Think b4 u Post:
Your Reputation and Privacy on Social Networking Sites

INTRODUCTION

This Teacher's Guide provides information to help you get the most out of *Think b4 u Post*. The contents of this guide will allow you to prepare your students before using the program, and to present follow-up activities to reinforce the program's key learning points.

PROGRAM DESCRIPTION

Social networking has transformed our society–many people of all ages now conduct business, interact with friends, meet new people, and take part in financial transactions via social networking sites. While there are tremendous benefits to these opportunities and connectivity, there are also hidden dangers and common pitfalls. Even unintentional or seemingly harmless online actions can damage an individual's security and reputation. This program addresses maintaining one's online persona and privacy in a straightforward, accessible manner, providing tips and making recommendations to stay safe and positive while interacting online.

LEARNING OBJECTIVES

After viewing the program, students will be able to:

- Recognize the benefits and potential pitfalls of social networking

- Enhance decision-making capabilities around online behavior

- Adopt simple activities to increase internet safety

- Recognize and avoid online scams and criminal activity

- Make positive social choices while interacting online

PROGRAM OVERVIEW

Ever been 'tagged' in an unflattering photo? Teased someone online? Forwarded a private post or text? Entered your credit card information or home address into an unfamiliar website? Often, these actions are harmless, and we've all done something like them without giving it much thought. Unfortunately, in other instances, online behaviors like these can negatively affect our reputations, our bank accounts, and our friendships. *Think b4 u Post* uses humor and real-life examples to illustrate not only what to avoid when interacting online, but also to recommend better choices to make. Taking even simple–seemingly obvious–steps can make a considerable difference in maintaining your online reputation and privacy. *Think b4 u Post* doesn't try to limit the fun and practicality of online interaction and social networking sites; conversely, it provides insight to enhance your online experience to keep you texting, posting, and emailing safely for years to come.

MAIN TOPICS

Topic 1: Your Reputation

In this section, *Think b4 u Post* points out that comments, photos, and actions easily forgotten in person can take on a long life of their own when posted online.

Topic 2: Public Exposure

Here, the program encourages viewers to imagine a model audience when posting comments and photos online. What does your online persona say about you?

Topic 3: Your Career

In this section, viewers learn that potential employers and others can access your social networking behavior and will make judgments about you based on it.

Topic 4: Cyberbullying

Even comments meant in a joking way could cause hurt feelings and real emotion. *Think b4 u Post* points out how to avoid and resolve online bullying.

Topic 5: Your Not-So-Personal Information

Here, the program points out that all internet activity leaves an online trail of personal information.

Topic 6: Unwanted Visitors

Identity theft, phishing, viruses, hackers, spammers…the internet sounds like a scary place! In this section, the program alerts viewers to these dangers and recommends ways to avoid them.

Topic 7: Data Mining

What is data mining and how is the data utilized? This section explains this ubiquitous information-gathering technique to viewers.

Topic 8: Online Predators

In this section, the program highlights the very real danger of online criminals and identifies ways to avoid becoming a victim.

Topic 9: The Important Stuff

The program concludes with key tips and information for making the best choices online.

FAST FACTS

- It's easy for an online photo or message to 'go viral,' meaning it can quickly circulate to hundreds or thousands of people without your knowledge.

- Admissions officers and employers check social networking sites and other online sources for information on potential students and employees. Negative or unflattering search results might limit future opportunities for school or work.

- Once something is posted or published online, it's very difficult to remove it entirely.

- Cyberbullying has many potential negative consequences–those bullied have harmed themselves in reaction, and those doing the bullying can be charged with a crime.

- Use caution when filling out applications or making financial transactions online–there are of course many legitimate places to take these actions, but also unsafe sites where personal information may be compromised. Look for the Ver-i-sign icon to verify legitimacy.

- Remember that your online activities are tracked and captured via data mining.

- Use caution when deciding to meet an online acquaintance in person. Tell someone where you are going, bring a friend with you, and select a public place to meet.

- Use good judgment when posting personal photos online–don't post anything you wouldn't want a parent, teacher, or future employer to see. Encourage your friends to use the same good judgment if they are posting photos that include you.

- Avoid logging in to social networking sites–or other sites that require a password–from a public computer. If you do so, ensure that you log out of the site and close the internet browser before you leave.

- Ensure that your social networking settings keep the majority of your personal information private.

VOCABULARY TERMS

Antivirus software: tools to prevent harmful viruses from infecting your computer.

Cyberbullying: using online sources to harass or pick on peers.

Data mining: using someone's internet activity to gather and store information on him or her.

Firewall: computer tool designed to limit access to your computer and to help prevent viruses and hacking.

Geo-location features: ability to broadcast your location in real time via your internet connection.

Identity theft: using information found online to impersonate someone and conduct activities and transactions as that person.

Online predator: criminal who uses the internet to target victims.

Privacy settings: tools to limit access to your personal information and photos online.

Social networking: connecting with friends, peers, and new acquaintances via various internet sites (such as Facebook and Twitter).

Ver-i-sign icon: indication that a website is legitimate and secure.

PRE-PROGRAM DISCUSSION QUESTIONS

1. What social networking sites do you use? How often do you use them?

2. Have you or a friend ever had a negative experience on a social networking site? What happened?

3. Why do you like social networking sites?

4. How has the internet changed the way people shop, job-hunt, and communicate?

5. Have you ever posted a comment or a photo online you later wanted to remove? Were you able to take it down?

POST-PROGRAM DISCUSSION QUESTIONS

1. What are some basic tips for using social networking sites in a safe manner?

2. How might you react and respond if your private personal information were to become public on a social networking site or elsewhere on the internet?

3. How can you protect yourself from becoming a victim of financial crime on the internet?

4. Would you (or have you) consider(ed) dating someone you met online? Why or why not?

5. What are some positive aspects of data mining?

SUGGESTED ACTIVITIES

Older teens and young adults are often quite computer and internet savvy, with years of experience online. However, a new generation of young teens and tweens are eager to join the social networking experience, and they may be less prepared to deal with maintaining personal security and their reputation while online. Viewing *Think b4 u Post*, coupled with their own experiences and history online, should give older students a great foundation of tips and recommendations to share. Ask your students to prepare relevant internet guidance for younger students–this could take the form of a guidebook, an oral presentation, or a filmed video. Students should incorporate relevant personal examples of what to do (and what not to do!) while interacting online. If possible, have your students present / share with the younger group and solicit feedback and reactions.

Considering various online scenarios gives students the opportunity to practice creative writing skills. Ask each student to imagine a challenging or negative interaction that could occur on a social networking site. For example–accidentally posting a private message on a public wall, sharing too much personal information with a stranger, or having an embarrassing photo forwarded around the school. Students should expand on these scenarios–and their resolutions and outcomes–in a creative format of their choice, such as a short story or one-act play. Ask students to infuse their stories with as much realistic detail as possible. Students may choose to share their stories and plays with the rest of the class.

While it's ideal to behave in a manner as to never run into a challenging or negative situation while online, the reality is that many people will find themselves navigating an unfortunate interaction while taking part in social networking. To that end, provide students with the opportunity to practice navigating and troubleshooting sticky online situations. Ask individual students or small groups of students to review various online challenges (you might use the creative writing scenarios from the previous exercise, create and distribute scenarios for the purposes of this exercise, or ask students to write short scenarios and exchange them with each other to solve). For instance, a scenario might read that a new college graduate is preparing to interview for jobs and is concerned about some of the posts and photos in her online profile. Independently or in small groups, students should work through these scenarios, brainstorm a few solutions, and then share these solutions with the rest of the class for additional input.

Not only does compromising your safety and reputation online have personal consequences, there are potential wider legal implications as well. For instance, if you provide your credit card information on an unverified website and someone uses this info to make fraudulent purchases, are you responsible for the charges? Ask students to choose a particular online safety issue (for instance, cyberbullying) and research what, if any, legal consequences could result from being involved. A student looking into cyberbullying, for example, might assess in what instances those bullied have chosen to report behavior to the authorities, and if any charges were filed against those doing the bullying. Students should capture their findings in a short paper and share these reports with the wider class.

ASSESSMENT QUESTIONS

Q1: Gathering information on someone by following his or her online activity is called
      a) phishing
      b) data mining
      c) scamming
      d) cyberbullying

Q2: What percentage of employers utilizes social networking when making hiring decisions?
      a) 5%
      b) 20%
      c) 45%
      d) 100%

Q3: If you believe you've been communicating with an online predator, you should
      a) Immediately log off and delete all communication history
      b) Avoid telling parents or friends
      c) Tell the person you believe he or she is a criminal
      d) Save records or screen shots of your communication to share with adults and possibly
         police

Q4: Using geo-location features on social networking sites allows others to
      a) view your precise location in real time
      b) access your privacy settings
      c) send you photos
      d) track your online activities and sell the results to advertisers

Q5: True or False: Someone can't forward a photo or message you sent him or her privately without
    your consent.
      a) True
      b) False

Q6: In order to keep your personal information and photos private, you can adjust your settings on
    social networking sites to
      a) open source
      b) public
      c) firewall
      d) private

Think b4 u Post:
Your Reputation and Privacy on Social Networking Sites
Instructor's Guide

Q7: True or False: Once you post something online, it's extremely difficult–sometimes impossible–
to remove it from the internet entirely.
a) True
b) False

Q8: Taking someone's personal information and utilizing it to pose as that person during social or
financial transactions is called
a) going viral
b) firewalling
c) identity theft
d) hacking

Q9: Using the internet and social networking sites to harass, tease, or intimidate others is know as
a) phishing
b) cyberbullying
c) geo-locating
d) posting

Q10: True or False: You can be fired from a job because of something you post online.
a) True
b) False

ASSESSMENT QUESTIONS ANSWER KEY

Q1: Gathering information on someone by following his or her online activity is called
    a) phishing
    b) data mining
    c) scamming
    d) cyberbullying
A1: (b) data mining
Feedback: Information gleaned through data mining is sold to advertisers and retailers, who can then target you for products and services in which you've expressed an interest.

Q2: What percentage of employers utilizes social networking when making hiring decisions?
    a) 5%
    b) 20%
    c) 45%
    d) 100%
A2: (c) 45%
Feedback: Not only do employers access social networking sites when making hiring decisions, they can also choose to rescind job offers based on online behavior.

Q3: If you believe you've been communicating with an online predator, you should
    a) Immediately log off and delete all communication history
    b) Avoid telling parents or friends
    c) Tell the person you believe he or she is a criminal
    d) Save records or screen shots of your communication to share with adults and possibly police
A3: (d) Save records or screen shots of your communication to share with adults and possibly police
Feedback: While it can be embarrassing to admit that an online acquaintance actually may be a criminal or scam artist, taking the action of reporting his or her behavior can help protect others in the long run.

Q4: Using geo-location features on social networking sites allows others to
    a) view your precise location in real time
    b) access your privacy settings
    c) send you photos
    d) track your online activities and sell the results to advertisers
A4: a) view your precise location in real time

Q5: True or False: Someone can't forward a photo or message you sent him or her privately without your consent.
>   a) True
>   b) False

A5: (b) False

Feedback: Not only can someone forward your messages and photos, but nothing is stopping the next recipients from continuing to forward on to their friends. This is how online photos and videos go viral.

Q6: In order to keep your personal information and photos private, you can adjust your settings on social networking sites to
>   a) open source
>   b) public
>   c) firewall
>   d) private

A6: (d) private

Feedback: Social networking sites give you the option to keep your photos and messages accessible only to those you specifically indicate can view them. This allows you to control access to your personal data.

Q7: True or False: Once you post something online, it's extremely difficult–sometimes impossible–to remove it from the internet entirely.
>   a) True
>   b) False

A7: (a) True

Feedback: Always give thought to what you post online and consider who might see it, even years down the line. It's hard to take back something you've posted to the web.

Q8: Taking someone's personal information and utilizing it to pose as that person during social or financial transactions is called
>   a) going viral
>   b) firewalling
>   c) identity theft
>   d) hacking

A8: (c) identity theft

Feedback: If you make purchases online using credit card or bank information, ensure you keep a close watch on your accounts to quickly spot any unauthorized transactions.

Q9: Using the internet and social networking sites to harass, tease, or intimidate others is know as
  a) phishing
  b) cyberbullying
  c) geo-locating
  d) posting

A9: (b) cyberbullying

Feedback: Cyberbullying–even when it's not intended as such–can have serious consequences. Ensure you stay positive when interacting with others online and avoid any personal attacks.

Q10: True or False: You can be fired from a job because of something you post online.
  a) True
  b) False

A10: True

Feedback: You may think what you do on your time outside of work doesn't concern your employer, but there have been instances of employees facing disciplinary action and even being fired based on their online activities.

ADDITIONAL VIDEO RESOURCES

7 Ways to Block a Cyberbully
Cyberbullies stay hidden behind technology and target students on the Internet and through cell phones. This video will help students learn how to avoid—and, if necessary, deal with—cyberbullying situations. Seven effective strategies for coping with a digital bully are outlined: understanding the e-bully; protecting passwords; guarding personal information; using safety software; cutting off communications; saying "No" to revenge; and telling someone. In addition, a special segment called "Cyberbully: The Adult Role" describes seven ways parents and educators can get involved in stopping cyberbullying. Viewable/printable educational resources are available online. (20 minutes) CC

Item#: BVL41237
Copyright date: ©2008
DVD ISBN 978-1-61616-781-3
3-Year Streaming

Dangers of Social Networking Video Clip Collection

No one doubts the power of social media to create positive connections among people who might otherwise never meet. But that same power has an ominous side. It can draw together individuals who should, in fact, not meet—such as predatory adults and gullible minors. It can facilitate bullying, emotional trauma, and cybercrime. And it can be highly addicting. This collection of five ABC News segments examines the issues in ways that are sure to spark discussion and further study. Contains mature content. Viewer discretion is advised. Clip duration ranges from 2 to 6 minutes.

Video clips include-

• Facebook Stole My Identity: The story of a teenager who had his Social Security number and financial information hijacked after playing an online game.

• Kicking Teens' Facebook Addictions: Profiles of teens who have become "hooked" on Facebook, followed by a discussion with online safety expert Parry Aftab.

• Cyberbullying Blamed for Teen's Suicide: Did Facebook harassment cause a 15-year-old to take her own life? Fellow students and Internet safety expert Parry Aftab comment

• The Dangers of Facebook: A report on several cases in which unsuspecting Facebook users were manipulated into dangerous and sometimes deadly situations.

• Chatroulette—Talking to Strangers: Inside a new online craze which connects users at random, enabling both harmless and explicit chat. It is free and open to minors. (23 minutes) CC

Item#: BVL43505
Copyright date: ©2010
DVD (Chaptered) ISBN 978-1-61733-535-8
3-Year Streaming

Growing Up Online

To study the impact of the Internet on adolescence, it helps to examine the subject through the eyes of teens and their parents. This episode of *Frontline* enters the private worlds that young people, for better or worse, are creating online. In doing so, it brings viewers face-to-face with issues that kids confront every day—bullying, harassment, alienation, sexuality, and even bizarre forms of celebrity. Viewers are enabled to explore the complicated and often nebulous lines being drawn between the real and virtual worlds and how these new paradigms are affecting today's impressionable minds. Distributed by PBS Distribution. (60 minutes)

Item#: BVL40893
Copyright date: ©2008
3-Year Streaming

CyberEthics

Most people learn traditional standards of behavior and respect for others by the time they are teenagers—but many don't realize that those rules are just as valid in cyberspace. This program helps students take the high road on the information superhighway and avoid the temptations of the fast lane, pointing the way toward an ethically sound Internet presence and lifestyle. Guidelines for the use of intellectual property are featured, with emphasis on the consequences of illegal downloading, copyright infringement, and plagiarism. Pornography, gaming sites, chat rooms, and online social networks are also discussed, helping viewers steer clear of antisocial and abusive activities, especially cyber-bullying. Comments from experts, as well as questions from peers who are confused about the fine points of cyber legality, serve to clarify central ethical principles. A viewable/printable instructor's guide is available online. Correlates to National ISTE Technology Foundation Standards for Students. A Cambridge Educational Production. (14 minutes) CC

Item#: BVL38816
Copyright date: ©2008
DVD (Chaptered) ISBN 978-1-4213-8838-0
3-Year Streaming

Securing the Web

The consequences of lax Internet security are severe! Use *Securing the Web* to awaken your students to the very real dangers posed by online security threats. In this video, a couldn't-care-less computer user is transported into his PC where he learns firsthand about phishing and pharming, spyware and adware, viruses and Trojans, and denial-of-service attacks and zombie networks. Weapons in the security arsenal—firewalls, antivirus software, software patches and updates, strong passwords, encryption protocols—are also profiled. This is vital information disguised as a darkly humorous sci-fi action drama. Viewable/printable educational resources are available online. (31 minutes) CC

Item#: BVL40211
Copyright date: ©2006
DVD (Chaptered) ISBN 978-1-60825-338-8
3-Year Streaming

ADDITIONAL INTERNET RESOURCES

FBI–A Parent's Guide to Internet Safety
http://www.fbi.gov/stats-services/publications/parent-guide/parent-guide

FTC - Social Networking Sites: Safety Tips for Tweens and Teens
http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

Teen Safety in Cyberspace
http://edis.ifas.ufl.edu/fy848