Digital Safety Moments
List of Topics for Student Safety & Privacy Videos

2015 Topics:
Login: Protect each of your accounts with a strong, unique password and do not share them with anyone else. Then device a way to ensure you remember your ID and password. Many social media sites support stronger authentication, such as two-step verification. Enable these stronger authentication methods whenever possible.

1. **USE NULS –** numbers, upper case, lower case, and symbols make a great, strong password
2. **Do not use your social media account to log in to other sites** - if one account gets hacked, then all of your accounts are vulnerable.
3. **Passwords and passphrases:** The more characters your password has, the stronger it is and the harder it is for an attacker to guess. However, long, complex passwords can be difficult to remember. So instead, we recommend you use passphrases. These are simple phrases or sentences that are easy to remember, but hard to hack.
4. **Password/passphrases are a secret**. If anyone else knows your passphrase, it is no longer secure. If you accidently share your passphrase with someone else or believe it may have been compromised or stolen, be sure to change it immediately.
5. **Privacy Settings:** Make sure you review and test your social media privacy settings regularly. Social media sites often change privacy settings and it is easy to make a mistake. In addition, many apps and services tags, or lets you tag your location when you post images or messages (called geotagging). Check these settings regularly if you wish to keep your physical location private. If you chose to make postings public, be aware so you don't expose yourself to strangers who can use your location to hurt you, or manipulate your information that damage your reputation.

Topics for the 2016 Student Video PSS Campaign

Choose your topic and prepare your video! All submissions are due **March 31, 2016**.
All videos open with: This is (first name only) from Houston Independent School District. I will talk to you about (insert your topic).
All videos close with: This is (first name only) from Houston ISD, reminding you to think before you click!

Topic: No Phishing!





Definition: When in doubt, throw it out: People send links in email, tweets, posts and online advertising. Sometimes, bad people send links that give them access to your personal information. If a message looks weird, or even a little bit suspicious, even if you know the sender, it's best to ask before you click. Often, phishing scam emails will try to convince you that you won a prize, or that someone wants to give you money. Sometimes they will pretend your password needs to be reset, and they send you a link to make that easier. Don't believe those emails! Delete any suspicious messages. You could be putting harmful files in your phone, tablet, or computer.
Talking Points:
• Emails, tweets or text messages may come to you with links you never asked for and don't recognize. Don't click them!
• You can't tell where a link goes just from looking at it. While it may appear to go somewhere safe, you can't be sure. It's always best to ask someone if they sent you a link before you click it.
• People don't really give away free valuable stuff on the internet. Deals that sound too good to be true are often phishing for your information.

• Clicking phishing email or text links may install invisible software that can steal your information and send it to someone far away.

Topic: WiFi Spy!



Definition: **Now you see me, now you don't!** Be careful about leaving your Wi-Fi and Bluetooth settings turned on when you're in public places. Very often stores will look for devices with Wi-Fi or Bluetooth turned on so they can track your movements while you are within range. Stores may do this to target your device for specific advertising or to watch what apps you use and what sites you browse and what games you play on your device. Other people may scan public Wi-Fi to try and capture your passwords or other private account information you share while using the public network. Turn off Wi-Fi and Bluetooth when not in use, and limit your use of free public wireless networks because others can use that information to track what you do online. When you do use public Wi-Fi, make sure you don't share any private data or account information.

Talking Points:

• Don't leave your Wi-Fi and Bluetooth settings "on" when you're in public places.
• Stores in malls, restaurants, movie theaters, amusement parks, and sporting events may offer you free Wi-Fi, but in return they're watching what you search, what you buy and which apps or games you use.
• Bad people may hang out in free Wi-Fi areas hoping someone will use a password they can steal.
• Make it a habit to keep your Wi-Fi and Bluetooth turned off when you're not using them or you're not in a secure location.
• Public computers (like those in libraries, stores or hotels) may have secret keylogging programs running that can capture personal information. Never use those computers for checking email, bank accounts, social media sites – or anything that may be private! You can use them to check for the news and local weather, or print your boarding pass, that's about it.

Topic: Be Share Aware!



Definition: Be aware of what's being shared: Everybody loves to post pictures! Sharing can be lots of fun, but you need to know what you're sharing *before* you post! Anytime you put a picture or video online, you may also be sharing personal information about others or personal details about yourself. Without meaning to, you might be letting strangers on the internet know where you go to school, where you like to hang out or even where you live. Check your phone's camera settings to be sure the GPS coordinates (latitude and longitude) are not automatically embedded in your pictures. Make sure your pictures don't have school names, team identification or any identifying background details. If you post a video or picture with other people in it, make sure you have their permission to share the image. If some people choose not to be included, crop them out or blur their image. Pictures and videos shared on sites like Tumblr, Flickr, Instagram, Vine and Animoto can be used by the company for marketing or downloaded by other users who may or may not respect someone's right to privacy.

Talking Points:

• Just because you enjoy sharing your pics online doesn't mean everyone feels the same way. Be sensitive to this!
• Be sure you get permission before sharing someone else's photo or video –. If the person is under 13, you need permission from their father, mother or legal guardian.
• You can use the privacy settings on your camera and social media websites to help limit the information in the pictures you share and the way you are tagged in other people's online photos.

• Besides being a potential safety concern, pictures online can be viewed by college admissions committee members and potential employers. You want to be sure the impression you convey is a good one!

Topic: Netiquette Matters!





Definition: How should I say this? Netiquette refers to the polite behavior people should follow when communicating with others online. When we talk to people in person, they use our body language, facial expressions and tone of voice to help understand our meaning. Over the internet, none of those important cues are available. It's very easy to misunderstand someone's meaning. Take the time to clearly say what you mean. Don't respond to text messages or emails when you're upset. Seek clarification before you decide someone has been disrespectful. Often people don't type in the same friendly way they speak. Once you press send you never know where that email will end up! You don't want your written words taken out of context and used to hurt another person's feelings.

Talking Points:

• Don't respond to text messages or emails when you're upset. Close the message and give yourself some time before you respond. Sometimes you may even wait a few days!
• Using all capital letters is considered yelling. Don't yell at people! Using all capital letters also makes your message more difficult to read.
• Read your message out loud to hear how it sounds. If you wouldn't feel right saying something to a person's face, don't put the message into a text or email.
• Be careful not to use "Reply All" when you mean to just "Reply" to one person.
• It is polite, if you must forward a long message, to clean off people's email addresses and signature lines. People may not want their contact information being shared.
• Don't text and email late at night or early in the morning. If people are resting, the incoming email/message tone might wake them.
• Be considerate! Treat other people the way you want to be treated.

Waiting in the Wings – Topics in development (Feel free to add and suggest more!)

1. **Own your online presence**: It's OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite online games, apps and platforms.
2. **Cyber attackers can analyze your posts:** and use them to gain access to your or your organization's information. For example, they can use information you share to guess the answers to the secret questions that reset your online passwords, create targeted email attacks against you (called spearfishing) or call someone in your organization pretending to be you. In addition, these attacks can spill into the physical world, such as identifying where you work or live.
3. **Privacy Settings:** If you use privacy settings, make sure you review and test them regularly. Social media sites often change privacy settings and it is easy to make a mistake. In addition, many apps and services let you tag your location to content that you post (called geotagging). Regularly check these settings if you wish to keep your physical location private.
4. **Social media sites:** use **encryption** called HTTPS to secure your online connections to the site. Some sites (like Twitter and Google+) enable this by default, while others require you to manually enable HTTPS. Check your social media account settings and enable HTTPS as the default connection whenever possible.
5. **Mobile Apps:** Most social media sites provide mobile apps to access your online accounts. Make sure you download these mobile apps from a trusted site and that your smartphone is protected with a strong password. If your smartphone is unlocked when you lose it, anyone can access your social media sites through your smartphone and start posting as you.
6. **Close your unused accounts:** if you are no longer using an account, be sure to close, delete or disable it.