**Julia Kovrigin**  **CTP 103**

# Lab 10: Network Security (31 points) PC Version

Objectives:

* Identify security settings on your computer
* Describe how your system is protected from malware and pop-up ads
* Identify common communications ports
* Identify spam phishing and pharming

Note: It is required that you complete this lab using your own computer (not a school computer).

##### Section I: Identify the security settings on your computer – 6 points

Investigate the settings on your computer from protecting it from malware

* Type Defender in the Search box on the Task Bar.
* Select Windows Defender. (If Defender is turned off you will get a message informing you that another security application is monitoring your system – open Security and Maintenance from the Control Panel to view the active malware programs on your computer).
* Read this article: <https://www.microsoft.com/en-us/security/pc-security/windows-defender.aspx>.

1. **(2 points) Describe how your system is protected from malware**: Identify if you use a feature of your operating system, a product such as McAfee or if you don’t use either of these methods. If you don’t use anti-malware software, be sure to explain why you do not see a need for malware protection. I currently use Norton Security to protect my computer.
2. **(2 points) Describe how your system handles pop-up ads:**

Access Internet Options using the Control Panel – Select the Privacy tab

* 1. Is the pop-up blocker on?  Yes  No

Click on the Settings option.

* 1. Are there any exceptions?  Yes  No
  2. Why would we want to allow for some pop-ups? Because you will not be able to access some websites or links when completely turning it off.

1. **(2 points) Describe how your system is protected from unauthorized access:**

Access the Windows Firewall using the Control Panel.

* 1. Is the Firewall on?  Yes  No
  2. If the firewall is off, how does your system protect against unauthorized access? Answer

##### Section II: Testing your system security – 20 points

1. **(2 points)** Go to the [ShieldsUP!](https://www.grc.com/x/ne.dll?bh0bkyd2) web site. Click on the **ShieldsUP!!** logo to enter the web site. Read the section on “**If you are new to this site and our services:**”

Before you click on proceed read the material in the box below it with the heading:

**The text below might uniquely  
identify you on the Internet**

* 1. What is your **machine name**? SER-JUL01
  2. In the second to last paragraph in that box you should see your **IP address**. What is it? 108.28.113.118

Click on **Proceed**

Before you run any scans read the following sections.

* + - Explain this to me
    - Am I really in danger?
    - What can I do about this?

1. **(2 points)** Now that you have read those sections, make sure you are back at the ShieldsUP page.

Click on **File Sharing** in the ShieldsUP!! Services area. What was the outcome? (Please do not use a screen shot here. I’d like you to answer these questions.)

* 1. Does Internet **Port 139 exist** on your system?  Yes  No What does this mean? My machine is deliberately hiding the port for protection.
  2. Was it able to connect to **NetBIOS** on your computer?  Yes  No What does this mean? My computer is not sharing any network protocol information which makes it more secure!

1. **(10 points)** Scroll down the page and click on **Common Ports** in the Shields UP!! Services area. What was the result of the test?
   1. Solicited TCP Packets:  Pass  Fail
   2. Unsolicited Packets  Pass  Fail
   3. Ping Reply  Pass  Fail (Note: often your ISP router firewall will be configured to allow incoming WAN ICMP Echo Requests to remotely connect to your computer causing this test to fail.)
   4. List any ports that are not listed with a **Stealth** status (if there are none, type “none”): None

Click on the following port numbers and indicate the purpose of each and give a brief description (use your own words):

* 1. Port 80: Name http, purpose World Wide Web HTTP. Port used for the www system. Web servers use this port to communicate web browser .
  2. Port 443: Name https, purpose http protocol over TLS/SSL. This port is used for secure data transfer. This port resist eavesdroppers and interception.
  3. Port 110: Name pop3, purpose post office protocol – Version 3. Used by email clients to get the email from the server to the computer.

Click on the “Internet Port Status Definitions” page and give a brief explanation of the following Port definitions:

* 1. Stealth: A port that completely ignores and drops any incoming packets without telling the sender weather the port is open or closed. This leads the intruder to believe that machine is turned off disconnected or not longer exists.
  2. Closed Closed is second best without firewall of nat router. It will reject connection attempts.
  3. Open Packet are being accepted and the prober can connect with your machine.

1. **(4 points)** Click the UPnP Test
   1. What is UPnP? Universal Plug and Play, is a zero configuration networking protocol that handles devises and service discovery and the configuration of consumer devices and networks.
   2. What were your UNnP results? No Response

Read the section “**About UPnP and What it Means**”.

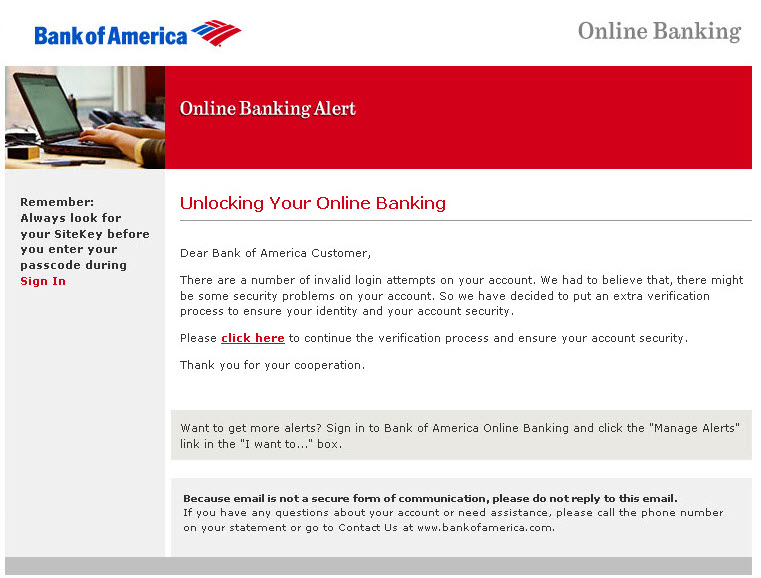
* 1. Is it safe for UPnP to be exposed to the Public network? Why? Or Why not? Not safe, its meant for devises to connect on a private local network not public. It exposes the private network to hackers.
  2. What applications are mentioned as being especially worrisome? Skype BitTorrent and gaming consoles are especially at risk.

1. **(2 points)** Given the results of these tests, explain your system’s intrusion risk. Be specific. Because my system did not respond to the probes this this means it is secure and will help deter probers and hackers.

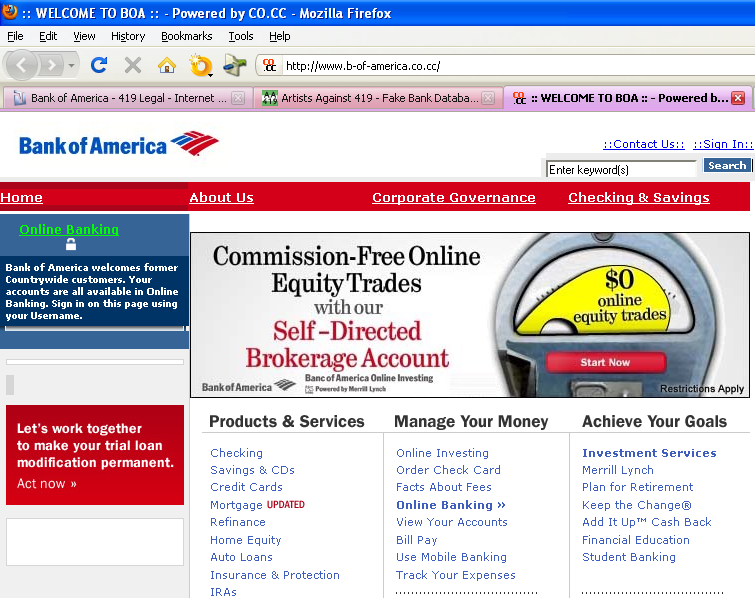
##### Section III - Security Issues Awareness – 5 points

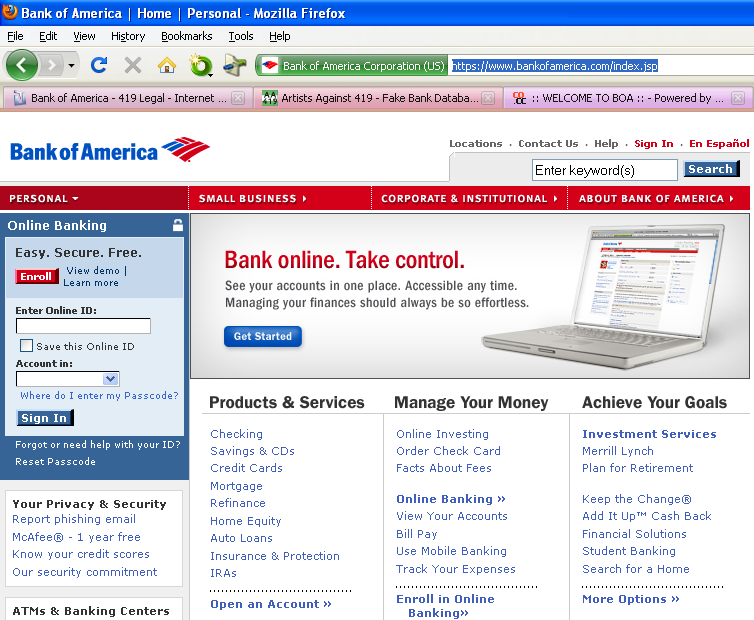
Note: to answer the questions below, you need to understand the difference between phishing and pharming and how to recognize how a website is valid and secure. This is addressed in the chapter and in the PowerPoint for the module.

1. **(3 points)** You receive the e-mail below from your bank. You read the message and become concerned; however, you realize that the message seems suspicious.



1. What should you do? Do not click on the link. Call your bank and report it.
2. This appears to be an example of a(n) Phishing attempt.
3. What made you suspicious? The wording and grammar of the email. It does not sound like a professional email that BOA would send.
4. **(2 points)** Examine the two websites on the next page. One is a fake site and the other is authentic.
   1. Which one is the authentic site, top or bottom? Bottom
   2. What are the differences and how did you know? The top has http the bottom https ,the top website is not the actual website of BOA, The bottom is a more professional interface of the webpage than the top.





##### Submission Instructions

1. Make sure you have entered your name and section number at the top of the document.
2. Save the document as **LastName\_Lab10.docx**, replacing LastName with YOUR last name.
3. Submit the assignment to the Lab 10 dropbox in Canvas by the due date.