

Natomas Charter School
Library Media Center
2009-2010

INTERNET SAFETY

Internet

- ⦿ Internet is a great tool, for both research and fun. But it can also be a great tool for some people **to hack, spam, bully or steal from** other people.
- ⦿ To protect yourself from those harms, you need to know what they are and what you can do.

Internet safety: what is it?

- Internet safety encompasses the laws and the guidelines that we should all follow to safely use the internet and protect ourselves from harm

Internet safety: why?

- ⦿ Because most people think they're safe, since they cannot see other people, or be seen by other users, they can do whatever they want.
- ⦿ So they actually display a very unsafe behavior while using the internet, sharing confidential information about themselves and/or their family, which puts them at risk since an ill-intentioned person can use this information for their own benefits.

- ⦿ However, the problem is that **any and all information that is posted on the internet can then be accessed by anybody.**
- ⦿ So, the same way you wouldn't give your name, address and phone number to a stranger, you also shouldn't share any private information on the internet.

- ◎ You also need to realize and remember: **everything that you post online will be there for a LONG time**, *even after you deleted that file or that picture.*
- ◎ So before sharing anything online, ask yourself:
“Would I like to see this again in 2 years? What would happen if the person running my college application or my job application saw this?”

The Laws

There are also many federal and state laws that protect you from hackers, spam, identity thieves and cyber bullies.

We will see those later on, in each subdivision.

The NCS Acceptable Use Policy:

You signed this form when you registered at NCS. Here are the rules that relate to internet safety :

- “Sending material likely to be offensive or objectionable to recipients is prohibited.”
- “Using programs that harass network users or infiltrated a computing system and/or damage the software components is prohibited. (Including, but not limited to any type of hacking software). “
- “You may not share your account with anyone or leave the account open or unattended.”
- “You will keep all accounts and passwords confidential and not accessible to others.”

Breaking the NCS Acceptable Use policy is punishable:

“Major violations of the Acceptable Use Policy, such as the willful tampering or destruction of other students’ computer files or folders, or *the use of school computers to access of distribute obscene or objectionable materials*, will result in **the immediate loss of all school computer privileges for the rest of the school year, and the student will be placed on technology probation for the following school year.**”

Internet dangers

- Email
- Hacking
- Spam
- Identity theft
- Sexting
- Cyber bullying and cyber harassment

Email

To protect yourself:

- ◎ **Remain anonymous.**

Keep your private information just that – *private*. So keep to yourself your full name, address, phone number, Social Security number, passwords, family members' names, credit card numbers, school's name, etc...

- ◎ **Do not give out your email address to anyone or any website.**

If you need to enter your email address to access some websites, you can either create a new address, separate from your personal email (used for personal information and communication), or make sure that your email provider has spam blocker available and ready.

- ① **Use a combination of letters and numbers** when you create an email address or screen name.

Also try to use words that do not give out whether you're a boy or a girl, your age/date of birth, your location or your interests.

- ① **Do not open attachments from unknown senders.**

They may contain viruses that will spread in your computer and can spread to the computers of anyone you send an email to.

Hacking

- Refers to the act of going around computer security to gain access to all, or part, of another person's computer or an institution's computer system.
- The law:
It is punishable by law (Access Device Fraud. [18 U.S.C. § 1029](#)) with a fine and/or imprisonment up to 20 years.

- ① To protect yourself: use firewalls, anti-virus and anti-spyware softwares, and update them often.
- ① To report a hacker, find out their IP address through a monitor software, find out who their Internet Service Provider (ISP) is and file a complaint directly with the ISP. If the ISP does not respond, contact the police.

Spam

- Refers to the method of sending the same email message to a large number of email addresses, to force recipients to read it.
- The law: Spamming sexually oriented material is a federal crime, punishable by a fine and/or imprisonment up to 5 years.

- ◎ To protect yourself, update your email spam blocker, and do not give out your personal email address. Should you need to give your email address to a website that you are not sure you can trust, create a new email address that will serve only that purpose – and keep your personal email address for the people you know.
- ◎ Report spam by forwarding the message to spam@uce.gov, and be sure to include the full email header.

Identity Theft

- Refers to the practice of using someone's confidential information to, illegally and without their consent, for one's own purposes.
- The law: It is a public offense, punishable by a fine and/or 1 year in prison.

- ① To protect yourself: **do not give out any personal information**, including but not limited to: your full name, your birthday, your home address, your phone number, your email, your Social Security number, your bank account/ debit card/ credit card number, and your family members' names. Companies and institutions never contact their clients by email with important details so emails from (people pretending to be) companies or institutions are a huge red flag.
- ① Report Identity Theft by calling the Federal Trade Commission's ID Theft Hotline-**1-877-IDTHEFT** (438-4338) or visit their webpage at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>

Chat rooms

To protect yourself:

- ⦿ **use a nickname that is different from your screen name**, that way, if someone is being inappropriate, they will not be able to look you up. Also in chat rooms, you can use the “private chat room” feature, so as to make sure that only people you know can get in your chat room.
- ⦿ **do not meet in real life people that you have only met online**. It is very risky, because some people hide their real identity behind a fake screen name and avatar.
- ⦿ **do not use webcams with anyone that you do not already know in real life**. People can capture videos from their computer, and use it to blackmail you, or put it on the internet, where you will have no control over it.

Sexting

- ⦿ Refers to the practice of taking a nude or semi-nude picture of yourself. While mostly done through the use of cell phones, the images sent can be uploaded to a computer and then onto the internet.
- ⦿ The law: Sexting may seem like “not a big deal” to teenagers – it’s your body, after all, right?
 - Wrong: sexting can fall under the child pornography laws (either production, distribution, or possession of child pornography, all of which are federal and state felonies). Punishments vary, going from community service to prison, or having to register as a sex offender.

◎ To protect yourself: The only protection from the possible consequences of sexting is **to not take those pictures in the first place** because just taking a picture and keeping it in your phone or on your computer could be considered a felony. If you feel pressured by someone to take and such pictures, remember two things:

-if caught, the consequences can be dire.

-you do not know where that picture will end up nor who will see it. Would you be comfortable knowing that the whole football team, the whole school, or a future coworker has seen it?

Cyber bullying and harassment

- “Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies”.

Quote from “The Educator’s Guide to Cyberbullying and Cyberthreats”, by N. Willard

- The law: Cyberbullying is not yet a federal offense, but it is punishable by a state law, which allows schools to punish cyber bullies with suspension or expulsion.

◎ To protect yourself:

1- keep track of all the messages they send you (print emails, messages, etc... showing their screen names, email address, the date and time),

2- find out their IP address, and

3- contact a parent, guardian or other trusted adult who will bring it to the police.

Resources

Net Smartz Kids:

<http://www.netsmartzkids.org/indexfl.htm>

Teens Health:

http://kidshealth.org/teen/safety/safebasics/internet_safety.html?tracking=T_RelatedArticle#

Wired Safety:

<http://www.wiredsafety.org/>

CyberTipline from the National Center for Missing & Exploited Children:

http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2446

Net Smartz 411:

<http://www.netsmartz411.org/>

Safe Teens:

<http://www.safeteens.com/>

Federal Trade Commission: Fighting Back Against Identity Theft

<http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>

Federal Trade Commission: Spam

<http://www.ftc.gov/spam/>

 *Be Safe!*

Natomas Charter School, Sacramento, CA

Created in June 2009 by Elsa Ouvrard-Prettol, NCS Library Media Technician