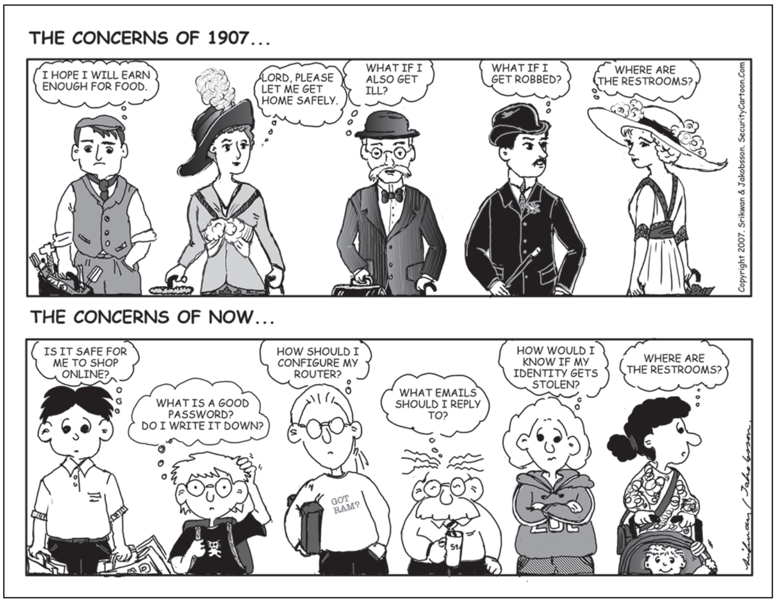
Introduction

Your students no doubt began hearing about Internet safety as soon as they were old enough to begin spending time online. But they may not realise that just as they take risks when crossing a busy street, riding a bike, playing a sport or driving a car, they also take risks when using the Internet. Many students may think they're experienced enough to know what the risks are, and are smart enough to avoid them, but research shows that this isn't the case for most students, because risks may not always be obvious.

Safe Practices for Life Online offers practical advice to help your students stay safe online by making better choices and minimising their risks. The purpose of this guide is to help your students understand *all* the issues and be "Web smarter".


THE CONCERNS OF 1907...
I HOPE I WILL EARN ENOUGH FOR FOOD.
LORD, PLEASE LET ME GET HOME SAFELY.
WHAT IF I ALSO GET ILL?
WHAT IF I GET ROBBED?
WHERE ARE THE RESTROOMS?
Copyright 2007. Srikwan & Jakobsson. SecurityCartoon.Com
THE CONCERNS OF NOW...
IS IT SAFE FOR ME TO SHOP ONLINE?
WHAT IS A GOOD PASSWORD? DO I WRITE IT DOWN?
HOW SHOULD I CONFIGURE MY ROUTER?
GOT RAM?
WHAT EMAILS SHOULD I REPLY TO?
HOW WOULD I KNOW IF MY IDENTITY GETS STOLEN?
WHERE ARE THE RESTROOMS?

People's concerns change over time

(Reprinted with permission. For more material, please visit www.SecurityCartoon.com.)

The authors have a combined experience of more than 50 years working with students, and since 1997 we've focused our attention on understanding the online issues that affect children and teens. We've surveyed and spoken to thousands of students about their Internet behaviours and experiences, and we've heard from teachers and administrators from dozens of schools about the issues they face related to their students' use of the Internet.

Here's an example of how students can create a very secure, yet easily remembered, password:

1. Use the first five words of the Australian National Anthem – "Australians all let us rejoice" – to create the acronym *aalur*.

2. Add two numbers that mean something to you, such as your grandmother's street address.

3. Play with UPPERCASE and lowercase, substitute @ for A, and add an = to create: *22=A@LuR!*

Other good examples:

!mYdoG8it=	(from "My dog ate it")
@DvaUfa!r	(from "Advance Australia Fair")
=bB3$t$!	(from "Better be safe than sorry")

Teach your students other methods they can use to develop secure passwords by working through **Exercise 1.8 – Create an Uncrackable Password**, and **Exercise 1.9 – Same Directions, Different Passwords**, which illustrates the variations possible in password creation. The PC Tools website (www.pctools.com/guides/password/) also has a secure password generator that allows you to change certain components of the password it creates for you. Once students have created their new passwords, **Exercise 1.10 – Test Your Password** gives them the opportunity to check their passwords through the Password Strength Checker at Cornell University.

Here's a home project for your students. Tell your students that their assignment is to teach their parents or guardians what makes a good or bad password. Tell them to make sure that their parents aren't using their children's names or birth dates anywhere in their passwords. Have the students encourage their parents to create new passwords for their online accounts using the skills the students learned today. Many of your students may be surprised to find that their parents have rather poor password-creation skills. This project helps students retain and practise the skills they've learned in this chapter, and it will help generate discussion at home around these security issues.

Students may not know what poses the greatest risks to their online security. **Exercise 1.11 – How'd They Do That?** asks students to consider the most and least common account security issues. Through this exercise students will find out that the biggest threat to their online

Exercise 1.4

Does Your Screen Name Give Away Information?

Students sometimes choose screen names that give away too much information about them. Ask your students what information the following screen names reveal:

Tom_Evans34

Missy-13

AndyKarateKid

ViolinGurl

restlinmatch

Exercise 1.5

Good and Bad Choices for Screen Names

Ask your students to look at the following screen names. Have them discuss whether they think these are good choices or poor choices, and explain why.

i8sushi2
Soccerstar
Puppygirl234
KeKe1995
Bookworm
2BorNot2b
Choco-holic
CapitlOfens

AmrcanIdol2
BellaIsabella
DarkAngel666
Karla-Love-1996
SimplyMe
gUn4hiRe
babyfaceLA
Watup?

SimplyMe, 2BorNot2B and Watup? are good choices from the list. Bookworm, i8sushi2, AmrcanIdol2, Soccerstar and Choco-holic may still be reasonably good choices, though you should point out that they do reveal something about the interests of the user. The other names listed are poor choices because they're provocative, reveal too much information or may attract unwanted attention.

Tools to Protect Your Privacy

Many tools and security suggestions are available to help your students protect their privacy online. Review each of the following items with your students. They can then check to see which are currently in use on their home computers and report back to you.

1. **Anti-virus protection software**
   Ask students if all of their home computers have had anti-virus software installed. If so, is their anti-virus subscription up to date? When was the last time it downloaded virus definitions so that their software could recognise the latest Internet viruses, worms, Trojan horses and attacks? (Note: Though Apple Macintosh viruses are rare, Apple computers can still pass on viruses to friends or family who have Windows operating systems on their computers.) AVG (http://free.avg.com/) and ClamWin (www.clamwin.com) produce a free, basic anti-virus application for PCs. ClamXav (www.clamxav.com) is a free anti-virus application for the Macintosh operating system.

2. **Anti-spyware protection software**
   It is recommended that PC users with the Windows operating system have two different anti-spyware software programs running on their computers simultaneously. Unfortunately, some anti-spyware software is useless, and some of it is actually disguised spyware. Which software can students trust? A great place to look for unbiased information about effective anti-spyware is Spyware Warrior (www.spywarewarrior.com). In the past they have recommended free products from:

   - Windows Defender:
     http://www.microsoft.com/windows/products/winfamily/defender/default.mspx
   - Ad-Aware, by Lavasoft: http://www.lavasoft.com/
   - Spybot – Search & Destroy: http://www.safer-networking.org/en/index.html

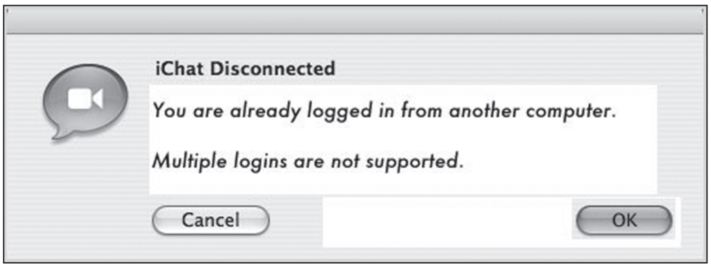
3. **Operating system and web browser updates and patches**
   This is valuable protection for both Mac and PC owners. Students must keep their computer operating system and web browser software updated. Some web browsers, such as Firefox, will update automatically, just like the operating system.

4. **Web browser security settings**
   Tell students: Don't leave your security settings on low. Crank them up to high!

Anna's Story

Anna couldn't wait to get home and log on. She'd had a horrible day at school and was desperate to talk to her best friend, Shelley. Bolting up the stairs two at a time, she slammed the door to her room and turned on her laptop. One hand scratching her cat's ear and the other guiding the mouse, she launched her IM software, all the while thinking that no matter how fast computers got, they were never fast enough for her. She typed out her eight-character password and hit enter. Instead of seeing her usual buddy list, Anna was startled to see an error message that alarmed her (Fig. 3.1).

Who was online pretending to be her? Anna picked up the phone to call Shelley.



iChat Disconnected

You are already logged in from another computer.

Multiple logins are not supported.

Figure 3.1 Is someone impersonating you online?

Identity Theft

Identity theft occurs when someone steals or otherwise obtains and uses a student's personal information, pretends to be that student online, and logs into the student's personal accounts.

Since early 2005 there has been a dramatic increase in the occurrence of identity theft and identity impersonation among students online. Take a quick survey of your class. Ask your students:

1. How many of you know someone who has had his or her online accounts used by another (unauthorised) person?
2. How many of you know someone who pretended to be another student online?