

## **Script: Internet Safety Ages 14-18**

**\*Please note that presenter's notes are italicized\***

**Slide 1: Deal.org talks about Internet Safety: facing the net realities**

**Slide 2: Internet Safety...**

- *Being safe online means knowing your way around the Internet. The net has become a regular part of most of your lives, which has a lot of benefits (instant messaging, e-mails, keeping in contact with friends, easy searching for information, etc.).*
- *The bad side is that the Internet can be deceiving in many ways. You must be careful on the Internet, especially in situations such as people or companies asking for personal information, meeting new people and with what you say and post online.*
- *The goal of this presentation is to make you think more critically about your Internet behaviour and practices and also to make you aware of the net's realities.*

**Slide 3: Do you know what your information is being used for?**

- *The Internet makes it easy to collect and store information about people. Companies may encourage you to answer online surveys, enter online contests and fill out registration forms that include questions designed to obtain your personal information.*
- *This information can be used for anything from creating advertising campaigns that target specific youth groups to being sold to other companies who then send you spam mail.*
- *For example, some social networking sites use the information you post on your profile to determine the different ads that appear on your profile and pages you visit.*

**Slide 4: Look out for websites that ask for your:**

- **Full name**
- **Home address, postal code or phone number**
- **E-mail address**
- **Friends' email addresses**
- **Hobbies and interests**

- *Just like any time you would give out your personal information offline, you should be cautious about whom you are sharing your information with.*
- *Your personal information can be obtained and misused in many ways. For example, it can happen when you:*
  - *provide information when registering for Internet services or software (i.e. file-sharing, instant messaging, e-mail).*
  - *complete a personal profile for a social networking or online gaming site.*
  - *fill out online surveys to enter competitions for prizes.*
  - *post messages on website message boards.*
  - *give out personal information in chat rooms or through instant messaging.*

- Before submitting any personal information online, you should:
  - try and find out why all of this information is needed and determine if they will keep your information confidential by reviewing their confidentiality clause.
  - always read the website or service provider's privacy policy before giving out your information or saying "okay" when signing up for anything.
- To maximize the security of your private information online, you can set up an alternate email address using false information to use in cases where you are asked to provide your email. This way, if your email is targeted with spam mail at least it won't be in your personal e-mail account.

#### **Slide 5:**

Ask the students the following questions. They can either answer out loud, or be given a few seconds to think of their responses in their heads.

- You receive this instant message from Studly\_04. What would you do, respond with the information since his avatar looks nice enough? Respond with mostly false information? Don't respond at all?
- What would you do if a friendly looking person in the mall turned to you and asked you these questions? Would you respond the same way?
- If you wouldn't do it in the mall, why do it online?

#### **Slide 6: Identity Theft**

- **When someone wrongfully obtains and uses another person's identifying information for the purpose of fraud or other criminal activity, typically for economic gain**
- **Repercussions can last for years**
- **Always think carefully about sharing information online and take the necessary steps to protect it!**

*If someone obtains personal information like your date of birth, address, social insurance number and employment information, they can use this information to impersonate you. They can apply for and obtain credit cards in your name without you ever knowing! They can also take over your financial accounts or create new ones, transfer your bank balance, apply for loans or purchase goods and services. Your information can also be used to obtain passports, visas, and other important documents.*

*The repercussions can last for years. If someone obtains a credit card in your name, it can affect your credit for up to ten years! This will make it next to impossible for you to get any kind of financial loan, to buy a car or to obtain a mortgage when you're ready to buy a house.*

*To help minimize your risk of identity theft, think carefully before sharing any information online. If it seems odd that you're being asked for certain information, don't give it out! Trust your gut instinct when it comes to giving out personal information online – if it doesn't feel right to be giving out certain details, don't do it!*

*If you're using online banking or other sites with confidential information, don't do so from computers in public places and make sure you sign out when you're finished. This makes it more difficult for other people to steal your information.*

### **Slide 7: Phishing Scams**

- **“Phishing” involves illegally obtaining information through spoofed (falsified) emails that appear to belong to a legitimate business (eg. banks, online auction sites).**
- **REMEMBER: A legitimate business will never ask you to give them your password!**

*These emails redirect the person to a spoofed website appearing to be from the same business. The website will ask for personal information such as account numbers and passwords. If the person enters the information, it goes directly to the people responsible for the scam.*

*Example: In June 2004, a [phishing scam targeted Royal Bank customers](#). Fraudulent emails purporting to come from the bank were sent to customers, asking them to verify account numbers and personal identification numbers (PINs) through a link in the email. The fraudulent email stated that if customers did not click on the link and enter this information, access to their account would be blocked.*

### **Slide 8: Shopping or Banking Online**

- **Only shop online from businesses you trust**
- **Ensure there is a locked padlock or unbroken key at the bottom right corner of your browser when making online purchases and when banking online**
- **Always log out properly**
- **Never use the same password for online banking that you do on any other website**

*A secure padlock or unbroken key in the bottom right corner of your browser means that you have a secure connection and that it is unlikely that intruders are viewing your information.*

*To log off properly, always click “log off” or “sign off” instead of just clicking the “X” in the top right corner to close the window.*

*Having different passwords is the smartest way to avoid invasions of your privacy. Don't share your banking password with anyone, and if you need to write it down, don't store it on your computer.*

### **Slide 9: Using Credit Cards Online**

- **Check company policies and keep records of your purchases**
- **Only use safe payment transfer systems (eg. SSL)**

- **Only buy from safe sellers: check the feedback left from other buyers and make sure they have a verifiable address and phone number**

*Any company that lets you pay using online payment transfers or credit card payments should use SSL (a Secure Socket Layer), which encodes all information. SSL makes it difficult for third parties to view your information. Websites that have SSL should start with “https” instead of “http” when you go to make a payment.*

*Most auction sites have a feedback system where buyers can rate sellers. Check the comments left by other buyers to see if the seller is safe.*

### **Slide 10: Online Contests**

**They’re so appealing because you might win something!! But they often ask for tons of your real info. What should you do?**

*Allow students to answer this question. It might be good to remind them that even though they may potentially win something, many scams can be found on the internet.*

*Before entering a contest online, ask yourself:*

- *Is it being held by a company you know?*
- *Is there a number to call to talk to someone about details, or a website to visit?*
- *What do you have to do to win? Answer an obviously easy question, or give them personal information to get the prize?*
- *Remind students that even if you follow all safety rules when it comes to online contests or shopping, you can sometime fall victim to an online scam. Online scammers can make fake websites and emails where it is virtually impossible to tell.*

*Most importantly, does it sound too good to be true?*

### **Slide 11: If it sounds too good to be true... it most likely is!**

**For more information, or to report any scams or fraud you come across, visit**

- [www.recol.ca](http://www.recol.ca)
- [www.phonebusters.com](http://www.phonebusters.com)

*Use your gut instinct when you run into these kinds of situations. If it sounds too good to be true, it most likely is! For more information, or to report any scams or fraud you come across, visit: RECOL (reporting economic crime online) [www.recol.ca](http://www.recol.ca) or the Canadian Anti-Fraud Call Center [www.phonebusters.com](http://www.phonebusters.com).*

### **Slide 12: Michel’s Story**

*Present Michel’s story (below) and allow students to answer the question, “What can happen as a result of Michel giving out this information?”*

*Michel’s Story:*

*Michel was looking for a rare video game he wanted on an online classified site (a site where individuals can post ads for items they are selling – examples are Craigslist and Kijiji). He finally found a seller named ill\_skillz who was selling the game and at a very*

reasonable price. Michel sent ill\_skillz a message saying he was interested in purchasing the game. Later that day, Michel received an email from ill\_skillz. Ill\_skillz told Michel that he was away on vacation, but asked Michel to contact his brother to complete the transaction. He gave Michel his brother's email address and asked him to send an email with his full name, mailing address and credit card number. This made Michel a little uncomfortable, but he felt better about it when ill\_skillz explained that his brother just needed the credit card number to as confirmation that Michel wanted the video game so that it wouldn't be sold to someone else.

Michel sent the email and waited anxiously to hear back from ill\_skillz or his brother. After a few days, he still hadn't received any confirmation that the video game was being sent to him. When he got his credit card bill at the end of the month, he discovered that it had been maxed out the day after he sent the email.

Remind students that:

- You should never give personal information or credit card numbers to an individual or company if you're not completely sure that it is a legitimate transaction.
- You should only make purchases online through secure payment systems.
- Once someone has personal information like your address and credit card, it's easy to steal your identity and ruin your credit (explain the concept of credit if students are unfamiliar).

### **Slide13: Chatting**

- Chatting online has become an everyday activity for the majority of youth whether it is through instant messaging services or social networking sites.

- 86% of grade 11 students use instant messaging on an average day.

- 86% of students report that they have email accounts ([Media Awareness Network. Key Findings. "Young Canadians in a Wired World Phase 2, 2005\)](#)

### **Slide 14: Benefits of Chatting**

- **Staying connected with friends from school or those who have moved away**
- **You can chat while browsing the web**
- **Make new friends from all over the world**
- **Chat programs can be used to work with others on school projects or to transfer files**

Ask youth if they can come up with other benefits of chatting.

### **Slide 15: Negative Aspects of Chatting**

- **Hard to convey emotion or tones of expression**
- **Can be habit forming**
- **Use of short-forms and slang may make its way into your everyday speech and writing**
- **Harder to determine who you should and shouldn't talk to**
- **People can lie about their age, sex, location and intentions**

- **You can become the victim of harassment, verbal abuse or cyberbullying**

*Ask youth if they can come up with other negative aspects of chatting.*

**Slide 16: Social Networking Sites**

- **Add only people you know as friends personally**
- **Set your privacy settings. If not, virtually anyone can see what you post online!**
- **Respect others online: if they do not wish to have their names or picture on your page, respect their wishes!**

**Remember: once you post something online, it is no longer private! You no longer have control over what or how it can be used.**

*Another way to keep in contact with friends and family is through **social networking sites**. While having a blog, personal website, or account on a website open to public viewing is great, it is important to be aware of what you post on such sites. You should also think critically about who you add as friends, what you say and do on the site, as well as whom you allow to access your information.*

- *Basic rule of thumb: Do not post or do anything you would not want your parents or grandparents to see!*

**Slide 17: Chatting Tips**

- **Use a nickname that does not say too much about you**
  - **Examples: SillyBee, Prostar\_22, \*hyper\_1\***
- **Don't give out personal information (which city you live in, which school you go to, sports teams you're on etc.)**
- **Don't send pictures of yourself – especially to people you don't know personally**
- **Don't meet up with people you meet online – especially not alone or without telling anyone where you are going and who you are meeting**
- **If anyone online makes you feel uncomfortable, tell a parent or trusted adult**

*To ensure you always have a good time chatting online, here are a few tips to keep in mind:*

- *Use an impersonal nickname. The more impersonal a nickname the better. Your name online is the first thing others see and it determines the first impression they have of you. Ex: SillyBee, Prostar\_22, \*hyper\_1\*.*
- *Don't give out personal information. Personal information is anything that you wouldn't feel comfortable telling a stranger on the bus or while waiting in line to buy something from the grocery store.*
- *Don't send pictures of yourself. It may seem as though sending a picture is harmless, but the truth is once it's out there you have no control over who sees that picture or what it is used for. You can't predict where this picture might end up posted or into whose hands it can fall. Imagine how weird it would be if you were visiting [www.crazypeople.com](http://www.crazypeople.com) and found your picture! Once you send out*

*your picture, how it may be used, modified or who may see it is out of your control.*

- *Also, the person you are sending your picture to may not be who they say they are, yet they now know exactly what you look like. Combined with other things you may have told that person, it can be easy for them to seek you out without your permission.*
- *Don't meet up with people you meet online, especially not alone or without anyone knowing where you are going and who you are going to see. It may be tempting to meet someone who you have come to like online, but the reality is you don't know who they truly are. Ask yourself this: have you ever lied to someone online? Most likely yes. That means that it's likely you have been lied to as well. The person you are meeting may not be who they say they are, or have other intentions than what they have led you to believe.*
- *If someone you are talking to online makes you feel uncomfortable, tell a parent or trusted adult.*

### **Slide 18: Cyberbullying**

*Cyberbullying involves the use of communication technologies such as the internet, social networking sites, websites, email, text messaging and instant messaging to repeatedly intimidate or harass others.*

### **Slide 19: Examples of Cyberbullying**

- **Sending mean or threatening emails or text/instant messages**
- **Posting embarrassing photos of someone online**
- **Creating a website to make fun of others**
- **Pretending to be someone by using his or her name**
- **Tricking someone into revealing personal or embarrassing information and sending it to others**

### **Slide 20: David Knight**

*Share David's story (below). You may be asked to reveal specific details about David's case. We suggest that you respond that the details of his case are not important and that what is important is to recognize the harm that bullying causes, whether done in person or online.*

#### David Knight

*As reported by [CBC, 2005](#):*

- *David Knight's life at school was hell.*
- *He had **no idea why** he was teased, taunted and physically hurt for years.*
- *The humiliation became unbearable when someone set up an abusive website about him.*
- *The website posted vulgar, sexual comments and hurt David's reputation. He also received nasty emails with similar messages.*
- *In David's case the bullying escalated from 30 people in the cafeteria saying something about him, to being posted online for 6 billion people to see.*
- *Feeling trapped, David left school to finish his last year of studies at home.*

- Seven months later, David and his family finally got the hurtful website taken off the internet.

**Slide 21:**

**How is cyberbullying different from traditional bullying?  
What can someone do if they are being cyberbullied?**

Ask the group the questions and write their answers on the blackboard or a flip chart. Should they have difficulty answering the question, give them some of the examples below and encourage participation. Once the discussion has dissipated, continue to the next slide.

1) How is cyberbullying different from traditional bullying?

- It has no boundaries: cyberbullying can follow one home after the school day is done, or anywhere else where communication technologies are accessible.
- It can be harsher: often things are said online that one would not normally say in person, mainly because one cannot see the other person's reaction.
- It is farther reaching: one can make fun of someone to an entire class with just a few clicks through an email or website, or post something for the whole world to see. Also, anyone can be cyberbullied, including teachers, principals and other adults.
- It can be anonymous: made-up screen names and email addresses are often used. Often times the cyberbully knows the victim, but the victim does not know who the cyberbully is.

2) What can someone do if they are being cyberbullied?

- Do not reply to messages or posts from cyberbullies. If possible, block the sender of the emails/messages.
- Keep a copy of the messages. You do not have to read them, but you may need a copy in the future if you decide to report the bullying.
- Tell someone about it, such as a parent, teacher, law enforcement officer or adult you trust.
- If the messages are on a website or webpage, contact the Internet Service Provider (ISP). Most ISPs have policies that include guidelines for using the service as well as actions that can be taken if they are not followed. Many websites also have a link or button where one can report inappropriate content. In some cases, the website owners themselves can remove the content and/or warn the individual who posted it, while others require an investigation into the incident.

**Slide 22: First Impressions?**

Ask students what first impressions they get from the avatar on the left. Then ask what first impressions they get from the avatar on the right. Ask students what they would think if you told them that the Avatar on the left was actually:

- 15 year old girl
- Lives in a rural town in Alberta
- Is part of the school choir and volunteers at a local retirement home

Ask students what they would think if you told them that the Avatar on the right was actually:

- 52 year old man
- Lives with his family in a townhouse located in a major city
- Works for a publishing company

After giving the students the descriptions, ask them if they are surprised. Was their first impression different from the description of the person?

**Slide 23: Think about this:**

- 1) First impressions online matter.
  - Ask youth to think about what impressions any pictures (real or fake) they put online may give others of them.
- 2) People are not always who they say they are.
  - Have you ever lied online (about your age, where you're from etc.)?
  - If you can lie, so can other people. Don't believe everything someone tells you online!

Tell youth that this exercise was fictional, and was created to get them to think about these two ideas.

**Slide 24: Internet Luring**

Most of you have probably made something up online before, from how old you are to which city you live in, which makes it likely that someone you have talked to was not totally honest with you either. Unfortunately, not everyone you meet online has the best intentions when making things up.

**Slide 25:**

Some people you meet online may be contacting you with a sexual interest, rather than a friendly interest in you. Using the internet to convince a youth to meet for sexual acts is called luring, and is a crime in Canada.

**Slide 26: Possible Warning Signs**

- offering you bribes, gifts or jobs.
- are overly affectionate and give you lots of compliments.
- offer to help you with homework or private problems.
- claim to be in an emergency situation and need you to do something right away.
- try to threaten, intimidate or boss you around.
- go out of their way to try and be friends with you.
- gradually introduce sexual content into conversations.

**Remember:** People may not be who they say they are. Just because someone sounds like they are around your age, does not mean that they are. Adults can pretend to be younger online. Also, adults who seem to be trustworthy can also have bad intentions.

- Here is the experience of a young Canadian girl who met someone online, as reported by CBC:

- This story is based on real events; however, the girl's real name was not released, so we will call her Katrina. In 2003, 12 year old "Katrina" met a boy in a chat room, who said he was 17 years old. They had two different conversations that were sexual in nature, later swapping contact information. He called Katrina, allegedly propositioned her for sex. She hung up and her father called the police ([CBC, 2003](#)).

**Slide 27:**

**Not everyone online has bad intentions...the Internet is a great place to meet new people and make new friends!**

*The point of this lesson is to make you more aware and hopefully inspire you to think critically about things you do online.*

**Slide 28: If someone makes you feel uncomfortable online...**

- stop all contact with the individual and block them if possible.
- save the messages and content if possible (including the person's screen name and email) in case the authorities need to be involved and conduct an investigation.
- tell a trusted adult, such as a parent, school teacher or law enforcement officer.
- You can also contact [www.cybertip.ca](http://www.cybertip.ca) to report anything that is offensive or makes you uncomfortable online.

**Slide 29: Chris**

*Read students the scenario below, and then ask them the following questions. Provide the following answers if the students do not mention them.*

*Chris had been doing some research about sexual assault for his Social Issues class when he came across a website that had pornographic pictures that claimed to be sexual assault pictures. Chris figured this website might not actually be real but he still felt uneasy about the fact that this website existed on the internet.*

1) What would you do if you were Chris?

- Tell a trusted adult
- Note the web address and time/date he found the website
- Report the website to [www.cybertip.ca](http://www.cybertip.ca)

**Slide 30: Report any illegal information you find online to the police**

- Cyber-stalking or harassment
- Internet scams or fraud
- Dangerous and illegal activities, such as bomb-making, terrorism or unlicensed trade of weapons
- Physical threats

- **Hate crimes**
- **Hacking (illegally breaking into individual computers or computer networks)**

*Tell students that while browsing online, there is always a chance you may come across uncomfortable material, or see something that bothers you. The RCMP recommends that you report any of the illegal online situations above to your local police:*

*Illegal situations that are not emergencies should be reported to the Internet Service Provider (ISP) as well as to the police. Most ISPs have Acceptable Use policies that define privileges and guidelines for those using the services and action that can be taken if those guidelines are violated.*

**Slide 31: The REAL deal**

**If you wouldn't do it in person, why do it online?**

**Think critically about what you do online!**

*End the presentation by telling students: everything you do online has consequences offline. If you wouldn't do something in person, then don't do it online.*

**Slide 32: Want more information?**

**Visit [www.deal.org](http://www.deal.org) and we'll show you how to get involved in your school and community!**

**Check out these websites:**

**[www.cybertip.ca](http://www.cybertip.ca)**

**[www.bewebaware.ca](http://www.bewebaware.ca)**

**[www.thinkuknow.com](http://www.thinkuknow.com)**

**[www.media-awareness.ca](http://www.media-awareness.ca)**

**[www.kidshelpphone.ca](http://www.kidshelpphone.ca) (1-800-668-6868)**

*Feel free to contact me if you have any other questions about what was presented today. You can also visit [deal.org](http://deal.org) for more information or email [deal-choix@rcmp-grc.gc.ca](mailto:deal-choix@rcmp-grc.gc.ca). If you would like to promote internet safety in your school or community, check out the Toolbox section of [deal.org](http://deal.org) for more information about how you can get involved! I have provided several other sites you may want to look at for more information. Thanks for inviting me to come talk to you today!*