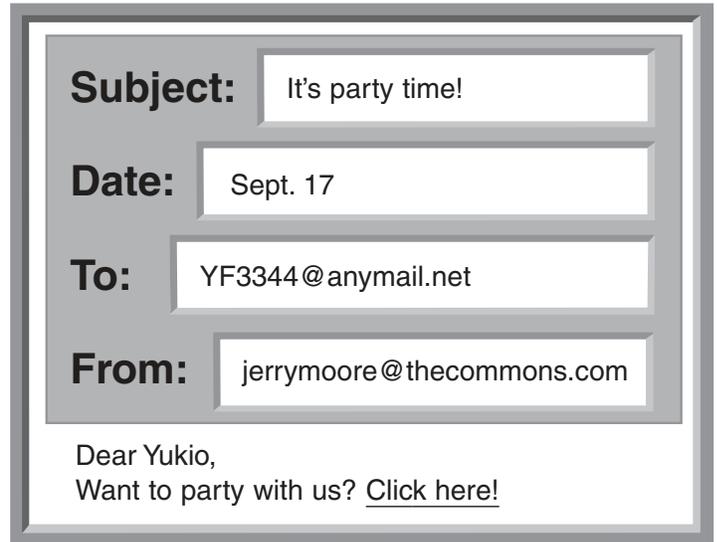Name _____ Date _____

Smart, Safe, and Secure Online

One day, Yukio gets a message online. Assuming it's from a friend, he opens it. Without much thought, Yukio clicks on the hyperlink. It takes him to a Web site showing photos that startle him. Embarrassed, Yukio tries to exit the site. However, new windows keep popping up. Finally, he quits his browser program and deletes the message. He wonders if he did something wrong.

Would it have helped if Yukio had checked who sent the message? Explain.

_____

_____

_____

_____

Subject: It's party time!

Date: Sept. 17

To: YF3344@anymail.net

From: jerrymoore@thecommons.com

Dear Yukio,
Want to party with us? Click here!

Yukio also wonders how the sender found him. What do you think?

_____

_____

Chat With jerrymoore

It's party time!

Dear Yukio,
Want to party with us?
Click here!

How should Yukio handle messages from unknown senders in the future?

_____

_____

_____

_____

_____

_____

Name _____ Date _____

We've Got Spam for You!

Thinking the message must be from a schoolmate, Yukio was excited to get a party invitation. In his haste, he ended up at an X-rated Web site. Had he checked who sent the message, he might have realized that it was from someone he did not recognize. Or he might not have. That's because the sender was trying to trick him into opening the message. It was from a company trying to sell things by sending out thousands of messages at a time. Commercial messages that you didn't ask for are called *spam*.

Many spam offers sound too good to be true ("Make $10,000 a day from home!"), and usually they are! Others may contain messages, pictures, or links to Web sites that are offensive.

These companies (called *spammers*) don't know if you're an adult or a kid—everyone gets the same messages. They collect e-mail addresses and screen names from many sources, including chat rooms, message boards, and social network profiles. Sometimes they just guess, and often they're correct.

Don't Read, Don't Reply

When you read spam, the spammer knows your address is "live." So if you don't know the sender, don't even open or click on the message— even if it includes your name. Simply delete the e-mail or close the IM. If you do read the message, never reply—even to say "Take me off your list." This only encourages the spammer to send more messages.

Beware of Attachments and Free Downloads!

Spam may seem like no big deal, but it can create very real trouble for you and your family. These messages may have *malware* attached. Malware is <u>mal</u>icious soft<u>ware</u>, created to damage your personal files or your computer, or steal your private identity information. There are many types of malware, of which viruses are one type. Sometimes the malware is hidden in a picture (also called an *image*). So don't download images or other attachments unless you know the sender and what is in the attachments.

Everyone likes the free animations, screen savers, and games you can find online. But think twice before downloading free software. It may be hiding malware. Unless the free software is from a site you and your family trust, don't download it.

CyberSmart! ®
21st century skills
for education
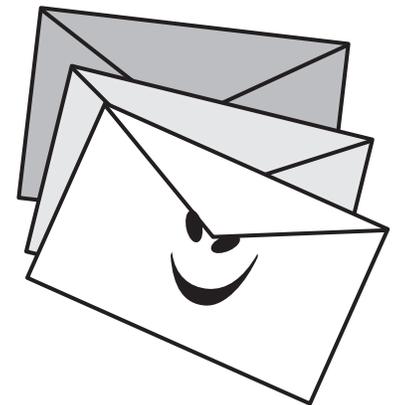
Break the Chain!

You know those messages that ask you to forward them to all your friends? They may contain jokes, sad but heart-warming stories, or warnings about dangers that are not true. Such messages are called Internet chain letters. The message comes from a friend, but its content has been passed all over the Internet—possibly for years. Chain letters can hide malware that your friend didn't realize was there. So don't download a file attached to chain letters, and don't forward the message!
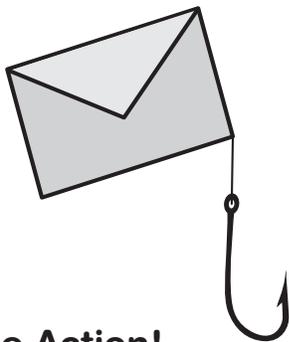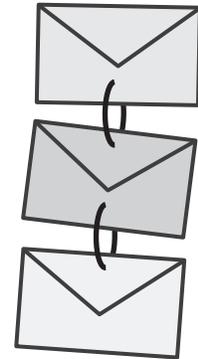
Spam Gone Phishing

Some spammers want to steal your private identity information. Such messages appear to come from places you know and trust, such as a bank or online store. The message may ask you to update your account information by clicking on a link. The link takes you to a phony Web site that looks exactly like the real thing. This trick is called *phishing*. Don't fall for it.

Take Action!

Create a cyber security cartoon or comic strip to hang at home. It can be serious or funny—as long as it makes the point about staying safe and secure online. Sketch and write your ideas below.

Be CyberSmart! ®

Help your family fight spam and malware.

Always

• back up your computers

• update your operating system

• use and update antivirus and other security software

• be sure you know what new software does before you install it

• report spam or phishing to your ISP (Internet Service Provider)