### Virginia RULES

# Technology and You



### Lesson goal

To improve students' understanding of some of the difficulties posed by technology, including hazards on the Internet and the dangers and consequences of sexting and cyberbullying.

### Students will learn:

- Virginia laws designed to protect Internet users
- Hazards on the Internet
- Laws relating to cyberbullying and sexting
- Strategies for safe Internet use

### Computer crimes

Many sections of the *Code of Virginia* address computer crimes. Internet Safety Laws touch on:

- Fraud
- SPAM or "junk mail"
- Computer trespass
- Invasion of privacy using a computer or computer network
- Using a computer to access information using deception

### Computer crimes, cont.

- Theft of computer services
- Personal trespass by computer
- Using a computer to harass another
- Child exploitation
- Posting/texting/disseminating nude/partially nude photos

Virginia law also makes it clear that, in addition to the criminal penalties, anyone injured by a computer crime may sue to recover damages.

### Computer use

- § 22.1-70.2 of the *Code of Virginia* addresses Internet use policies for public and private schools.
- Virginia was the first state to require Internet safety programs in all schools.

### **SPAM**

§18.2-152.3:1(A) of the *Code of Virginia* makes it a **Class 1** misdemeanor to use a computer or computer network with the intent to falsify or forge electronic mail transmission information in connection with the transmission of unsolicited bulk electronic mail ("SPAM").

### Computer trespass

§ 18.2-152.4 of the *Code of Virginia* prohibits computer trespass by making it a **Class 1** misdemeanor for any person, with malicious intent, or through intentionally deceptive means and without authority, to do any of the following:

- temporarily or permanently remove, halt, or disable any computer data, computer programs or computer software from a computer or computer network;
- cause a computer to malfunction, regardless of how long the malfunction persists;
- alter, disable, or erase any computer data, computer programs or computer software;
- effect the creation or alteration of a financial instrument or of an electronic transfer of funds;

### Computer trespass, cont.

- use a computer or computer network to cause physical injury to the property of another; or
- use a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network.
- install or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another; or

### Computer trespass, cont.

• install or cause to be installed on the computer of another, computer software for the purpose of (i) taking control of that computer so that it can cause damage to another computer or (ii) disabling or disrupting the ability of the computer to share or transmit instructions or data to other computers or to any related computer equipment or devices, including but not limited to printers, scanners, or fax machines.

This crime is a Class 6 felony (one to five years imprisonment) if any of these actions cause damage to another person's property valued at \$1,000 or more or if you install, or cause to be installed, software described above on five computers or more. It is also a Class 6 felony if any such actions target the government or utility company computers or networks.

### Harassment

A key law designed to protect you while you are online is §18.2-152.7:1, harassment by computer, which states:

• If any person, with the intent to coerce, intimidate, or harass any person, shall use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act, he is guilty of a Class 1 misdemeanor.

This type of illegal behavior is referred to as **cyberbullying** and may include **cyber-stalking**.

# Cyberbullying

Bullying is an aggressive behavior that is intentional, involves an imbalance of power or strength, and is usually repeated over time.

Bullying that uses technology is called **cyberbullying**, and can involve:

- Sending mean, vulgar, or threatening messages or images;
- Posting sensitive, private information about another person;
- Pretending to be someone else in order to make that person look bad; or
- Intentionally excluding someone from an online group.

# Cyberbullying, cont.

#### Cyberbullying can occur through:

- Social media including Facebook, Instagram, Snapchat, Twitter, and TikTok
- Direct messaging on social media or other online messaging services
- Texts; including words and digital images
- Blogs or webpages
- Chat rooms or discussion groups; or
- Other information communication technologies

### Cyberbullying, cont.

- In 2019, 13.91 percent of high school students in Virginia said they were electronically bullied
- 15 percent of students ages 12 to 18 said they had been bullied online or by text
- In 2019, the National Center for Education Statistics and Bureau of Justice indicated that about 15.7 percent of students in grades 9-12 experiences cyberbullying on a national basis.

# Cyberbullying, cont.

- 20.4 percent of female students in grades nine through twelve said they had been electronically bullied during the previous 12 months, as compared to 10.9 percent of male students. This means almost twice as many female students experienced cyberbullying as male students.
- 26.6 percent of students identifying as gay, lesbian, or bisexual reported being electronically bullied, which was higher than the percentage of students identifying as heterosexual (14.1 percent).
- Students who participated in the 2019 survey, experienced cyberbullying through texting, Instagram, Facebook, and other social media.

## Sexting

- The National Center for Missing and Exploited Children (2009) defines sexting as "youth writing sexually explicit messages, taking sexually explicit photos of themselves or others in their peer group, and transmitting those photos and/or messages to their peers."
- It is against the law in Virginia to produce, reproduce, store, or share lewd or explicit pictures or videos of minors. Many of these images are classified as child pornography. (Code of Virginia §§ 18.2-374.1 and 18.2-374.1:1).

### Sexting, cont.

- It may start as a joke or an image sent between boyfriend and girlfriend, but sexting has **serious consequences**.
- Legally, taking such photos, sharing them, or just knowingly having the images on your cell phone can be classified as a felony. This can mean years in prison and having your name on the sex offender registry for the rest of your life.
- You may also be suspended from school, dismissed from jobs or other organizations, denied admission to college, and lose jobs and other opportunities later in life.

### Sexting, cont.

- Nearly 1 in 7 children ages 9-12 shared their own nude photos in 2020, and there was a sharp increase of children who admitted seeing a non-consensually re-shared nudes of others;
- 1 in 5 girls ages 13-17 shared their own nudes;
- 1 in 10 boys ages 13-17 shared their own nudes;
- 40% of teens (13-17) agreed "it's normal for people my age to share nudes with each other;"

## Sexting, cont.

- 25% of 9-17 year olds reported having an online sexually explicit interaction with someone they believed to be an adult;
- The number of "sexts" children attempted to send (including girls as young as 6) rose 183% during the COVID lockdown; and
- Nearly 40% of children have received and/or sent a "sext" by the age of 13.

<u>https://enough.org/stats\_social\_media</u> (Enough is Enough: Making the Internet Safer for Children and Families. Accessed June 28, 2022)

### Sexting, cont.

How can you avoid this very serious crime?

- Think about the consequences of taking, sending, or forwarding a sexual picture of someone underage, even if it's of you.
- Never take images of yourself that you wouldn't want everyone — classmates, teachers, family and employers to see.
- Before hitting SEND, remember that you can't control where this image may go.

## Sexting, cont.

How can you avoid this crime, cont.

- Don't hit forward if you forward a sexual picture of someone underage, you are as responsible for this image as the original sender. You could face child pornography charges, go to jail and have to register as a sex offender.
- Report any nude pictures you receive to an adult you trust.
  Do not delete the message. Instead, get your parents or
  guardians, teachers and school counselors involved
  immediately.

### **Expectation of privacy**

It is unlawful for a person to publish on the Internet a videographic or still image made in violation of the current law prohibiting filming, videotaping, or photographing a nonconsenting person in certain situations where there is an expectation of privacy.

This is a **Class 6** felony when the violation involves a person under 18. (Code of Virginia § 18.2-386.1).

### Strategies for staying safe online

#### E-mails from unknown persons or businesses

#### Danger:

 May contain computer viruses and "worms" that can damage your computer.

#### Strategies:

- Do not open these e-mails at all.
- Never open any attachments.

### Strategies for staying safe online

#### **Phishing**

#### Danger:

 You can accidentally give away valuable personal information like a password, social security number, bank account number or credit card number to a criminal pretending to "verify" information.

#### Strategies:

- Do not provide personal information unless you are absolutely sure a website is legitimate and secure.
- Don't respond to unsolicited e-mails.

### Strategies for staying safe online

#### Social Media

#### Danger:

 Social media posts and messaging can be used to harass someone or to engage in inappropriate or sexually explicit conversations. SPAM can also be sent through social media messages. Usually this appears in the form of someone from the user's friend list sending a link and telling the user to click on it.

### Strategies for staying safe online

#### Social Media, cont.

#### Strategies:

- Only message and add to your friend list people you know in real life and who are approved by your parents.
- Use privacy settings to limit contact to only those on your friend list.
- Make sure you are familiar with the blocking features available on most social media websites and report and block unknown senders.

### Strategies for staying safe online

#### Posting videos or photographs online

#### Danger:

- Digital files can easily be saved and distributed to other people, beyond the circle of trusted friends and family.
- Saving, sending and posting any images that are sexually provocative or inappropriate may have serious legal and lifetime consequences.
- Employers and colleges are increasingly checking the web for images of, or information about, job applicants.

### Strategies for staying safe online

#### Posting videos or photographs online, cont.

#### Strategies:

Assume that anything sent or posted online is there forever.

- Ask yourself "Would I be embarrassed if my friends or family saw these pictures or videos?" If the answer is yes, stop.
- Be aware of what is in the camera's field of vision and remember to turn it off when not in use.
- Do not send or post identity-revealing or sexually provocative photographs.
- Do not post photos of friends without their parents' permission.
- If you receive an inappropriate image, do not delete it, but show it to a trusted adult.

### Strategies for staying safe online

# Here are some general tips from the National Crime Prevention Council for staying cyber-safe:

- Never post or share your personal information online.
- Never share your Internet passwords with anyone, except your parents.
- Never respond to messages from unfamiliar persons.
- Never enter an online area that charges for services without getting your parents' permission first.
- Never meet face-to-face with anyone whom you only know online.
- Talk to your parents about what you do online.

### Strategies for staying safe online

Complete the activity in "What Would YOU Do Staying Safe Online"

### Review and Recap

#### You have learned:

- That there are many Virginia laws addressing computer crimes and that some of these laws are specifically intended to help protect you while you are online;
- That bullying using a computer takes many forms and is called cyberbullying;
- What sexting is and how it violates Virginia law; and
- That there are risks associated with being online, but there are strategies you can use to reduce those risks.

### Virginia RULES



#### OFFICE OF THE ATTORNEY GENERAL

COMMONWEALTH OF VIRGINIA • WWW.AG.VIRGINIA.GOV

For more information about Virginia laws that affect teens, visit virginiarules.org