



# Learning to Learn eCourse

## Module 5: Risks and Dangers

### Handout

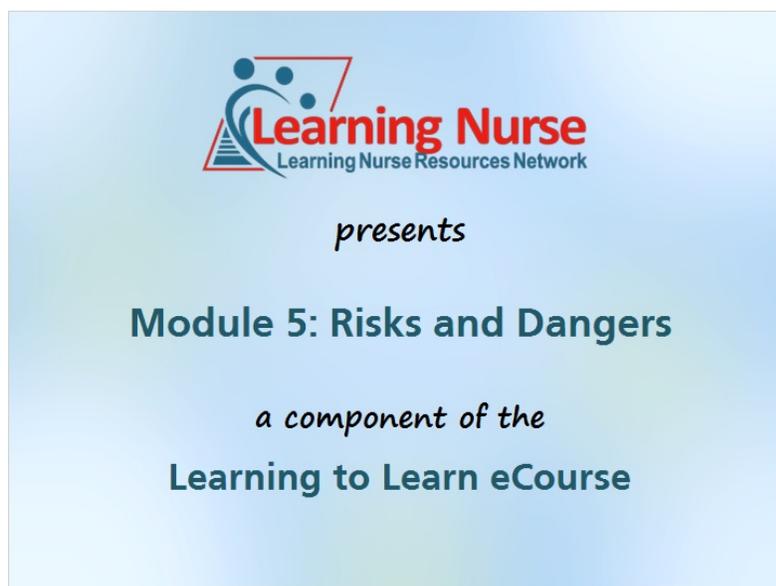
© 2018 – 2019 Steppingstones Partnership, Inc. / Learning Nurse: All Rights Reserved

See: *Terms of Use* at [LearningNurse.org](http://LearningNurse.org) for acceptable uses

# Learning to Learn eCourse – Module 5: Risks and Dangers

## 1. Module 5: Risks and Dangers

### 1.1 Welcome



MENU
<a href="#">Module Topics</a>
<a href="#">Identity Theft</a>
<a href="#">Infection Control</a>
<a href="#">Personal Safety</a>
<a href="#">Privacy &amp; Confidentiality</a>
<a href="#">Unethical Conduct</a>
<a href="#">Professional Boundaries</a>
<a href="#">Malware</a>
<a href="#">Avoiding Malware</a>
<a href="#">Summary</a>

### Narration

No narration, only music.

## 1.2 Topics

Topics	MENU
<p><i>Identity theft</i></p> <p><i>Infection prevention &amp; control</i></p> <p><i>Personal safety</i></p> <p><i>Privacy and confidentiality</i></p> <p><i>Unethical conduct</i></p> <p><i>Professional boundaries</i></p> <p><i>Malware</i></p>	<p>Module Topics</p> <p>Identity Theft</p> <p>Infection Control</p> <p>Personal Safety</p> <p>Privacy &amp; Confidentiality</p> <p>Unethical Conduct</p> <p>Professional Boundaries</p> <p>Malware</p> <p>Avoiding Malware</p> <p>Summary</p>



## Narration

**JILL:** Welcome to Module 5 of this *Learning to Learn* course. In this module, we will discuss some of the major online risks and dangers and provide suggestions as to how to protect yourself.

**CARLOS:** Hi Jill. What are the specific topics that we will be covering?

**JILL:** The specific risks and dangers that we are going to discuss are: identity theft, infection prevention and control, personal safety, privacy and confidentiality, unethical conduct, professional boundaries, and the different types of malware.

**CARLOS:** Sounds important.

**JILL:** Yes it is.

## 1.3 Identity theft

### Identity Theft

*Obtaining and using another person's online personal information*

*Limit sharing personal information*

*Learn about and avoid online scams*

*Manage privacy settings*

*Use strong passwords and change regularly*

*Maintain up-to-date antivirus software*

### MENU

[Module Topics](#)

[Identity Theft](#)

[Infection Control](#)

[Personal Safety](#)

[Privacy & Confidentiality](#)

[Unethical Conduct](#)

[Professional Boundaries](#)

[Malware](#)

[Avoiding Malware](#)

[Summary](#)

## Narration

**JILL:** Let's begin with identity theft. Identity theft is simply the act of illegally obtaining an individual's online "personal" information and using it for criminal activities. Here are some common sense suggestions on how to protect yourself from identify theft.

**CARLOS:** Limit the sharing of personal information online. Learn how to identify and avoid scam e-mails and fake websites. Manage your privacy settings on social media and other websites.

**JILL:** Other things you should do is have strong and secure passwords and change them regularly. Also have up-to-date antivirus and spyware protection programs. Be sure that the virus definitions can be updated frequently.

## 1.4 Infection control

### Infection Prevention & Control

*Devices can carry pathogens*

*Avoid use of mobile devices in clinical areas*

*Do not use devices when handling patients*

*Use medical gloves*

*Clean and disinfect hands*

*Clean mobile devices with disinfectants*

### MENU

Module Topics

Identity Theft

Infection Control

Personal Safety

Privacy & Confidentiality

Unethical Conduct

Professional Boundaries

Malware

Avoiding Malware

Summary

## Narration

**CARLOS:** Smartphones and other mobile devices may act as carriers of pathogenic and nonpathogenic bacteria. This is because they are used everywhere including the toilet. Here are some precautions.

**JILL:** Avoid the use of mobile devices in clinical areas and particularly when handling patients. If you are using a mobile device, wear medical gloves. Clean and disinfect hands after handling your smartphone or tablet. And finally, clean your mobile device frequently using disinfectant solutions or wipes.

## 1.5 Personal safety

### Personal Safety

*Risk of psychological or physical harm*

*Avoid giving out contact information*

*Avoid meeting people met online*

*Be careful what you post*

*Be careful what you download*

### MENU

Module Topics

Identity Theft

Infection Control

Personal Safety

Privacy & Confidentiality

Unethical Conduct

Professional Boundaries

Malware

Avoiding Malware

Summary

## Narration

**JILL:** Criminals on the Internet are not always after financial or material gain. In some cases, they have more malicious motives that may cause psychological and even physical harm. For example, Internet users are at risk of being stalked, harassed or physically assaulted by people they have met online. Here are some measures to take to protect your personal safety.

**CARLOS:** Avoid giving out contact information or any other personal information to strangers on the Internet. Avoid meeting people you connect with online unless you can verify their true identity. If you want to meet them, do so in a public place or bring along a friend.

**JILL:** Really be careful about what your post online. And finally, use caution about what you download from the Internet. Verify the information, site and its authenticity. Have your antivirus program scan any downloads.

## 1.6 Privacy

### Privacy and Confidentiality

*Automatically delete cookies after each session*

*Make use of cloud storage encryption*

*Encrypt Internet communications*

*Surf the Internet anonymously*

#### MENU

[Module Topics](#)

[Identity Theft](#)

[Infection Control](#)

[Personal Safety](#)

[Privacy & Confidentiality](#)

[Unethical Conduct](#)

[Professional Boundaries](#)

[Malware](#)

[Avoiding Malware](#)

[Summary](#)

## Narration

**CARLOS:** Privacy refers to the Internet user's right to safeguard his/her personal information from other Internet users. Confidentiality refers to the responsibility of the service provider to protect consumer data from third party access.

**JILL:** To protect your personal privacy online, set your browser to automatically delete cookies after each browsing session. Another good tip is make use of cloud storage encryption. If practical, encrypt Internet communications such as chat and e-mail. And finally, surf the Internet anonymously either using private or incognito windows or a virtual private network (VPN).

## 1.7 Unethical conduct

### Unethical Conduct

*Inappropriate access / use of patient data*

*Digital plagiarism*

*Software theft and breaking copyright*

*Improper use of devices*

*Spreading of malware*

*Creating and distribution of misinformation*

### MENU

[Module Topics](#)

[Identity Theft](#)

[Infection Control](#)

[Personal Safety](#)

[Privacy & Confidentiality](#)

[Unethical Conduct](#)

[Professional Boundaries](#)

[Malware](#)

[Avoiding Malware](#)

[Summary](#)

## Narration

**JILL:** The use of the Internet and other digital technologies has resulted in a surge of unethical behavior. Ethics are moral principles that define acceptable behavior.

**CARLOS:** Some examples of unethical behaviours are: inappropriate access, use and sharing of patients' health information; digital plagiarism; software theft and breaking of copyright laws.

**JILL:** Other examples of unethical behaviours include the improper use of computers and mobile devices such as checking Facebook and Twitter during work hours. Another unethical behaviour is the acquiring and spreading of malware, either intentionally or unintentionally. The Internet also seems to foster the creation and distribution of misinformation or "fake news".

**CARLOS:** These unethical behaviours should be avoided as they may result in unprofessional conduct or criminal proceedings. Also, as a professional you are obligated to report any unethical conduct you observe in your nursing practice.

**JILL:** Yes, that is a good reminder.

## 1.8 Professional boundaries

### Professional Boundaries

*Avoid transmitting patient data*

*No photos on personal devices*

*Limit social media contact with patients*

*Follow guidelines for work-related postings*

*Do not make online negative or offensive remarks or comments*

### MENU

[Module Topics](#)

[Identity Theft](#)

[Infection Control](#)

[Personal Safety](#)

[Privacy & Confidentiality](#)

[Unethical Conduct](#)

[Professional Boundaries](#)

[Malware](#)

[Avoiding Malware](#)

[Summary](#)

## Narration

**CARLOS:** Social media and other Internet technologies may encourage the violation of professional boundaries. Colleagues get an often unwarranted open window into one's personal life. The use of social media in clinical settings may also blur professional boundaries between nurses and patients.

**JILL:** To avoid violation of professional boundaries, do not transmit patient-related information or images that degrade, humiliate or violate a patient's right to privacy.

**CARLOS:** Do not take photos or videos of patients on personal devices. Maintain professional boundaries online. This includes limiting social media contact with patients and their families.

**JILL:** Stay within organizational guidelines and policies for work-related postings. Do not use the Internet to make negative remarks or other comments about employers, co-workers or even instructors. This may be considered unprofessional conduct!

**CARLOS:** Most nursing associations and healthcare employers have policies regarding use of digital technologies. If you are in doubt, become familiar with these policies and adhere to them.

**JILL:** Good point. When in doubt, check it out!

## 1.9 Malware

### Malware

- Viruses
- Adware
- Spyware
- Worms
- Trojans
- Ransomware



### MENU

- Module Topics
- Identity Theft
- Infection Control
- Personal Safety
- Privacy & Confidentiality
- Unethical Conduct
- Professional Boundaries
- Malware
- Avoiding Malware
- Summary

### Narration

**JILL:** Our last section is about malware. Malware is any software that seeks to illegally access, infect and harm a host computer. There are several different types of malware.

**CARLOS:** Viruses are contagious codes that infect software on a host system and spread when software is shared between computers.

**JILL:** Adware is constant, unwanted advertisements on the screen that make reading and navigation difficult.

**CARLOS:** Spyware is a type of malware that spies on a computer user and tracks the user's Internet activities. These are often difficult to detect.

**JILL:** Worms are software that replicates itself and destroys all information and files stored in the host system.

**CARLOS:** Trojans are a type of malware that deceives the user that it is safe. However, the software is programmed to access personal information and take over the host system's resources.

**JILL:** Ransomware is a type of malware that restricts access to the host system's files and information unless the user pays a certain fee.

## 1.10 Avoiding malware

### Avoiding Malware

- Install firewall*
- Antivirus software*
- Anti-spyware*
- Use strong passwords*
- Keep operating systems updated*
- Keep browsers updated*



### MENU

- Module Topics
- Identity Theft
- Infection Control
- Personal Safety
- Privacy & Confidentiality
- Unethical Conduct
- Professional Boundaries
- Malware
- Avoiding Malware
- Summary

### Narration

**CARLOS:** Here are some suggestions and recommendations to protect yourself from becoming a victim of malware.

**JILL:** First of all, install and activate a firewall on your computer or device. Install and keep up to date antivirus and anti-spyware software programs.

**CARLOS:** Use strong passwords and change them regularly. Keep Windows and Apple operating systems up-to-date. Also use the latest versions of browsers. Browser software is regularly updated to address security issues. Make sure you install these latest browser updates.

## 1.11 Summary



## Narration

**JILL:** This brings us to the end of this module on the risks and dangers of the Internet. Carlos, one last time?

**CARLOS:** Sure thing. We identified the risks and dangers of being online, and what you can do to protect yourself. The risks included: identity theft, infection prevention and control, personal safety, privacy and confidentiality, unethical conduct and violation of professional boundaries. We concluded our presentation by examining the different types of malware – viruses, adware, spyware, worms, Trojans and ransomware – and ways to protect yourself against these.

**JILL:** Thanks for doing that. Since this is the last module in the *Learning to Learn* course, Carlos and I would like to thank you for your attention and participation. We wish you success in your lifelong professional development activities and your nursing careers. Goodbye and thanks.

**CARLOS:** Goodbye and thanks from me as well.

## 1.12 The End



## Narration

No narration, only music.