- **Keep private information private**– Personal Identifiable Information, such as Social Security number, street address, phone number, or family financial information should not be shared online.
- **Password discipline**– Create long passwords that use upper and lower case and characters. Use a different password for each account, and store passwords in a password manager. Finally, do not share passwords with strangers or their friends.

PHISHING–

Introduce your children to the concept of "phishing." Phishing is an identity theft technique where a scammer sends a text, email, or pop-up message with embedded web links designed to gather personal and financial information. Clicking on the link could also install malware on your device.

Remind your children not to reply to messages that ask for personal information. Also that they should not give personal information on the phone in response to a text message. And they should be wary of clicking on links in text messages, emails or pop-up messages.

Encourage your children to tell you if they see phishing attempts on their devices. Forward phishing emails to the Federal Trade Commission at spam@uce.gov.

Show your kids phishing emails and texts that you receive. Explain to them why they are dangerous and how you knew that you should not click on their links.

TEXTING–

Texting with friends is a natural activity for children and teens.

Encourage them to,

- **Be respectful.** *Think about how a text message might be read and understood before sending it.*
- **Ignore text messages from people they do not know.**
- **Learn how to block numbers from their cell phone.**
- **Avoid posting their cell phone number online.**
- **Never provide financial information in response to a text message.**

Sexting. *Encourage your child not to send or forward sexually explicit photos, videos, or messages from their smartphone. Be sure that they understand that doing so risks their reputation and their friendships. It is against Washington State law for a minor under 18 to send a sext message of another minor older or younger than 13.*

CYBERSECURITY– MOBILE SECURITY

Smartphones are an integral part of modern life in the 21st Century. Your children will want to (and they should) use this communications and computing tool. Of course when to allow your child to use a smartphone is up to you, based on your child’s age, personality, and maturity.

Along with the fun stuff like calling and texting friends, your child should learn how to use their smartphone safely and securely. Some learning points to emphasize include,

- **Keeping a close eye on their phone.** Be sure that they never leave their phone unattended.
- **Keeping the phone locked.** Use biometrics such as fingerprints or facial recognition to open the phone so that no one else can use it.
- **Be careful of the apps that they load onto the phone.** Ask your child to check with you on any apps that they want to download so that you and your child can review the settings.
- **Only connect to the internet if absolutely needed.** Other than at home, teach them to consider Wi-Fi as unsecure. Disconnect from the internet when not using it and set your

phone not to automatically connect to Wi-Fi.

- **Use photo and video sharing with care.** Encourage your teens to think about their privacy and the privacy of others before sharing a photo or video.
- **Emphasize not to use their smartphone while driving.** When your teen begins to drive, be sure that they understand that it is dangerous to talk, text, or surf the web while driving.

You can take actions to supervise your child’s smartphone use such as,

- **Develop cell phone rules.** Give them a sense for when and where it is appropriate to use their smartphone.
- **Use parental controls.** Use parental controls to protect the safety and privacy of your child. Also, some cell phones are designed to be used by children that are easy to use but may limit features such as internet access and may have minute management, etc.

CYBERSECURITY- FENTANYL

Fentanyl has made the news in the last few years with reports of overdose deaths that include the homeless on the streets and the well off in their comfortable homes. Overdose deaths have included the old and the young. By some accounts, opioid related deaths have nearly doubled for 15-to 24-year-olds since 2015. And more and more, fentanyl, which is 50 times more potent than heroin, has been the synthetic opioid that causes the death.

Some illicit drug observers have stopped calling such deaths overdoses. Now they call them poisonings.

Fentanyl has flooded the illegal drug market. Cheap to make, fentanyl is not bulky making it easy to transport over the border or send in the mail. And someone seeking an opioid can easily afford fentanyl.

Now, most opioid users are not looking for fentanyl alone. They have tended to look for heroin or another drug. But, to save on costs and/or to give the heroin a bigger kick drug dealers would include some fentanyl. Drug dealers have been selling fake pills such as Oxycotin, Percocet, Vicodin, Adderall, Xanax, etc. with fentanyl in them.

So someone could order an Adderall, Xanax, or Percocet and be dead by the evening.

That someone could be your teenage son or daughter. Teens are becoming more susceptible to receiving deadly fentanyl doses through social media.

Drug dealers are using the internet and social media more and more to sell their illicit drugs. Social media is convenient, as close as your smartphone, and discrete; not having to go to the local drug corner to buy your drug of choice.

According to some reports, drug dealers like to target youth as new users. Some Drug Enforcement Administration (DEA) publications have even claimed that drug dealers want to get “customers” hooked on fentanyl for easy repeat sales.

Drug dealers use modern social media tricks to sell their deadly wares, such as slang terms, emojis, hyperlinks and QR codes. They also use marketing techniques to attract new buyers.

Gone are the days of experimenting with the drug of the day. Your teen could be looking for something to relieve pain or stress and find they are addicted to fentanyl. Or, since the fentanyl doses are not carefully measured, dead from one pill of a fake Xanax.

FENTANYL- 3 STEPS TO SELL DRUGS ONLINE

The smartphone has become the convenient way to purchase drugs, like ordering food delivery or ordering an Uber.

Be sure your teen understands the following points,

- *Drugs purchased on the street/ online could look like the real thing but be fake.*
- *Fentanyl has been found in pills claiming to be other drugs. It takes only 2mg of fentanyl to be deadly, which can be placed on the tip of a pencil. One pill can kill.*
- *Only purchase medications from a legitimate healthcare provider. Don't trust ads that may show up on their social media feeds.*

For more information on fentanyl and its distribution on social media go to,

<https://www.dea.gov/onepill>

CYBERSECURITY- RESOURCES

Guiding your children in using the internet successfully and safely is an important task. Educating yourself about cybersecurity and how to talk to your children about cybersecurity can help you to be more successful.

Here are some resources that can help you.

From the Cybersecurity and Infrastructure Security Agency (CISA):

- <https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-program-parent-and-educator-resources>
- <https://www.cisa.gov/sites/default/files/publications/Families%2520Cybersecurity%2520Presentation.pdf>
- <https://www.cisa.gov/sites/default/files/publications/Kids%2520Cybersecurity%2520Presentation.pdf>
- https://www.cisa.gov/sites/default/files/publications/Chatting%20with%20Kids%20Booklet_0.pdf

The following are some resources on how to talk to your child about cybersecurity.

- <https://www.safesearchkids.com/how-to-teach-kids-about-cybersecurity/>
- <https://www.pandasecurity.com/en/mediacenter/technology/cybersecurity-for-kids/>
- <https://www.globalsign.com/en/blog/cybersecurity-explained-to-5-year-old-and-90-year-old>

Safe Online Surfing Internet Challenge-

The Federal Bureau of Investigation (FBI) has developed an interactive learning tool that teaches cybersecurity and safety to children between third and eighth grade. The tool is available to schools or to families independently.

- <https://www.fbi.gov/how-we-can-help-you/outreach/safe-online-surfing-sos-program>
- <https://sos.fbi.gov/en/>

SHERIFF'S OFFICE RESOURCES

CRIME PREVENTION UNIT

CRIME PREVENTION UNIT EMAIL:

crime.prevention@snoco.org

CRIME MAPPING:

For information about crime incidents around your neighborhood checkout this link:

<https://www.snohomishcountywa.gov/236/Community-Crime-Map>

SHERIFF'S OFFICE CRIME PREVENTION WEB PAGE:

<http://www.snohomishcountywa.gov/289/Crime-Prevention>

NEWSLETTER INFO

EDITOR

Steve Moller

If you have questions regarding this newsletter or any articles that appear in it, please contact the editor at neighborhoodwatch@snoco.org

TIP LINES



Snohomish County Sheriff's Office: 425-388-3845

<http://snohomishcountywa.gov/303/Anonymous-Tips>

Crime Stoppers of Puget Sound: 1-800-222-8477