

JROTC Distance Learning Courses

Study Guide

Internet Safety

Distance Learning



Navy Junior Reserve Officer Training Corps

Name: _____

Date: _____

STUDY GUIDE: INTERNET SAFETY

Lesson 1
Screen 3 of 13

Seven (7) practices for safer computing:

1. _____
2. _____
3. Use antivirus and antispyware software, as well as a firewall, and update them all regularly.
4. Be sure to set up your operating system and browser software properly, and update them regularly.
5. _____
6. _____
7. _____

Lesson 1
Screen 5 of 13

Identifying secure web pages:

Webpage	Secure	Not Secure
https://mfa.lanxtra.com/	<input type="checkbox"/>	<input type="checkbox"/>
http://forecast.weather.gov	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>

Lesson 1
Screen 5 of 13

Four (4) ways to prevent identity theft:

1. _____
2. _____
3. _____
4. _____

Lesson 1
Screen 6 of 13

Phishers send _____ or pop-up messages claiming to be from a familiar business or organization – an Internet Service Provider (ISP), bank, online payment service, or even a government agency. The purpose is to trick you into giving personal information.

Lesson 1
Screen 7 of 13

Spyware is _____

Antivirus software is _____

A Firewall is _____

Lesson 1
Screen 9 of 13

Minimum, a password should be _____ characters long.

Minimum, a password should be changed every _____ days.

Lesson 1
Screen 8 of 13

Operating systems and browser setup:

Lessen your risk by changing the settings in your _____ or operating system and increasing your online security. Check the "Tools" or "Options" menus for built-in security features. If you need help understanding your choices, use your "Help" function.

Your operating system may also offer free software called _____ that close holes in the system that hackers could exploit. If possible, test your operating system to automatically retrieve and install patches for you.

If you're not using your computer for an extended period, disconnect it from the Internet. When it's disconnected, the computer doesn't send or receive information from the Internet and isn't vulnerable to _____.

Lesson 2
Screen 5 of 24

Three (3) nationwide consumer reporting companies to contact to place an initial fraud alert on credit reports if Social Security number is stolen:

1. _____
2. _____
3. _____

Lesson 2
Screen 9 of 24

Eight (8) guidelines to follow to avoid online auction and shopping pitfalls:

1. _____
2. _____
3. _____

4. _____
5. _____
6. _____
7. _____
8. _____

Lesson 2
Screen 13 of 24

Seven (7) measures to protect yourself whenever using P2P file-sharing:



1. _____

2. _____

3. _____
4. _____
5. _____
6. _____
7. _____

Lesson 2
Screen 15 of 24

The best defense to avoid “drive-by downloads” and other hazards of HTML is _____

Lesson 2
Screen 16 of 24

Copyright infringement is _____

Lesson 2
Screen 17 of 24

A hacker is _____

A cracker is _____

Lesson 2
Screen 17 of 24

Eight (8) things to do to protect against crackers:

1. Change default administrator passwords and usernames.
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. Position the router or access point safely.

Lesson 2
Screen 19 of 24

Online profiling is _____

REMEMBER: If you suspect that an online stalker knows your actual location it is imperative that an official report be filed with your local law enforcement agency IMMEDIATELY. This is especially true if threats of physical violence are part of the abuse. The one thing known about stalkers is that there is no way to predict how they will act.

Lesson 2
Screen 20 of 24

Online “groomers” are _____

Lesson 2
Screen 20 of 24

Cyber-bullying is _____

REMEMBER: In the United States it is a federal crime to anonymously "annoy, abuse, threaten, or harass any person" via the Internet or telecommunication system. It is punishable by a fine and up to two years imprisonment.

Lesson 2
Screen 22 of 24

Filing a complaint:

If your computer gets hacked or infected by a virus, disconnect from the Internet and scan it with fully updated anti-virus software, and update your firewall. Then notify your Internet Service Provider (ISP) and the hacker's ISP, if you can tell what it is.

Finally, file a complaint with the _____.

If you believe your computer has spyware, file a complaint with the _____.

Lesson 3
Screen 4 of 26

Definitions:

A _____ is a program or algorithm that replicates itself over a computer network and usually performs malicious actions. A worm can use up your computer's resources and possibly shut your system down.

A _____ is a destructive program that masquerades as a benign application. Unlike viruses, these do not replicate themselves. When installed on your computer, these enable unauthorized people to access it and sometimes to send spam from it.

A _____ combines the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities.

An _____ is a utility that searches a hard disk for viruses and removes any that are found.

Lesson 3
Screen 7 of 26

Three (3) ways viruses spread:

1. _____
2. _____
3. _____

Lesson 3
Screen 8 of 26

A cookie is _____

Lesson 3
Screen 9 of 26

Six (6) steps to controlling cookies using Internet Explorer:

1. _____
2. _____
3. _____
4. _____

5. _____
6. _____

Lesson 3
Screen 10 of 26

Four (4) things spyware can do:

1. _____
2. _____
3. _____
4. Open applications and transfer information over the Internet to an unknown third party.

Lesson 3
Screen 13 of 26

Some of the best practices to protect e-mail privacy:

1. _____
2. _____
3. _____

Lesson 3
Screen 14 of 26

Encryption software is _____

Lesson 3
Screen 16 of 26

Five (5) things you can do to reduce spam:

1. _____
2. _____
3. _____
4. _____
5. _____

Lesson 3
Screen 20 of 26

A smurf attack is _____

Lesson 3
Screen 21 of 26

Mobile code is _____

Lesson 3
Screen 22 of 26

Seven (7) best Internet surfing practices:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Lesson 3
Screen 23 of 26

Carnivore and Magic Lantern are data _____ systems.

Name: _____

Date: _____

CHECK YOUR UNDERSTANDING: INTERNET SAFETY

1. Are the following true or false?

_____ It is usually okay to give out your last name, e-mail, home address, account numbers, Social Security Number, or your phone number on the Internet.

_____ If you get an e-mail or pop-up message asking for personal information, don't reply or click on the link in the message.

_____ If you are shopping online, don't provide your personal financial information through a company's website until you have checked that the site is secure, like a lock icon on the browser's status bar or a website URL that begins "https;" (the "s" stands for "secure").

_____ Some scammers forge security icons.

_____ There is no need to read website privacy policies.

_____ Phishers send spam or pop-up messages claiming to be from a familiar business or organization – an Internet Service Provider (ISP), bank, online payment service, or even a government agency. The purpose is to trick you into giving personal information.

_____ File-sharing is risk-free.

2. Match the term to its definition.

_____ Spyware

A. This software protects your computer from viruses that destroy data, slow your computers performance, cause a crash, or allow spammers to send e-mail through your account.

_____ Antivirus Software

B. Installed on your computer without your consent, this software monitors or controls your computer use.

_____ Firewall

C. This is like a guard, watching for outside attempts by hackers to access your system and blocking communications you don't permit.

- 3. How often should you change your passwords?**
- A. Every 30 to 60 days
 - B. Every 90 to 180 days
 - C. Every 7 to 10 days
 - D. Every 180 to 365 days
- 4. If your information has been misused, file a report about your identity theft with the police, and file a complaint with the _____.**
- A. Internet Service Provider (ISP)
 - B. Federal Trade Commission (FTC)
 - C. Federal Bureau of Investigation (FBI)
 - D. Central Intelligence Agency (CIA)
- 5. If you are shopping online, don't provide your personal or financial information through a company's website until you have checked for _____.**
- A. An email address
 - B. An unlocked icon on the browser's status bar
 - C. A website URL that begins https
 - D. A website URL that begins http
- 6. Using _____ allows you to receive email from certain addresses and block others.**
- A. Firewall software
 - B. Anti-virus software
 - C. Filters
 - D. Cookies
- 7. What should you do if your computer gets hacked or infected by a virus?**
- A. Scan your main data folder with anti-virus software that you have on hand.
 - B. Keep your machine connected to the internet to give your friends the heads up.
 - C. Scan your entire computer with fully updated anti-virus and anti-spyware software, and update your firewall.
 - D. Buy another computer, this one is toast.
- 8. What should you do if you get an email or pop-up message asking for personal information?**
- A. Click on the link in the message.
 - B. Don't reply and don't click on the link in the message.
 - C. Reply and forward the link to all your friends so they don't miss out.
 - D. Definitely reply, you could be missing out on a great deal.
- 9. What best describes a firewall?**
- A. It is like a guard, watching for outside attempts to access your system and blocking communications to and from sources you don't permit.
 - B. It allows others to remotely access your computer to help you fix problems.
 - C. It allows spam email to get through, thus protecting your computer from harmful viruses.
 - D. It allows you to make sure online sellers are legitimate.

- 10. A secure website will display a _____ in the bottom right hand corner of your web browser.**
- A. Padlock icon
 - B. Thumbs Up icon
 - C. Shield icon
 - D. Security logo



Navy Junior Reserve Officer Training Corps