EC-Council | Academia

C | SCU
Certified Secure Computer User

Course Syllabus

CERTIFIED SECURE COMPUTER USER

Instructor Contact Information

Instructor Name: **Office Location:**

Email: **Phone Contact:**

Office Hours:

The following text will be required for this course:

1. Certified Secure Computer User (CSCU) Version 2

- Information Security Principles and Practices
- The Antivirus Hacker's Handbook
- Computer Viruses for Dummies
- CISSP: Certified Information Systems Security Professionals Study Guide
- Handbook of Cloud Computing
- Cloud Computing: A Practical Approach
- Cloud Computing Bible
- Securing Cloud Services
- Networking Bible

I. Purpose of Class:

This course is aimed at end users in order to educate them about the main threats to their data's security. It also equips the students with the basic knowledge that helps them to keep their devices and data secure in daily life. It teaches basic techniques of being secure both online and offline.

II. Course Objectives:

After successfully completing this course, students will be able to:

1. Understand the need and importance of data security.
2. Implement Operating System security measures on their computers.
3. Understand Malware and its symptoms.
4. Make an informed decision about choosing the antivirus which is most relevant to their needs.
5. Understand the risks associated with different online activities.
6. Understand why and how to secure web browsers.
7. Identify safe websites.
8. Safeguard against the threats associated with online social networking.
9. Understand how to make their social networking accounts secure.
10. Understand the threats associated with email communications and how to safeguard against them.
11. Understand the threats to mobile devices and how to safeguard against them.
12. Understand the threats associated with cloud accounts and how to safeguard against them.
13. Make an informed decision about a cloud service provider which fulfills their requirements.
14. Understand the various types of networks and the threats associated with them.
15. Configure a home network.
16. Make their networks secure.
17. Understand the threats to data and the need for data backups.
18. Backup and restore data on their computers.
19. Destroy data permanently.

III. SCHEDULED OUTLINE OF COURSE TOPICS

WEEK ONE:

MODULES COVERED:

- Module 01 - Introduction to Data Security

WEEK'S OBJECTIVES USED:

1. Understand the need and importance of data security.

WEEK 1 ASSESSMENTS:

These are found in the course under Week One.

- Quizzes: 2 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 3 questions from readings (1 pt. each)

QUIZZES:

1. What is Authenticity?

    a. It refers to it being known or accessible to only authorized users.

    b. It ensures that the information is accurate, complete, reliable, and is in its original form.

    c. **It refers to truthfulness of origin of data.**

    d. It ensures that once the user captures data in a computer system, it must make the data available to users when they request it.

2. The process of involving actions, which support the precautionary measures and help in securing the devices is called.

    a. **Maintenance.**
    b. Reaction
    c. Precaution
    d. Nonrepudiation

DISCUSSION THREAD:

1. Harold was using an ATM, as he needed to withdraw some money to pay for his classes. When is swiped the card at the machine, and processes to enter the pin, Harold has noticed that another man behind him was trying to peek over his shoulder while he was entering his PIN. What should Harold do in this situation?
2. In case of a suspected data breach, what course of action should a person take?
3. When you buy a new laptop or a tablet, what are the different security measures you can take to keep the data on the device secure?

CASE STUDY:

News: Fraudsters' access to Barclays data revealed

Source: http://www.dailymail.co.uk/wires/pa/article-3174144/Fraudsters-access-Barclays-data-revealed.html

Fraudsters had access to the personal details of 30,000 Barclays customers for up to seven years, it has been revealed.

Private information on jobs, salaries and debts was found on a memory stick by chance in a police raid, and it is feared that multiple copies of the data may have been made.

The Daily Mail reports that the treasure trove of information also included names, dates of birth and addresses, and that victims have been offered £250 in compensation for the breach.

A Barclays spokesman said: "This is not a new theft of data from Barclays. Every indication is that the data here was part of the same theft of data that was reported last year, relating to data stolen in 2008. It is simply a separate USB data stick that was not received at that point in time and was recently discovered by the police.

"As with the theft last year, the details on the recently discovered USB data stick belong to a group of customers linked to the Barclays Financial Planning business which ceased operating in 2011. The data concerned was from 2008 or earlier."

He added: "We have proactively contacted the affected customers to apologies, as well as to offer them enhanced fraud protection and monitoring.

"We have also proactively offered customers compensation for the inconvenience this will have no doubt caused them.

"We are asking each customer to call if they feel their individual circumstances warrant different compensation, especially if they believe that they had a fraudulent event at any point since this data was stolen.

"We have also proactively reviewed all data that we hold to see if we can see any sign of suspicious activity and will continue to do that.

"Protecting our customers' data is our highest priority, and we take this issue extremely seriously."

Questions:

1. Discuss about the series of data thefts that were happening in banks.
2. Explain proper measures to be taken to avoid such incidents in future.

READINGS:

- Read the following chapter from the Certified Secure Computer User v2 book,
    - Module 1 – Introduction to Data Security

ASSIGNMENTS FROM READINGS:

1. Understand the different kinds of threats to the data.
2. Explain about the elements of security.
3. What are the security implementation practices?

ADDITIONAL RESOURCES:

White papers:

1. Top 10 Threats to SME Data Security

   https://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp.pdf

2. Data Leakage Worldwide White Paper: The High Cost of Insider Threats,

   http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html

3. The threats posed by portable storage devices,

   http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf

4. Security Threats, https://msdn.microsoft.com/en-us/library/cc723507.aspx

5. Data Leakage Worldwide: Common Risks and Mistakes Employees Make, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Videos:

1. Data Security Essentials, https://youtu.be/9WckTTqpD_M

WEEK TWO:

MODULES COVERED:

- Module 02 – Securing Operating Systems

WEEK'S OBJECTIVES USED:

2. Implement Operating System security measures on their computers.

WEEK 2 ASSESSMENTS:

These are found in the course under Week Two.

- Quizzes: 2 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 3 questions from readings (1 pt. each)

QUIZZES:

1. Which of the following is not the function of OS?

    a. **It deletes unnecessary files from the hard disks**
    b. It accepts inputs form the keyboard
    c. It controls peripheral devices
    d. It displays the end results on the screen

2. The system locking functionality facilitates which of the following?

    a. It prevents virus affected files
    b. It provides security from external attacks
    c. **It preventing unauthorized access and protecting the data**
    d. It grants access permission to the acquaintances of the owner of the system

DISCUSSION THREAD:

1. Ross, an 18-year-old boy, is going to an adventure camp with his friends. In the meantime, his cousins will be staying at his house. Since Ross's cousins are very mischievous, he does not want them using his new Windows laptop. What steps can Ross take to prevent his cousins from accessing his laptop?
2. Katie shares her laptop with her brother Ian. Katie has some personal photos in her folder, which she does not want Ian to see. In what ways could Katie prevent Ian from accessing her folder?
3. Gareth's parents found him watching porn online on the new Mac they gave him on his birthday. They obviously do not want Gareth to repeat this behavior. What action can Gareth's parents take to ensure this?

CASE STUDY:

News: Microsoft Issues Windows 10 Preview Build, Patches Critical Flaws

Source: http://www.toptechnews.com/article/index.php?story_id=12000007BKPC

With less than a month to go until the release of the Windows 10 Anniversary Update, Microsoft this week put out a new build that fixes a number of bugs in Windows, Office, Edge and other applications. In addition, Microsoft's Patch Tuesday release featured 11 updates for vulnerabilities, including six rated as "critical."

One of those vulnerabilities opens up Microsoft Windows -- Vista and later versions -- to possible man-in-the-middle attacks via printers or workstations. The problem can effectively turn printers into drive-by exploit kits that could let hackers access laptops or desktops connected to the affected printers.

Meanwhile, the Windows 10 Insider Preview Build 14388 released Tuesday includes 44 fixes to address everything from inconsistent keyboard displays in the mobile version of the Microsoft Edge browser to reliability and battery life issues. The build arrives just three weeks ahead of the scheduled August 2 release date for the Windows 10 Anniversary Update.

'Almost Too Good To Be True' for Hackers

Described as a "watering hole" attack, the 20-year-old printer vulnerability was identified and analyzed by security researcher Nick Beauchesne. Noting that Microsoft worked with the cybersecurity firm Vectra Networks to investigate the vulnerability, Beauchesne posted an analysis of his findings on Vectra's Web site Tuesday.

"This attack results in having 'system' rights on any workstation that connect[s] to your printer," Beauchesne wrote. "We are effectively transforming a printer in[to] an internal drive-by exploit kit, where we can just wait for people to come get infected without any warning."

Beauchesne said the vulnerability opened up a number of ways for attackers to use printers for remote code execution on laptops or PCs. The problem stemmed from an exception that Microsoft created to avoid account controls and make it easier for users to install printer drivers.

"So in the end, we have a mechanism that allows downloading executables from a shared drive, and run them as system on a workstation without generating any warning on the user side," Beauchesne said. "From an attacker perspective, this is almost too good to be true, and of course we had to give it a try."

Anniversary Update 'Getting Down to the Wire'

Among the other critical vulnerabilities Microsoft patched this week were bugs that could allow remote code execution via the Internet Explorer and Microsoft Edge browsers, along with similar flaws involving Microsoft Office, Adobe Flash Player and the Windows JScript and VBScript scripting engines.

"In addition to the critical updates, there are two important updates this month that warrant special mention," Chris Goettl, product manager for the Microsoft-focused security firm Shavlik, wrote in a blog post this week. Those two bugs "both include Public Disclosures, meaning they have a vulnerability included that has already leaked enough information to the public to allow an attacker to gain a head start on developing an exploit. As a result, this puts these vulnerabilities at higher risk of being exploited."

The scheduled August 2 Anniversary Update will be Microsoft's first significant update to Windows 10 since the operating system was released late last July. To date, the operating system has been downloaded onto more than 300 million devices worldwide, according to Microsoft.

Questions:

1. Discuss about the 'Water hole' attack in detail.
2. Explain about the remote code execution.

READINGS:

- Read the following chapter from the Certified Secure Computer User v2 book,
    - Module 2 – Securing Operating Systems

ASSIGNMENTS FROM READINGS:

1. Explain the concept of operating system and its functionalities.
2. Discuss the guidelines for securing the Windows 10 OS.
3. Discuss the guidelines for securing the MAC OS X.

ADDITIONAL RESOURCES:

White papers:

1. Windows 10 security overview, https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-10-security-guide
2. Microsoft Windows® 10 Security and Privacy, http://www.welivesecurity.com/wp-content/uploads/2016/06/windows-10-security-privacy.pdf
3. Windows 10 hardening and enterprise security, http://www.computerworld.com/article/2968394/microsoft-windows/windows-10-hardening-and-enterprise-security.html

Videos:

1. Windows 10 Security Issues, https://youtu.be/9rFXFH4oMKI
2. MAC OS X Security Features Part I, https://youtu.be/VApM1Wovxn8
3. MAC OS X Security Features Part II, https://youtu.be/Iw8BpxPgEyg

WEEK THREE:

MODULES COVERED:

- Module 03 – Malware and Antiviruses

WEEK'S OBJECTIVES USED:

3. Understand Malware and its symptoms.
4. Make an informed decision about choosing the antivirus which is most relevant to their needs.

WEEK 3 ASSESSMENTS:

These are found in the course under Week Three.

- Quizzes: 3 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 4 questions from readings (1 pt. each)

QUIZZES:

1. A kind of malware which finds its way into a system and encrypts all the files on it and holds the password which can decrypt those files is called?

    a. Virus
    b. Trojan
    c. Ransomware
    d. Spyware

2. What is a Rootkit?

    a. A malware which finds its way into a system and encrypts all the files on it and holds the password which can decrypt those files
    b. Once attackers have access to these systems, they steal important data (login details, financial information, passwords, electronic money, photos, and videos), inject more malware, monitor user activity, or even modify files
    c. It harms the computer by consuming excessive bandwidth, deleting files, or by sending documents through email
    d. Once it is installed, malicious parties remotely access the files, modify security settings, steal crucial information, or control the computer and use it to attack other computers

3. Which of the following is not the limitation of an Antivirus?

    a. Detected virus cannot be removed
    b. Limited detection technique
    c. Doesn't fully protected
    d. Slow down the system or network

DISCUSSION THREAD:

1. If a person suspects his or her computer is infected with malware, which indicators can confirm that this is the case?
2. Emma won a laptop at her college science fair. The laptop does not have antivirus software installed on it; hence Emma has to purchase one. What factors should Emma keep in mind before purchasing the software?
3. Gloria suspects that her laptop is infected with malware. Upon scanning the system using antivirus software, no malware is detected. Despite this, her laptop continues to display symptoms of malware infection. What may be the reason for this?

CASE STUDY:

News: UNIVERSITY OF CALGARY PAYS $20K FOLLOWING RANSOMWARE ATTACK,

Source: https://threatpost.com/university-of-calgary-pays-20k-following-ransomware-attack/118562/

Officials at the University of Calgary admitted this week that the school recently paid $20,000 CDN to rid its systems of ransomware that hampered productivity for 10 days. Linda Dalgetty, the school's VP of Finance and Services, acknowledged via press release on Wednesday that the school paid the ransom, which translates to roughly $15,756 USD, to maintain "all options to address system issues." According to the Canadian Broadcasting Corporation, at a press conference on Tuesday she told a crowd the school paid the ransom "because we do world-class research here … and we did not want to be in a position that we had exhausted the option to get people's potential life work back in the future if they came today and said, 'I'm encrypted, I can't get my files.' We did that solely so we could protect the quality and the nature of the information we generate at the university." Dalgetty said that while it did pay the attackers, the school is still in the process of assessing and evaluating decryption keys. "The actual process of decryption is time-consuming and must be performed with care," Dalgetty wrote, "It is important to note that decryption keys do not automatically restore all systems or guarantee the recovery of all data." It's unclear exactly what type of ransomware hit the school – it only claimed it was "software intended to damage or disable computers and computer systems." Regardless, it managed to take some parts of the school's network offline for 10 straight days. According to Dalgetty, it wasn't until this past Monday that the University of Calgary's IT department was first able to "isolate the effects of the attack" and secure access for students and faculty to the university's email service. There was a point last week where students and staff were encouraged to call or text recipients as only a select number of individuals had access to email. The school, which counts approximately 20,000 undergraduate students and 5,000 graduate students, said it's working alongside law enforcement to investigate the attack, as is the protocol in cases like this. Dalgetty said that since it's an ongoing investigation, the school can't divulge how it plans to address the attack, nor "how or if decryption keys will be used." "A great deal of work is still required by IT to ensure all affected systems are operational again, and this process will take time," Dalgetty wrote. The school began experiencing what it called system issues on May 28 and warned students not to use any U. Calgary-issued computers and not to connect classroom computers to the U. Calgary network. The school admitted the next day that malware was the cause of the issue and again stressed not to use any university-issued machines. According to the CBC, there had previously been a minor data breach at the school but this attack was different because it encrypted the university's email server. Paying the ransom that attackers demand in situations like this is largely discouraged by experts, because it's not guaranteed victims will receive all of their personal information back, nor is it certain victims won't be attacked again. The news comes a few weeks after the FBI issued a warning to businesses, urging them not to pay attackers. Instead companies and organizations alike should back up their data and ensure browsers, operating systems, and third party apps are kept up to date, the agency stressed. "Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity," FBI Cyber Division Assistant Director James Trainor said at the time, "And finally, by paying a ransom, an

organization might inadvertently be funding other illicit activity associated with criminals." Ransomware has been a scourge for companies, but especially hospitals, so far this year. Methodist Hospital, a care facility in Henderson, Ky. was knocked offline for four days in March while Hollywood Presbyterian Medical Center, a hospital in Hollywood, Calif. was crippled in February after attackers demanded a staggering $3M to unlock their records.

Questions:

1. Discuss about the Ransomware decryption process and its fruitful results.
2. Explain about the reasons for Ransomware became a scourge for the companies.

READINGS:

Information Security Principles and Practices

- Read the following chapter from Information Security Principles and Practices, http://file.allitebooks.com/20160522/Information%20Security,%202nd%20Edition.pdf
  - Chapter 11 – Software Flaws and Malware (Section 11.3 – Malware)

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 3 – Malware and Antiviruses

The Antivirus Hacker's Handbook

- Read the following chapter from The Antivirus Hacker's Handbook, http://file.allitebooks.com/20150910/The%20Antivirus%20Hacker-s%20Handbook.pdf
  - Chapter 1 – Introduction to Antivirus Software

Computer Viruses for Dummies

- Read the following chapters from Computer Viruses for Dummies, http://file.allitebooks.com/20150521/Computer%20Viruses%20For%20Dummies.pdf
  - Chapter 1 – Understanding Virus Risks
  - Chapter 2 – Does My Computer Have a Virus?
  - Chapter 3 – Does Your Computer Have Antivirus Software?
  - Chapter 4 – Obtaining and Installing Antivirus Software

ASSIGNMENTS FROM READINGS:

1. Explain about various types of malware.
2. Discuss about the antivirus, its misconceptions, and features.
3. Understand the common symptoms of a virus affected machine.
4. Understand how to find and fix the viruses.

ADDITIONAL RESOURCES:

White papers:

1. The Ongoing Malware Threat: How Malware Infects Websites and Harms Businesses — and What You Can Do to Stop It, https://www.geotrust.com/anti-malware-scan/malware-threat-white-paper.pdf
2. Ransomware Whitepaper, https://www.cert.be/files/ransomware_whitepaper.pdf
3. Five Steps to Advanced Malware Protection: A Cisco Reality, http://www.cisco.com/c/en/us/products/collateral/security/whitepaper_c11-733367.pdf

Videos:

1. Introduction to Malware, https://www.youtube.com/watch?v=1Vz4f4nGIHM
2. Introduction to Malware. https://www.youtube.com/watch?v=74Pgy9-yM-4

WEEK FOUR:

MODULES COVERED:

- Module 04 - Internet Security

WEEK'S OBJECTIVES USED:

5. Understand the risks associated with different online activities.
6. Understand why and how to secure web browsers.
7. Identify safe websites.

WEEK 4 ASSESSMENTS:

These are found in the course under Week Four.

- Quizzes: 3 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 3 questions from readings (1 pt. each)

QUIZZES:

1. _____ is a popular software used to encrypt and decrypt emails sent over the Internet.

    a. Web Browser
    b. **Pretty Good Practice**
    c. Web of Trust
    d. Firefox

2. What is Cyberbullying?

    a. **Sending messages of an intimidating or threatening nature through electronic communication**
    b. These are websites that use misleading URLs to increase their site traffic
    c. An act of befriending and establishing an emotional connection with children, so as to prepare them for child abuse
    d. Sending spam messages

3. What is Impersonation?

    a. **It is the process of ensuring user identity to access protected resources**
    b. It checks the access rights of the user account in which ASP.NET is running for NTFS file permissions
    c. It allows or denies access to user for a particular directory by using username or role
    d. This approach uses permission demands to authorize users

DISCUSSION THREAD:

1. Karen noticed that her son was not himself lately. He did not want to go to school or play with his friends and had a morose look on his face perpetually. When Karen questioned him about this, he broke down and told her that some kids from his class made a Facebook page just to ridicule his appearance and make fun of him publicly. What can Karen do to prevent further cyberbullying of her son?
2. What browser security features can one turn on to keep their computers safe while browsing the Internet?
3. Joan recently introduced her 10-years old daughter Georgia to the Internet to help her in her studies. Joan is a very cautious person and she does not want Georgia exposed to online threats. What steps can Joan take to prevent this?

CASE STUDY:

News: Kelly Brook named UK's 'most dangerous cyber celebrity' of 2015

Source: http://www.telegraph.co.uk/technology/internet-security/11898905/Kelly-Brook-named-UKs-most-dangerous-cyber-celebrity-of-2015.html

Model and TV personality Kelly Brook is the most dangerous celebrity to search for online in the UK, exposing internet users to more possible viruses and malware than anyone else, it has emerged.

Ms Brook was named the UK's most dangerous cyber-celebrity of 2015 in Intel Security's annual study, overtaking Cheryl Fernandez-Versini, who dropped 18 places from the top spot last year.

This is Ms Brook's first time in Intel Security's list of the most dangerous celebrities and, by topping the poll, she beats the likes of Katie Price, X Factor judges Nick Grimshaw and Rita Ora, and Victoria Beckham.

The terms "Kelly Brook", "Kelly Brook HD downloads", "Kelly Brook free MP4", and "Kelly Brook torrent" were used to search for Kelly Brook, and similar terms were used for each celebrity on the list.

The study was conducted using McAfee SiteAdvisor site ratings, which determines the number of risky sites generated by each search term and calculates an overall risk percentage for that celebrity.

Intel Security said that cybercriminals are always looking for ways to take advantage of consumer interest around popular culture events including talent shows, movies premieres, album releases and celebrity breakups.

They capitalise on this interest by enticing unsuspecting consumers to sites that download harmful malware onto devices and steal their private data.

The desire for consumers to have access to the latest celebrity gossip can often make them vulnerable to cybercrime," said Nick Viney, VP consumer, mobile and small business, Intel Security.

"Most consumers are unaware of the potential risks they are exposing themselves to by clicking on sites that provide them with the latest news and entertainment. But cybercriminals are quick to exploit this desire for breaking celebrity news."

Intel Security added celebrity names combined with the terms "free MP4", '"HD downloads", or "torrent" are some of the most searched terms on the Internet.

The company warned that people looking to download free music and films that are not made available through legitimate channels may be especially at risk from cybercriminals.

Questions:

1. Explain the need to avoid clicking suspected links in the websites.
2. Analyze the increasing number of incidents happening in the internet, which uses the celebrities fame to spread viruses and attacks.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 4 – Internet Security

ASSIGNMENTS FROM READINGS:

1. Discuss about the concepts Internet, Web browser, and Internet Security.
2. Explain the steps involved in securing the Windows Edge, Mozilla Firefox, Safari, Google Chrome, and Internet Explorer.
3. What is instant messaging and its mitigation security issues?

ADDITIONAL RESOURCES:

White papers:

1. Microsoft Edge has inherited many of Internet Explorer's security holes, http://www.infoworld.com/article/3012987/microsoft-windows/microsoft-edge-has-inherited-many-of-internet-explorers-security-holes.html
2. Google wants to turn browser signals of Web encryption upside down, http://www.computerworld.com/article/2861583/google-wants-to-turn-browser-signals-of-web-encryption-upside-down.html
3. The best 8 secure browsers 2016, http://www.techworld.com/security/best-8-secure-browsers-2016-3246550/
4. HTML5 Security The Modern Web Browser Perspective whitepaper, https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2012/december/html5-security-the-modern-web-browser-perspective-whitepaper/

Videos:

1. Browser Security essentials - Safe Browsing with Kaspersky Extension, https://www.youtube.com/watch?v=kuIuTAbRKIU

WEEK FIVE:

MODULES COVERED:

- Module 05 - Security On Social Networking Sites

WEEK'S OBJECTIVES USED:

8. Safeguard against the threats associated with online social networking.
9. Understand how to make their social networking accounts secure.

WEEK 4 ASSESSMENTS:

These are found in the course under Week Four.

- Quizzes: 2 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 3 questions (5 pts. each)
- Questions from Readings: 2 questions from readings (1 pt. each)

QUIZZES:

1. Which of the following is not a risk associated with social networking sites?

    a. Phishing
    b. Identity Theft
    c. Clickjacking
    d. MAC Spoofing

2. What is Geotagging?

    a. It the process of adding geographical information, in the form of latitudes and longitudes, to various forms of media
    b. It is the process of tagging in the social media
    c. The process of creating a fake URL mimicking a legitimate one.
    d. The process of creating a malicious cover over a genuine link that is transparent to the use

DISCUSSION THREAD:

1. Monica, a 21-year-old woman, regularly uploads selfies and statuses on Facebook. Gina, who considers Monica to be her social rival, regularly posts sarcastic and rude comments on Monica's updates. In addition, some strangers have been posting vulgar comments on her photos as well. What steps can Monica take to prevent Gina and these strangers from viewing her Facebook activity?
2. What risks do people face on social networking sites if they are not careful about their online activities?
3. When communicating with an unknown person online, what are the warning signs that tell you that you might be a victim of a social media scam?

CASE STUDY:

News: Facebook 'fake friend' phishing attack uncovered - here's how to spot it

Source: http://www.telegraph.co.uk/technology/2016/07/06/facebook-fake-friend-phishing-attack-uncovered---heres-how-to-sp/

A 'global' Facebook phishing scam has been uncovered, with the cyber-attack spreading rapidly and initially claiming a new victim every 20 seconds, according to internet security experts.

Facebook users have been receiving rogue messages from 'friends' who appear to have mentioned them in posts on the social network.

Compromised devices were then used to hijack Facebook accounts and spread the infection through the victim's own Facebook friends, Kaspersky Lab security experts say.

"Between the 24th and 27th June, thousands of unsuspecting consumers received a message from a Facebook friend saying they'd mentioned them in a comment," explains the cybersecurity company.

"The message had in fact been initiated by attackers and unleashed a two-stage attack. The first stage downloaded a Trojan onto the user's computer that installed, among other things, a malicious Chrome browser extension.

"This enabled the second stage, the takeover of the victim's Facebook account when they logged back into Facebook through the compromised browser."

The attack gave hackers the ability to change privacy settings, steal data and spread the infection through the victim's Facebook friends, Kaspersky Lab say.

An estimated 10,000 Facebook accounts have been infected in South America, Europe, Tunisia and Israel, with the majority of incidents occurring in Brazil. It is not thought to have reached the UK.

"Two aspects of this attack stand out," said Ido Naor, Kaspersky Lab's Senior Security Researcher. "Firstly, the delivery of the malware was extremely efficient, reaching thousands of users in only 48 hours.

"Secondly, the response from consumers and the media was almost as fast. Their reaction raised awareness of the campaign and drove prompt action and investigation by the providers concerned."

Social media users who believe their computer has been infected by the virus have been advised to run a malware scan or to log out of Facebook, close the browser and to disconnect the network cable from their computer.

Facebook say it has now mitigated the threat and is blocking techniques used to spread malware from infected computers, according to Kaspersky Lab.

Questions:

1. Explain about the phishing scams in the social media.
2. Discuss about the process used by the attackers in compromising the browser and sending fake messages.
3. Understand the safety measures and avoid responding to such fake messages.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 5 – Security On Social Networking Sites

ASSIGNMENTS FROM READINGS:

1. Explain the concept social networking and the risks associated with them.
2. Understand the concept Geotagging.

ADDITIONAL RESOURCES:

White papers:

1. The Risks of Social Networking, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf
2. Security Guide to Social Networks, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_security_guide_to_social_networks.pdf
3. Social Networking and Security Risks, http://www.fieldbrook.net/TechTips/Security/SocialNetworkingSecurity.pdf

Videos:

1. Privacy and Security Issues in Social Networking, https://www.youtube.com/watch?v=XzyiMAFcQOw

WEEK SIX:

MODULES COVERED:

- Module 06 - Securing Email Communications

WEEK'S OBJECTIVES USED:

10. Understand the threats associated with email communications and how to safeguard against them.

WEEK 5 ASSESSMENTS:

These are found in the course under Week Five.

- Quizzes: 3 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Questions from Readings: 3 questions from readings (1 pt. each)

QUIZZES:

1. What is an Email?

    a. A method to send letters from one place to another
    b. Communication protocol
    c. It is a method used to communicate electronically by sending messages from one computer to another via internet
    d. Email is an instant messenger

2. Which of the following does not contain in an Email?

    a. Margin
    b. Header
    c. Body
    d. Signature

3. The process of converting information into unreadable coded form to prevent unauthorized access is called.

    a. Decryption
    b. Encryption
    c. Message Hiding
    d. Digital Signature

DISCUSSION THREAD:

1. Richard received an email from a person claiming to be his childhood friend, Kate. The email ID is unknown to Richard but the mail says that it is Kate's new mail ID. It also has an attachment, which according to the mail, is a childhood picture of them. What steps should Richard take to verify the authenticity of Kate's new email ID? In addition, how should Richard make sure that the attachment is not malicious?
2. Kyle has recently started a firm that handles food delivery operations. He wants to create an email ID for the new business. Hence, what factors should Kyle keep in mind while choosing an email service provider?
3. After a spate of email related threats and breaches at his firm, Ryan has decided to improve the security measures to secure his company network. What email security measures can Ryan implement?

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
    - Module 6 – Securing Email Communications

CISSP: Certified Information Systems Security Professionals Study Guide

- Read the following chapter from CISSP: Certified Information Systems Security Professionals Study Guide, http://ebooks.cawok.pro/Sybex.CISSP.Certified.Information.Systems.Security.Professional.Study.Guide.2nd.Edition.Jul.2004.eBook-DDU.pdf
    - Chapter 4 – Communications Security and Countermeasures (Section: Managing Email Security)

ASSIGNMENTS FROM READINGS:

1. Understand the concepts of Email, its security and functioning.
2. Explain the encryption, types of encryption, and its limitations.
3. Discuss the goals and issues of Email security.

ADDITIONAL RESOURCES:

White papers:

1. Email security, http://www.computerweekly.com/feature/White-Paper-Email-security
2. Email Attacks: This Time It's Personal, http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf
3. ADAPTIVE, INTELLIGENT, SCALABLE DEFENSE AGAINST EMAIL-BORNE THREATS, https://www.fireeye.com/products/ex-email-security-products.html
4. EMAIL SECURITY: DEFENDING THE ENTERPRISE, https://webobjects.cdw.com/webobjects/media/pdf/Solutions/Security/144921-Email-Security-Defending-the-Enterprise.pdf

Videos:

1. Email Security: When Good News Goes Bad, https://youtu.be/tkgLHoaFeFk
2. How your email server works, https://youtu.be/1X3dX2JEhLE
3. How Email is Sent and Received on The Internet, https://youtu.be/g6NMFHuef6Y
4. Cisco Email Security Protects Against Emerging Sophisticated Threats, https://youtu.be/RczyV-A0JCA

WEEK SEVEN:

MODULES COVERED:

- Module 07 - Securing Mobile Devices

WEEK'S OBJECTIVES USED:

12. Understand the threats to mobile devices and how to safeguard against them.

WEEK 5 ASSESSMENTS:

These are found in the course under Week Five.

- Quizzes: 2 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 4 questions from readings (1 pt. each)

QUIZZES:

1. What is IMEI number?

    a. **It is used to identify a device that uses cellular networks**
    b. It is used for mobile security
    c. It is used for encryption
    d. It is used for decryption

2. Expand IMEI.

    a. Internet Mobile Enhancement Identifier
    b. **International Mobile Equipment Identity**
    c. Interconnect Mobile Equipment Identity
    d. International Mobile Enhancement Identity

DISCUSSION THREAD:

1. Amy works as a marketing executive for QW Agency. While coming home from work, Amy misplaced her recently purchased iPhone. The loss of Amy's iPhone worried her as it contained the launch strategy of a new product, and Amy did not want it to fall into the wrong hands. How should Amy proceed in order to prevent the data from falling into the wrong hands as well as to recover her iPhone?
2. Billie works an executive reporter for News Today. The assignment on which she is currently working on will expose a major cover-up at the mayor's office. All the information Billie has gathered until now is stored on her phone. She is worried that someone may attempt to steal the phone in order to kill the story. What security measures can Billie take to secure her mobile device?
3. What are the risks a person should be aware of when using a smartphone?

CASE STUDY:

News: Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge

Source: http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-5-Key-Risks-and-a-Surprising-Challenge

Employees aren't just bringing their mobile devices to the workplace — they're *living* on them. A 2015 study by Bank of America found that 55 percent of respondents sleep with their smartphones on their nightstands to avoid missing a call, text message or other update during the night. The devices are also the first thing on their minds in the morning: while 10 percent reported thinking of their significant other, 35 percent reserved their first thought of the day for their smartphone.

As smartphones and tablets become constant companions, cyber attackers are using every avenue available to break into them. Many people expect that iPhone or Android devices are secure by default, when in reality it is up to the user to make security configuration changes. With the right (inexpensive) equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and either mirror the device and see everything on it, or install malware that will enable them to siphon data from it at their leisure.

The nature and types of cyber-attacks are evolving rapidly, and mobile devices have become a critical part of enterprise cyber-security efforts with good reason. Analysts predict that by 2018, 25 percent of corporate data will completely bypass perimeter security and flow directly from mobile devices to the cloud.

Chief information security officers (CISOs) and other security executives are finding that the proliferation of mobile devices and cloud services are there a significant barrier to effective breach response. In order to secure the corporate data passing through or residing on mobile devices, it is imperative to fully understand the issues they present.

5 Security Risks and a Surprising Challenge

The threat and attack vectors for mobile devices are largely composed of retargeted versions of attacks aimed at other endpoint devices. These risks can be categorized into five areas.

1. Physical access

Mobile devices are small, easily portable and extremely lightweight. While their diminutive size makes them ideal travel companions, it also makes them easy to steal or leave behind in airports, airplanes or taxicabs. As with more traditional devices, physical access to a mobile device equals "game over." The cleverest intrusion-detection system and best anti-virus software are useless against a malicious person with physical access. Circumventing a password or lock is a trivial task for a seasoned attacker, and even encrypted data can be accessed. This may include not only corporate data found in the device, but also passwords residing in places like the iPhone Keychain, which could grant access to corporate services such as email and virtual private network (VPN). To make matters worse, full removal of data is not possible using a device's built-in factory reset or by re-flashing the operating system. Forensic data retrieval software — which is available to the general public — allows data to be recovered from phones and other mobile devices even after it has been manually deleted or undergone a reset.

2. Malicious Code

Mobile malware threats are typically socially engineered and focus on tricking the user into accepting what the hacker is selling. The most prolific include spam, weaponized links on social networking sites and rogue applications. While mobile users are not yet subject to the same drive-by downloads that PC users face, mobile ads are increasingly being used as part of many attacks — a concept known as "malvertising." Android devices are the biggest targets, as they are widely used and easy to develop software for. Mobile malware Trojans designed to steal data can operate over either the mobile phone network or any connected Wi-Fi network. They are often sent via SMS (text message); once the user clicks on a link in the message, the Trojan is delivered by way of an application, where it is then free to spread to other devices. When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

3. Device Attacks

Attacks targeted at the device itself are similar to the PC attacks of the past. Browser-based attacks, buffer overflow exploitations and other attacks are possible. The short message service (SMS) and multimedia message service (MMS) offered on mobile devices afford additional avenues to hackers. Device attacks are typically designed to either gain control of the device and access data, or to attempt a distributed denial of service (DDoS).

4. Communication Interception

Wi-Fi-enabled smartphones are susceptible to the same attacks that affect other Wi-Fi-capable devices. The technology to hack into wireless networks is readily available, and much of it is accessible online, making Wi-Fi hacking and man-in-the-middle (MITM) attacks easy to perform. Cellular data transmission can also be intercepted and decrypted. Hackers can exploit

weaknesses in these Wi-Fi and cellular data protocols to eavesdrop on data transmission, or to hijack users' sessions for online services, including web-based email. For companies with workers who use free Wi-Fi hot spot services, the stakes are high. While losing a personal social networking login may be inconvenient, people logging on to enterprise systems may be giving hackers access to an entire corporate database.

5. Insider Threats

Mobile devices can also facilitate threats from employees and other insiders. Malicious insiders can use a smartphone to misuse or misappropriate data by downloading large amounts of corporate information to the device's secure digital (SD) flash memory card, or by using the device to transmit data via email services to external accounts, circumventing even robust monitoring technologies such as data loss prevention (DLP). The downloading of applications can also lead to unintentional threats. Most people download applications from app stores and use mobile applications that can access enterprise assets without any idea of who developed the application, how good it is, or whether there is a threat vector through the application right back to the corporate network. The misuse of personal cloud services through mobile applications is another issue; when used to convey enterprise data, these applications can lead to data leaks that the organization remains entirely unaware of.

Mobile security threats will continue to advance as corporate data is accessed by a seemingly endless pool of devices, and hackers try to cash in on the trend. Making sure users fully understand the implications of faulty mobile security practices and getting them to adhere to best practices can be difficult. Many device users remain unaware of threats, and the devices themselves tend to lack basic tools that are readily available for other platforms, such as anti-virus, anti-spam, and endpoint firewalls.

The Productivity Challenge: Blessing, or Curse?

Increasing worker productivity is the leading factor driving bring your own device (BYOD) program deployment.

It may therefore seem surprising that a 2015 CareerBuilder study of top ten productivity killers at work ranked cell phones as the number one thing causing people to waste time at the office.

Mobile devices enable workers to accomplish tasks wherever and whenever they choose, but they can be distracting. Flitting between numerous screens and apps and continuously checking email and Twitter feeds is enough to disrupt even the most focused employee.

"It is an epidemic," Lacy Roberson, Learning and Organization Development Director at eBay has said. At most companies, it's a struggle "to get work done on a daily basis, with all these things coming at you." In order to avoid the inevitable—people checking in on their devices and checking out of conversations — organizations like eBay have implemented a no-device policy for certain meetings. Even the White House is facing an inappropriate phone use problem. In an article entitled "How To Get People Off Their Phones In Meetings Without Being A Jerk", *Forbes* detailed the President's phone-drop protocol: before meeting with him, cabinet members attach yellow sticky notes with their names to their cell phones and leave them in a basket before entering the room.

While office distractions are nothing new, the lure of 24/7 social-networking streams and email alerts that accompany mobile devices is intensifying the problem.

Meeting the Mobility Challenge

Mobile device threats are increasing and can result in data loss, security breaches and regulatory compliance violations. You can take a number of steps to reduce the risks they pose and address related productivity issues and legal, privacy, and security requirements. These steps are similar to those involved with other security issues — such as robust program and policy creation, communication, risk assessment, technology implementation, and continuous monitoring and evaluation — but are tailored to the unique challenges associated with mobile devices. With well-supported mobility and security awareness programs in place, your organization can keep users happy and your network secure, so you can compete effectively in today's mobile-first environment.

Questions:

1. Explain why mobiles have become the major targets for the attackers.
2. Understand the 5 security risks that are facing by the mobile devices in recent times.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 7 – Securing Mobile Devices

ASSIGNMENTS FROM READINGS:

1. Understand mobile device threats.
2. Understand various mobile security procedures.
3. Explain how to secure iPhone and iPad devices.
4. Explain how to secure Android devices.

ADDITIONAL RESOURCES:

White papers:

1. Mobile Security and Management, http://www.symantec.com/content/en/us/enterprise/white_papers/b-mobile_security_and_management_WP_21155057.en-us.pdf
2. Need for a Secure Mobile Platform, http://www.infineon.com/dgdl/Infineon-Need+for+a+Secure+Mobile+Platform-WP-v01_15-EN.pdf?fileId=5546d4624b0b249c014b831934057800
3. Elevation of Mobile Security Risks in the Enterprise Threat Landscape, http://www.happiestminds.com/whitepapers/elevation_of_mobile_security_risks_in_enterprise_threat_landscape.pdf
4. Mobile Security: Threats and Countermeasures, http://www.mobileiron.com/sites/default/files/security/Mobile-Security-Threats-and-Countermeasures-WP-MKT-6361-V1.pdf

Videos:

1. Mobile Security - What you need to know, https://youtu.be/klJu-KR-jcs

WEEK EIGHT:

MODULES COVERED:

- Module 08 – Securing the Cloud

WEEK'S OBJECTIVES USED:

12. Understand the threats associated with cloud accounts and how to safeguard against them.
13. Make an informed decision about a cloud service provider which fulfills their requirements.

WEEK 6 ASSESSMENTS:

These are found in the course under Week Six.

- Quizzes: 3 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 3 questions (5 pts. each)
- Questions from Readings: 4 questions from readings (1 pt. each)

QUIZZES:

1. Which of the following does not come under cloud architecture?

    a. Private Cloud
    b. Public Cloud
    c. Static Cloud
    d. Hybrid Cloud

2. What is portability in cloud computing?

    a. Easy accessing of the resources from the cloud whenever and wherever
    b. Storing portable amount of data in the cloud
    c. Storing large volumes of data in the cloud
    d. Easy to store the data

3. What is data breach cloud computing?

    a. **Attacking the cloud to access unauthorized data**
    b. Safeguarding the cloud with additional security
    c. Encrypting the cloud data
    d. Decrypting the cloud data

DISCUSSION THREAD:

1. Harry, a wildlife photographer, is about to go to Africa for an assignment. In the past his equipment has suffered damage in the wild resulting in him losing all his pictures. Thus Harry has decided to subscribe to a cloud service this time so that he can back up his pictures regularly to keep them safe. What factors should Harry keep in mind before choosing a cloud service provider?
2. Jackie is writing a novel and she feels that her manuscript would be safer if it is stored on cloud and not on a local computer. After a bit of research she found out that even though cloud has its advantages, it faces several threats. What threats should Jackie be aware of before selecting a cloud service?
3. Max, a lawyer, has stored confidential data regarding his clients on a cloud service. Of late, there have been many reported cases of cloud accounts being hacked. Max wants to make sure that his data is not stolen. What precautionary measures can Max take to protect his data?

CASE STUDY:

News: Hackers see cloud as 'a fruit-bearing jackpot' for cyber attacks

Source: http://www.computing.co.uk/ctg/news/2429256/hackers-see-cloud-as-a-fruit-bearing-jackpot-for-cyber-attacks

Cyber-criminals and hackers are increasingly attacking cloud infrastructure, which they see as a "fruit-bearing jackpot" as more organizations are making use of public cloud to store their data than ever before, a security company claims.

While organizations are embracing the cloud - as confirmed by *Computing* research - a report by security-as-a-service provider Alert Logic suggests that IT decision-makers shouldn't assume that data they store off-premise is harder for hackers to acquire.

The company warns that there has been a 45 per cent increase in application attacks against cloud deployments.

Alert Logic bases its research on an analysis of one billion events in the IT environments of more than 3,000 of its customers between January 1 and December 31 2014, which revealed more than 800,000 security incidents.

One of the key findings was an increase in attack frequency on organizations that store their infrastructure in the cloud.

"This is not surprising," says the *Alert Logic Cloud Security* report. "Production workloads, applications, and valuable data are shifting to cloud environments, and so are attacks.

"Hackers, like everyone else, have a limited amount of time to complete their job," the report continues, adding: "They want to invest their time and resources into attacks that will bear the most fruit: businesses using cloud environments are largely considered that fruit-bearing jackpot."

The pattern of attacks directly follows the increase in the number of organizations using cloud hosting from providers such as Amazon, Google and Microsoft.

"Attackers are seeing this trend as well and are making concerted efforts to infiltrate businesses making use of cloud environments, just as they previously did with physical data centers."

The report claims that some businesses have a misconception about what security precautions they need to take when using cloud-based storage, services, and other software deployments.

Alert Logic suggests that many "mistakenly assume cloud providers take care of all their security needs" when in reality "security in the cloud is a shared responsibility".

Cyber-criminals are now more sophisticated, with attackers using "advanced techniques" in order to infiltrate the networks of their target organization.

"Unlike in the past when hackers primarily worked alone using 'smash-n-grab' techniques, today's attackers work in groups, each member bringing his or her own expertise to the team," says the report, which argues that these techniques also allow cyber-criminals to avoid capture.

"With highly skilled players in place, these groups approach infiltration in a much more regimented way, following a defined process that enables them to evade detection and achieve their ultimate goal: turning sensitive, valuable data into profits."

However, while there has been a rise in cyber-attacks that target the cloud, Will Semple, vice president of security services for Alert Logic, warns organizations that on premise networks are still a significant target for cyber-criminals.

"While cyber-criminals are increasingly targeting cloud deployments, on-premises deployments are still being targeted at the same frequency as they always were," he says.

"The key to protecting your critical data is being knowledgeable about how and where along the 'cyber kill chain' attackers infiltrate systems and to employ the right security tools, practices and resource investment to combat them," Semple adds.

Questions:

1. Analyze why the cloud has become a "fruit-bearing jackpot" for hackers.
2. Discuss why people are thinking that the cloud providers will take care of their resources in the cloud?
3. Discuss how the hackers are participating in a hacking attempt to infiltrate the cloud.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 8 – Securing the Cloud

Handbook of Cloud Computing

- Read the following chapter from Handbook of Cloud Computing, https://studytm.files.wordpress.com/2014/03/hand-book-of-cloud-computing.pdf
  - Chapter 1 – Cloud Computing Fundamentals

Cloud Computing: A Practical Approach

- Read the following chapter from Cloud Computing: A Practical Approach, http://file.allitebooks.com/20160407/Cloud%20Computing.pdf
  - Chapter 1 – Cloud Computing Basics
  - Chapter 2 – Your Organization and Cloud Computing

Cloud Computing Bible

- Read the following chapter from Cloud Computing Bible, http://file.allitebooks.com/20150527/Cloud%20Computing%20Bible.pdf
  - Chapter 1 – Defining Cloud Computing
  - Chapter 3 – Understanding Cloud Architecture
  - Chapter 12 – Understanding Cloud Security

Securing Cloud Services

- Read the following chapter from Securing Cloud Services, http://file.allitebooks.com/20151105/Securing%20Cloud%20Services.pdf
  - Chapter 1 – Introduction to Cloud Computing
  - Chapter 3 – The Security Balance
  - Chapter 4 – Security Threats Associated with Cloud Computing

ASSIGNMENTS FROM READINGS:

1. Understand the concept of cloud, types of cloud, and its working functionality.
2. Explain the various threats to the cloud security and its privacy issues.
3. Explain the terms cloud computing and cloud services.
4. Discuss about the cloud components and applications.

ADDITIONAL RESOURCES:

Whitepapers:

1. White Paper Cloud Computing, http://www.t-systemsus.com/umn/uti/508260_1/blobBinary/White+Paper+Cloud+Computing+%257B%257BPDF%252C+351+KB%257D%257D.pdf
2. Securing the Cloud for the Enterprise, http://eval.symantec.com/mktginfo/downloads/21187913_GA_WP_SecuringtheCloudfortheEnterprise_05%2011.pdf
3. The dirty dozen: 12 cloud security threats, http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

Videos:

1. Cloud Computing for beginners - What is cloud?, https://youtu.be/G2HkIar0G7k
2. How Cloud Computing Works, https://youtu.be/DGDtujmOBKc
3. Addressing the Top Five Cloud Security Challenges, https://youtu.be/YqDU1Twzfi8

WEEK NINE:

MODULES COVERED:

- Module 09 – Securing Network Connections

WEEK'S OBJECTIVES USED:

14. Understand the various types of networks and the threats associated with them.
15. Configure a home network.
16. Make their networks secure.

WEEK 7 ASSESSMENTS:

These are found in the course under Week Seven.

- Quizzes: 3 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 discussion threads (5 pts. each)
- Case Studies: 1 case study with 2 questions (5 pts. each)
- Questions from Readings: 3 questions from readings (1 pt. each)

QUIZZES:

1. A network that exist over a large-scale geographical area is called.

    a. LAN
    b. **WAN**
    c. MAN
    d. CAN

2. What is Virtual Private Network?

    a. A private network created between two or more computers
    b. A company network
    c. A connection between two systems
    d. A private network

3. Arrange the following steps in an order for setting up a home network.

   I. Select the type of network
   II. Setup a router
   III. Obtain necessary hardware
   IV. Configure the network
   V. Connect the devices and system to the network
   VI. Create a home group

   a. I, II, III, IV, V, VI
   b. II, I, IV, III, V, VI
   c. I, III, II, IV, V, VI
   d. VI, V, I, II, III, IV

DISCUSSION THREAD:

1. Phil noticed that his Wi-Fi data plan is getting exhausted earlier than usual for the past couple of months. He suspects that someone else may be tagging on to his Wi-Fi signal and using up the data. What can Phil do to secure his connection?
2. Recently, Claire's laptop was infected with malware and she took it to the service center to be formatted. What steps can Claire take to prevent the same thing from happening again?
3. What steps can a person take while setting up a home network?

CASE STUDY:

News: Public Wi-Fi use raises hacking risk

Source: http://abcnews.go.com/Business/story?id=3454066&page=1

Laptop road warriors beware: Wi-Fi hot spots that let you hop onto the Internet anywhere you travel leave you wide open to hackers.

The basic problem: T-Mobile and AT&T t— the largest providers of Wi-Fi hot spots in coffee shops, bookstores and airports — don't require encryption of data traveling wirelessly between laptops and the Internet. Neither do hotels and municipalities with free Wi-Fi hookups in public areas. T-Mobile and AT&T do recommend customers download and use their free encryption software.

"If you're using Wi-Fi in a public place and you're not getting hacked, it's only because there's nobody around bothering to do it," says Robert Graham, CEO of consultancy Errata Security.

Wi-Fi eavesdropping has long been a security concern. Anyone with a Wi-Fi-equipped laptop can download free Wi-Fi monitoring programs. An eavesdropper can sit up to 100 feet away and monitor what you do on the Net, says Rick Farina, security engineer for wireless security firm AirTight Networks.

There are no estimates of how often this happens. No one has ever been arrested for Wi-Fi hacking. But with Wi-Fi now in mainstream use — T-Mobile and AT&T supply hot spots at more than 15,000 locations in the USA, and cities such as New York and San Francisco supply free public access points — intruders are starting to take advantage, said security experts at recent Black Hat and DefCon security conferences.

Wi-Fi hot-spot hacks "are absolutely taking place," says Tom Brennan, technology risk manager for security consultant Access IT Group. "It's easy to do, and the reward is very high."

Brennan cites an example of a tech systems manager on a lunch break in New York's Bryant Park, who used his laptop via the city's free hot-spot hookup. The manager logged onto his company's network to troubleshoot a computer server. An eavesdropper nabbed his username and password. Later, someone used the information to access the server. "People are on the road using wireless, they get breached, and when they go back into their network, they're owned," Brennan said.

Crooks are using off-the-shelf routers, equipped to broadcast Wi-Fi hookups around the home, to spoof the popular paid services. The spoofer broadcasts a bogus T-Mobile or AT&T connection signal, then captures data transmitted by victims, says Pravin Bhagwat, AirTight's chief technology officer.

"If I'm at a location where a particular hot-spot provider does not provide a service, but still I see its service being advertised, that means it's a spoof," says Bhagwat.

Farino estimates 95% of Wi-Fi data traffic is unencrypted.

Questions:

1. Discuss about the awareness need required for the public to use public Wi-Fi hotspots.
2. Explain about the Wi-Fi eavesdropping.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 9 – Securing the Network Connections

Networking Bible

- Read the following chapter from Networking Bible, http://file.allitebooks.com/20151128/Networking%20Bible.pdf
  - Chapter 1 – Networking Introduction

ASSIGNMENTS FROM READINGS:

1. Understand various networking concepts.
2. Explain how to setup a wireless network connection on various operating systems
3. Discuss about the threats that are related to wireless network security.

ADDITIONAL RESOURCES:

Whitepapers:

1. Setting up a wireless network, https://support.microsoft.com/en-in/help/17137/windows-setting-up-wireless-network
2. How to manage wireless network connections in Windows 10, http://www.windowscentral.com/how-manage-wireless-network-connections-windows-10
3. Configuring your Mac's network settings, http://www.macworld.com/article/2027960/configuring-your-macs-network-settings.html

Videos:

1. Networking Tutorial For Beginners - How to network to grow your business - Ask Evan, https://youtu.be/xAX6SKCw3_g
2. How to Manage Wireless Networks Windows 10, https://youtu.be/tCiGpKLIYBs
3. How to set up a wireless router on a mac, https://youtu.be/XJ7gvLUxtCc

WEEK TEN:

MODULES COVERED:

- Module 10 – Data Backup and Disaster Recovery

WEEK'S OBJECTIVES USED:

17. Understand the threats to data and the need for data backups.
18. Backup and restore data on their computers.
19. Destroy data permanently.

WEEK 8 ASSESSMENTS:

These are found in the course under Week Eight.

- Quizzes: 2 quiz questions (each question is worth 1 pt.)
- Discussion Threads: 3 Discussion thread (5 pts. each)
- Case Studies: 1 Case study with 2 questions (5 pts. each)
- Questions from Readings: 4 questions from readings (1 pt. each)

QUIZZES:

1. What is data backup?

    a. **It is the process of creating duplicate copies of important data and storing it on the media storage devices such as CD/DVD, USB, external HDD, Internet servers, cloud, etc.**

    b. It is the process of storing the data in secret place

    c. It is the process of retrieving the data from damage

    d. It is the process of deleting the unnecessary data from the media storage devices such as CD/DVD, USB, external HDD, etc.

2. Which of the following is not a data backup type?

    a. Full System Backup
    b. Incremental Backup
    c. Confidential Backup
    d. Differential Backup

DISCUSSION THREAD:

1. The management of a firm decided to replace all the desktop computers in its offices with laptops. The system administrator was instructed to sell the computers at a discounted rate to recover some of the cost of the upgrade. What should the system administrator do before selling off the computers?
2. Percy wants to back up some confidential data, but is not sure whether to do an online or an offline backup. After conducting a thorough research, he concludes that online data backup is more advantageous as compared to offline backup. What advantages of online backup vis-a-vis offline backup did he come across?
3. After reading a research paper on data loss, Anne backed up her important data. Which reasons for data loss could have prompted Anne to start backing up her data?

CASE STUDY:

The Recent TalkTalk security breach affects 157,000

Source: http://www.ehackingnews.com/2015/11/the-recent-talktalk-security-breach.html

In October 2015, the UK broadband and telecom provider TalkTalk suffered a huge data breach, which potentially put its 4 million customers at risk. The data breach included confidential information of customers such as names, addresses, dates of birth, phone numbers, email addresses, TalkTalk account details and payment card information. After the data breach occurred, the TalkTalk website was taken down as a security measure. In wake of the security breach, the share price of TalkTalk fell by a third.

However, in early November, TalkTalk downplayed the seriousness of the attack by stating that only 4% of its customers—approximately 157,000 people were affected.

The telecom firm also stated that the 28,000 obscured debit and credit cards, which were accessed by the attackers, would not be of any use to them as it was not possible to identify the customers through the stolen data.

Given the magnitude of this attack, it was initially suspected to be the doing of a foreign government. Upon investigation, it was discovered that the mastermind of the security breach was not a foreign government, but a bunch of teenagers.

This just goes on to show that even the largest firms can be brought down to their knees, if their data security measures are shambolic.

Questions:

1. Explain how would you follow precautions in such situations to avoid data theft.
2. Discuss about the credibility loss of an organization, who got affected with such data breach.

READINGS:

Certified Secure Computer User

- Read the following chapter from Certified Secure Computer User,
  - Module 10 – Data Backup and Disaster Recovery

ASSIGNMENTS FROM READINGS:

1. Explain the data backup concept and types of backup.
2. Understand the Windows 10 backup and restore process.
3. Understand the Mac OS X backup and restore process.
4. Discuss about safe data destruction concept.

ADDITIONAL RESOURCES:

Whitepapers:

1. Zero Data Loss Recovery Appliance http://www.oracle.com/us/products/engineered-systems/recovery-appliance-twp-2313693.pdf
2. Developing a Backup Strategy, https://www.jadeworld.com/pdf/white-papers/WP_BackupStrategy.pdf
3. Guide to Data Protection Best Practices, http://www.tandbergdata.com/default/assets/File/white_papers/WP_BackupGuide.pdf

Videos:

1. Data Backup Solutions & Disaster Recovery Solutions, https://youtu.be/K85xsV6eTIs
2. Disaster Recovery Solutions, https://youtu.be/pVvZ19fCwHo

WEEK ELEVEN:

WEEK'S OBJECTIVES USED:

1. Understand the need and importance of data security.
2. Implement Operating System security measures on their computers.
3. Understand Malware and its symptoms.
4. Make an informed decision about choosing the antivirus which is most relevant to their needs.
5. Understand the risks associated with different online activities.
6. Understand why and how to secure web browsers.
7. Identify safe websites.
8. Safeguard against the threats associated with online social networking.
9. Understand how to make their social networking accounts secure.
10. Understand the threats associated with email communications and how to safeguard against them.
11. Understand the threats to mobile devices and how to safeguard against them.
12. Understand the threats associated with cloud accounts and how to safeguard against them.
13. Make an informed decision about a cloud service provider which fulfills their requirements.
14. Understand the various types of networks and the threats associated with them.
15. Configure a home network.
16. Make their networks secure.
17. Understand the threats to data and the need for data backups.
18. Backup and restore data on their computers.
19. Destroy data permanently.

Week Discussion Question

Initial Response: Course Reflection – Post a short summary of your course experience. Include 3 to 5 course topics that had meaning for you in some way. Think about topics that were new for you, topics that allowed you to expand your knowledge in a particular area, or most importantly items that you see yourself applying in the future to enhance and improve your personal and/or professional life.

Participation Postings: None

***Written Assignment*:**

Summative Assessment Research Project:

Directions on Project:

The instructor will provide information about project topics, scope of work, and submission requirements. Review scoring rubric for project to aid in the construction and organization of the project. Listed below are potential guidelines your instructor **MAY** follow.

Guidelines on Graduate Project

Following are the guidelines for a graduate project. Apart from these guidelines, the instructor may also suggest guidelines and instructions as required during the course of the graduate project.

Selecting a Topic (Students)

- Choose a project on a topic of your interest related to your subject of study. The idea for a project may come from your own curiosity, from your coursework, interactions with colleagues, faculty members, and general observation.
- Explore the idea; examine its significance and feasibility. Go through the existing projects on similar topics. Conduct a preliminary research on the idea. Review the relevant literature. Examine the gap areas in research and identify issues you want to address. The idea should be new or must add significant value to the existing projects.
- Prepare a rough outline of project proposal you would like to submit. Discuss the topic and draft project proposal with your project coordinator, exchange ideas and incorporate suggestions.
- Conduct further research on the topic. Make a detailed proposal. In the project proposal you should:
    a. Introduce the topic
    b. Explain your rationale for selecting the project
    c. Describe significance of the project
    d. State the objective of the project and project outline
    e. Describe the methodology to be adopted
    f. State the timeline for the project completion
    g. Include references
- Finalize the proposal with your instructor by week five (specific instructors may vary that date)

Working on the Project (Students)

- On approval of the project, you should start working on your project. It is recommended you do this prior to the 5th week of the course, but speak with your instructor to clarify dates. Limit your research to the approved proposal.
- You have to complete your project within the stipulated deadlines. Plan your project accordingly
- While meeting the executives of a company in relation to your project, make sure you have appropriate approvals and request letters from the concerned university department.
- Make sure your instructor approves questionnaires designed for any survey in relation to the project.
- You must use any data collected in course of the research, only for the approved project. You must not share collected information with other candidates.
- Make notes of key points during the course of research. It would save lot of time in preparation of project report.
- Make sure all relevant journals, magazines, papers and books are available in the university library. Please check with the library information desk for information on resources, currently not available with the library.
- Analysis is the most critical part of the project and forms basis for all findings. Make sure you make use of appropriate statistical tools in analysis. Take guidance of your project coordinator during the analysis. Do validate your findings with your project coordinator.

Writing a Project Report (Students)

- Review the style guidelines for project report
- The project report should not exceed 7,000 words
- Abstract should be between 150-250 words
- Select A4 size; page orientation should be portrait. Specify “1” margin on all sides.
- Number all pages consecutively. Start every chapter on a new page.
- Provide double spacing
- You should use Times New Roman Font- “12” for text and “10” for footnotes. Use a larger font size for section headings.

- A project report must contain:

Content	Section
a. Title Page	Preliminaries
b. Table of Contents	
c. Abstract	
d. Introduction and background	Body of the report
e. Problem statement	
f. Objectives of the project	
g. Literature review	
h. Methodology adopted	
i. Results - project findings	
j. Recommendations	
k. Conclusion	
l. Bibliography	References
m. Appendix	
n. List of figures and tables	
o. Index words (if required)	

- Be clear and precise. Express your ideas in a logical way.
- Abstract should reflect the essence of the project
- The introduction should provide the overview of the topic and highlight its significance
- Clearly indicate the objectives of your project.
- Describe all the methods used such as interviews, questionnaires in the methodology section.
- Ensure that literature review is in your own words. Analyze other person's contribution to the topic. Identify the gaps in the literature. Emphasize on the likely contribution of your project to the existing literature on the topic.
- Describe your findings from analysis in the results section. As this is the most critical part of the project, ensure that there are no errors in analysis. Make proper inferences from analysis and findings.
- The conclusion section should summarize your objectives, findings and learning's from the project. Provide useful supplementary information in the Appendix.
- Avoid plagiarism. The project report should reflect your understanding of the topic. The majority of the paper should be in your own words and reflect your own ideas.

- Give credit for all referenced work. Provide appropriate citation and references for all quotations.
- Ensure that papers referenced are relevant and not outdated.
- Your paper should be reader friendly. Use footnotes to explain difficult terms.
- Don't use text from Wikipedia in footnotes
- All tables and figures must be suitably numbered and titled. Give appropriate credit.
- On completion, go through the entire project. Ensure there are no proofing errors and you have adhered to all guidelines related to the project.
- Submit spiral bound copies of the project to your project coordinator and the project review committee. If suggested, create a soft copy of the project in PDF format and submit it relevant authorities.

Presentation – Possible Scenarios

- On completion of your project, speak with you instructor about the presentation of the project.
- Possible considerations for the presentation (check with your instructor on specific guidelines)
- Make adequate preparation for the presentation. You should be confident while making presentation
- Your presentation must focus on:
  a. The goals of your project
  b. Key findings of the report
  c. Implications of findings
  d. Learning's
  e. Further work that needs to be done
- The presentation should not exceed 20 minutes.
- Ensure that you are aware of the guidelines related to presentation. Make sure all modes of presentation such as projectors are in order.
- Don't use more than 15 slides
- Your answers to queries from panel members must be to the point. Do not hesitate from giving examples to explain your viewpoint.
- On approval of the project, submit the requisite number of signed copies to the project coordinator, department head, university library and other authorities as prescribed.

WEEK TWELVE:

WEEK'S OBJECTIVES USED:

1. Understand the need and importance of data security.
2. Implement Operating System security measures on their computers.
3. Understand Malware and its symptoms.
4. Make an informed decision about choosing the antivirus which is most relevant to their needs.
5. Understand the risks associated with different online activities.
6. Understand why and how to secure web browsers.
7. Identify safe websites.
8. Safeguard against the threats associated with online social networking.
9. Understand how to make their social networking accounts secure.
10. Understand the threats associated with email communications and how to safeguard against them.
11. Understand the threats to mobile devices and how to safeguard against them.
12. Understand the threats associated with cloud accounts and how to safeguard against them.
13. Make an informed decision about a cloud service provider which fulfills their requirements.
14. Understand the various types of networks and the threats associated with them.
15. Configure a home network.
16. Make their networks secure.
17. Understand the threats to data and the need for data backups.
18. Backup and restore data on their computers.
19. Destroy data permanently.

Summative Assessment Final Exam:

During week ten you will be required to complete a final exam that incorporates several areas of critical thinking and decision-making.