Internet Safety

Playing it safe while playing online

Hi there kids! I am Charlie Cardinal and this is Speedy the Crime Fighting Hamster. We are here to introduce you to the basics of Internet Safety and some of the villains you need to watch out for. There are some bad characters out there, so you have to protect yourself. Your parents won't always be there to watch out for you, so stay sharp, learn all you can, and stay safe!

Privacy & Personal Information

Privacy is being able to keep things secret or hidden from others.

Personal Information is information about you or your family such as your address, a social security number, your parent's bank account, or how much money they have.

Criminals love to get people's personal information because they can pretend to be you, or use your money to buy things.

They can also make money off of your information by selling it to others. Companies or other criminals will use your info to send you junk mail or spam emails.

Criminals learning your address can be very bad. They may break in and steal from you. Protect your safety and your belongings, by keeping your information a secret.

These bad people may even use your personal information to trick someone else in your circle of friends and family. People sometimes tell criminals things that they shouldn't if they think that they are communicating with someone they know.

Think before you click

Do you know who sent that email?

Passwords

One of the most important things you need to learn is how to create strong passwords. A password is a code you type in to let the computer know it is really you.

Having an easy to guess password could allow someone to snoop around in your private information.

The way to make your password strong is to never use your name or your birthday. Use something hard to guess, but easy for you to remember. Make your password at least 8 characters long, and mixing numbers, symbols, and upper and lower case letters makes the password strong just like Speedy. Avoid using the same password over and over. That way if they do figure out your password, they only gain access to one account. And never leave your passwords written down where someone can find it.

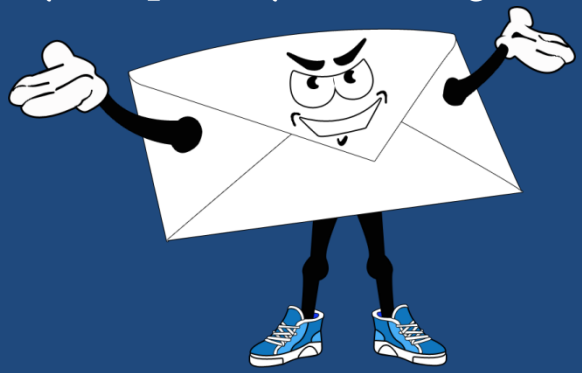
A great tool online that creates kid friendly passwords is the website, www.dinopass.com

Spam

Spam is basically email that you receive from different companies or strangers that you did not sign up for. Most times it isn't from real companies and usually the sender is up to no good.

Spam emails can sometimes be a phishing scam. Phishing emails are emails that look like it is from some trusted source. A place like your bank, the IRS where taxes are collected, or some other business you shop with often. They make their email look like it is the real thing with logos, and they put links in the email baiting you to click them. Once you click the link, you could be launching a program that can damage your computer in some way or collect your personal information.

Spam emails can also use winning a sweepstakes or some other type prize to trick you into trusting the email source. After they hook you in, they inform you that to collect your prize, you must give them your credit card number.



How do you know it is spam?

Spam emails typically have a bunch of spelling and grammar errors or a mention of someone you don't know in the subject line. Don't Open It! Delete those emails right away.

Malware

Malware is a program written with the intent to harm your computer in some way.

Programs such as this, may be waiting for you to do something(a trigger), so that it can run. This could be the clicking of the link or opening an email attachment.

When searching for free downloads online, be very careful. There are a lot of sites out there trying to trick you. They will pay to make their site get returned at the top of the list of search results. Then when you access the page, they use blinking buttons to trick you to click. The result of clicking usually ends up being your computer loaded up with malware.

Once your machine is infected, it can change browser settings, create unusual popup ads on your computer and then pass the malware on to someone else.

Spyware

Spyware is a program that gets onto your computer through a download or a virus and it gathers information about you and sends this back to its creator.

Some of the types of information spyware might send back to home base is email addresses of you or your contacts, passwords, account numbers, and credit card numbers.

Some spyware out there records how you use your computer and what you search for online.

Adware

Adware is software that you are allowed to use by the author because of the advertisements that pop up occasionally during the game. Many of these type games you will find in the form of apps on your phone or devices.

Through the addition of advertisments, the developer gains some income that may supplement a discount to the user, sometimes making the software free.

Often after using the product with the ads,
a consumer will purchase the software to get rid of the ads.

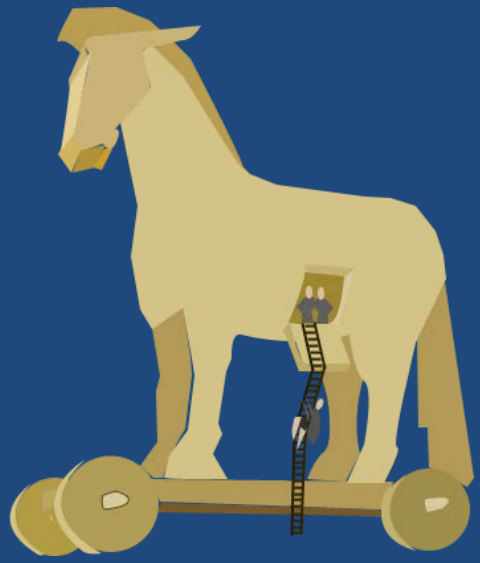
http://www.pctools.com/security-news/what-is-adware-and-spyware/

Trojan Horse

The name for the Trojan Horse virus was derived from tale of the Trojan Horse constructed by the Greeks to gain access to the city of Troy. The wooden horse was left at the gates as an offering to Athena. The horse was then wheeled into the city and out came Greek fighters hiding inside. http://www.britannica.com/topic/Trojan-horse

A Trojan horse virus is a form of malware that is dressed up as something interesting or software from a source we are familiar with. The purpose is to trick the person into installing it. This allows the creator of the Trojan to do damage to data or software on your computer. They also will set up a 'back door' or access point that allows them to access your system.

Trojan viruses don't spread by infecting other files and they cannot duplicate themselves.
http://www.webopedia.com/DidYouKnow/Internet/virus.asp



Worms

Worms are malware that can duplicate itself and spread to other computers. Worms always do something bad, even if it is just slowing things down.

Worms will frequently set up the ability for computers to be taken over by the worm's author by creating backdoors on the host computer. These computers are then called a "zombie computer". "Zombie computers" can be used to send out spam or as a shield to hide the web address of people who want to do bad things.

http://www.webopedia.com/TERM/Z/zombie.html

Virus

A virus is a small program that is created to spread from one computer to the next and to mess up the way your computer works.

Many times viruses hop from computer to computer via email attachments or messages. They can also hide in funny pictures(memes), e-cards, or other desirable file attachments. It can also be sent through an instant message.

A virus can corrupt your data, or worse, delete it. It can also email copies of itself to your friends.

Keeping your anti-virus software up to date is key to protecting against the latest viruses and other security threats.

https://www.microsoft.com/security/pc-security/virus-whatis.aspx

Social Media

Privacy settings on social media accounts are set up as public when you first get one. Unless you want everyone to be able to look at all of your photos and other private stuff, you must go into your account settings and change this.

Something to remember is whatever you post and say on your page can be shared by your friends. Think about what you post online, BEFORE you do it. What you post, could be seen by anyone at any time depending on your settings and the friends you keep. Because we can take pictures of our screens, there is really no setting that can protect you. Think twice about what you are sharing with others, so there are no regrets later.

Make sure you know the people that you accept friend requests from. Sometimes people try to friend you to hack your Facebook account or access your contacts. Once you are hacked they will send out strange messages or friend requests to your contacts. Protect your friends and yourself by being cautious with friends and creating strong passwords for your social media accounts.

Geotagging

Geotagging is the bit of data that your electronic device packages with your picture that has information about where the picture was taken. This is something that can be turned on and off in your device and typically comes turned on until you change the setting.

When your photo is geotagged, this gives people information about your location. Letting outsiders know where you are, can allow them to plan to steal your belongings or vandalize your home.

Consider if you post a photo every Wednesday in your outfit ready to walk to ball practice and geotagging is turned on. This shows you have a routine and gives a rough area you will be in. A predator could come and take you away.

Another issue with allowing the geotagging to occur is you don't have control of your own privacy. Everyone does not need to know where you are all of the time, keep this information private.

http://www.nytimes.com/2010/08/12/technology/personaltech

Be Careful of What You Say!

Defamation: Defamation is the blanket word used for all types of untrue statements made about others. Definition of Defamation on Law.com

Slander: When someone orally tells one or more people an untruth about someone, which will harm the reputation of the person it is about. It is not slander if the untruth is in writing of some sort or if it is broadcast through television or radio. Definition of Slander on Law.com

Libel: This is where someone publishes to print(including pictures), written word, online posts, blogs, articles, or broadcast through radio, television, or film, an untruth about another which will do harm to the person's reputation. Definition of Libel on Law.com

Be Careful of What You Say!

Much of the things people post online may get ignored, and you may get lucky and avoid legal action. But, when someone gets angry and files a lawsuit it can cause a major headache and possibly hit you hard in the wallet.

You might think you should have a right to openly complain about a company and their bad service or lousy product. Well when it comes to this, it is not always that simple. You can get sued for this and even if the judge agrees with you, you still have to pay for a defense attorney. Think twice and make sure that whatever you have to say is worth any headache you may have pop up later.
http://ideas.time.com/2013/01/07/yelp-reviewers-beware-you-can-get-sued/

On social media, people get into the habit of letting their emotions get the better of them and they end up speaking their minds about others online. When that person feels that this damages their character, they may opt to sue the other person for defamation. Even if their case is not successful, the stress, money, and time that you spend defending yourself is not worth it. To read more about defamatory social media posts, click here.

Stranger Danger Online

When you think of being on your computer or other electronic device in your own home, you probably think you are safe. Your mom is in the next room, what could happen?

Well there are people online that are up to no good. They go in chat rooms and pop up on your instant messenger, looking for someone to “groom”.

What is grooming you say? Well, grooming is when a stranger(can be any age) finds someone they are interested in, usually a minor. They act really nice and maybe they pretend they are much younger than they really are, like they are a kid just like you. Then they try to get you to like them and to trust them. They may ask you not to tell anyone you are talking to them. This is not okay and is a warning sign of a possible groomer.

How to Protect Yourself in Online Chats

- Choose chat sites designed for kids, such as www.kidzworld.com. Kidzworld is moderated and its aim is to protect kids from unwanted requests and online bullying.
- Beware of people you don't know. If they are asking too many questions or being too friendly they may be up to no good.
- If someone asks you to send them a picture or sends you a picture or video that is inappropriate, tell an adult or report them to the site moderators.
- Don't give out personal information to strangers online
- Don't tell strangers where you live or give them your telephone number
- Don't send strangers pictures of you or others
- If you are being bullied or threatened online, tell an adult or someone you trust

Cyberbullying

- Cyberbullying is the **willful and repeated harm** inflicted through the use of computers, cell phones, and other electronic devices.
- Using PhotoShop or other tools to create harassing images.
- Posting jokes about another person on the internet
- Using the internet to entice a group to physically harm another person.
- Making threats online using IM, email, social networking sites, or other electronic devices.

Consequences of Cyberbullying

Anything that you write, pictures that you post, or videos that you upload can be used by your school to **suspend** you.

College students have been removed from their athletic teams and lost college funding for writing negative comments about their coach.

When applying to colleges, they will search online to see what kind of person you are. They can deny you access if they don't like what they find.

When businesses are looking at people to hire for a job they will many times use social media to see what kind of person they are. Mean or inappropriate type posts can prevent you from getting the job you desire.

Cyberbullying can also be considered a crime and participating in this type of behavior can land you in big trouble.

Consequences of Cyberbullying

- § 18.2-152.7:1. Harassment by Computer; Penalty makes cyberbullying a crime.
- Carries a $2500 fine and punishable by up to **12 months in prison**.

There are many websites designed to inform and decrease the number of bullying cases we see each year. The U.S. Department of Health and Human Services has created a website with lots of resources to help combat bullying of all kinds - www.stopbullying.gov
If you experience cyberbullying or witness it, tell someone such as a school counselor, teacher, or a parent.

The Effects of Cyberbullying

- Victims feel depressed, sad, angry, and frustrated.
- Victims become afraid and/or embarrassed to attend school.
- Can lead to low self-worth, family problems, academic problems, school violence, and bad behavior.
- Victims can also develop thoughts of killing themselves and possibly act on these feelings.
- There are no positive effects of cyberbullying, only pain and suffering for the victims.
- The affects of being bullied can affect the victim into adulthood and prevent them from being all they can be in the future.

Dealing with Cyberbullying

- Never do the same thing back, 2 wrongs don't make a right
- Tell them to stop
- Block their access to you
- Report it to the site you are on such as Facebook or Twitter
- NEVER pass along messages from cyberbullies, stop the spread of this behavior
- Set up privacy controls and keep the bully out of your friends list
- Don't be a cyberbully yourself
- If you witness someone getting bullied, tell someone so it can be stopped. Many times the person being bullied won't tell out of fear.
- Spread the word that bullying is not cool
- Don't laugh or encourage the bully, it is not funny and it can lead to major trouble for the person doing the bullying.

About Sexting

"Sexting" is when someone sends or receives sexually explicit or non-PG Rated pictures or video electronically, mainly via cell phones or tablets.

The numbers on how many teens say that they have sent/posted nude or semi-nude pictures or videos of themselves is upsetting.
20% of teens between 13 to 19 years of age have engaged in sexting.
22% of teen girls
18% of teen boys
11% of teen girls between 13 to 16 years of age have engaged in sexting.

Did you know that if you forward a picture of a sexual or nude photo of someone underage, you are as responsible for the image as the original sender?? You can be charged with a crime.

Many teens don't realize that if you send a picture of yourself that is inappropriate and that picture ends up online, it could be there forever. You can never fully delete things that end up on the web.

About Sexting

There is no age minimum that protects young people from getting charged with a sexual offense.

Something that you think is okay or just a joke, might land you in a ton of trouble. For example, you might take a picture of your friend naked to embarrass them, but if they are under the age of 18, this is considered production of child pornography.

If you are sent something inappropriate, do not share it and don't delete it. Tell an adult immediately. You may feel like you are getting your friend into trouble, but you are protecting yourself and you are protecting them. They may not be thinking about the consequences or the effect this behavior can have on their future.

Anyone that gets convicted of a sex offense, will have to register as a sex offender. Sex offenders have to keep their address updated and keep a current photo with the police. The information goes on the sex offender registry where anyone can go and see your picture and where you live online.

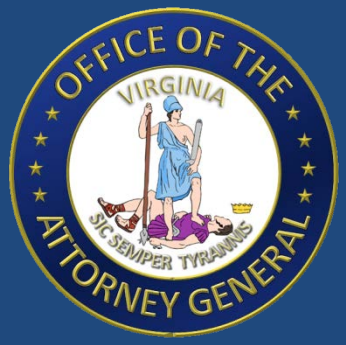
REMEMBER: You can't control what other people do with your photos. Even if you think you are sending it to someone you can trust, they may end up surprising you. You can't trust anyone with something as private as that. Don't Do It!

Legal Consequences of Sexting

- The Virginia Department of Education has an excellent resource with real life examples of the consequences of sexting that can be found here.

- The Attorney General's Virginia Rules website is designed to give Virginia Youth information on all the laws in the state. Virginia Rules has extensive information on sexting and other internet security risks.

- This article in The Virginian-Pilot tells a story of five Virginia teens getting charged with felonies for sexting and being in possession of sexually explicit photos of a minor, read more about it here.



Information Provided By:

Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-2071
www.ag.virginia.gov