8/17/2019

Online Cybersecurity Course

Authors

Erdem Bozdag (V00104104), Lovereet Kaur (V00104104), Avneet Kaur Kahlon (V00104104), Lok In Liang (V00104104), David Lee (V00104104)

Department of Electrical and Computer Engineering, University of Victoria

Contents

1. Introduction

1-1 Background

Every September, over 400 students enter the Faculty of Engineering as first-year students. Most of them have no prior knowledge of cyber security. As a result, there are security issues, intentional and unintentional, created by these new incoming students. It would be ideal if every incoming student is made aware of the problems and issues associated with cyber security, as well as acting appropriately to prevent potential problems. The main goal of this project is to design an online, introductory course to cyber security, for first-year engineering students, with exam questions that a student must pass.

Students expect to be able to learn and study whenever and wherever they want to. This is the reason why education paradigms are shifting to online learning. The objective of the project is to design and develop a highly effective online course that not only fulfills the current needs of the university but should be beneficial to them in the long run. There were no specific requirements for the course structure, design and duration, the key idea is to create an environment for effective learning for students. The project follows a pre-defined process which divided into three deliverables:

1. Investigate and review what a first-year engineering student should know about cyber security.
2. Formulate security guidelines for first-year engineering students.
3. Design an online, introductory course to cyber security, for first-year engineering students, with exam questions that a student must pass

To work on this project, we are a team of five members. We specified our roles and responsibilities, and our mentor was constantly involved through the entire duration of the project.

1-2 Purpose and Scope

This course is quite beneficial as the student can learn the subject from the comfort of their home. Further they can take up in their spare time and need not to sacrifice their busy hours. Along with that they can do revision as many times as they needed because revision is one of the keys for daily study and exam preparations. Revision does not need a teaching but a constant grading of performance or updating the knowledge. Performance refers to ability to

recall the subject while updating refers to improving the current knowledge of a topic from the one already had before. Since students might forget what they heard from teachers in school or college, revision them recall and remember that teaching. Therefore, this course is to be designed in such a way that they should be able to review the lecture notes or videos as many times they want to. This will clear their concepts deeply by going through again and again until they are satisfied.

Therefore, the overall scope of the project is:

1. First of all, the course should provide effective and interesting learning material to the students
2. The platform should be user-friendly
3. Login functionality is required for the course.
4. Online system should be attractive and time efficient for the students
5. There should be an exam that students must pass
6. Course should be beneficial for students and university for long run
7. Course material should be accessible as many times as students want, so that they can revise.
8. Exam should not be very hard as the main motive of the course is to create awareness of cyber security among students
9. Course should touch all the important topics of cyber security which are affecting a daily life of a student
10. Course must be in easy and simple language as all first-year students are not from technical background (difficult security terms should be explained well)

1-3 Problems encountered and Solutions

First of all, we have decided to utilize an efficient learning management system (lms) so that we can focus on the content and our customer's need. After careful investigation, we found a commercial cloud environment (talentlms) gives us a fast solution to prepare our courses. The main problem of the lms system was to customize it according to our needs. Thus, we needed to investigate in detail. Moreover, we got in touch with customer service to learn it more. One problem we thought about was to use only one course containing all our materials. In this way, the navigation of the course would be so complicated. Thus, we planned our all domains as a different course that uses the same pattern. Finally, we don't want to force all students to complete all courses, yet they can just study whatever they want. Furthermore, some students can just take the final exam since the exam is also designed as a separate course.

One of the main problems we have has been to study as a group. We have been almost all the time busy with courses and other responsibilities. Arranging meetings, making decisions would be challenging if we didn't plan how to do it. Fortunately, at the start point, we have decided to have a team leader and a note-taker. To provide equality, we have reassigned these responsibilities to different people. In this way, we have targeted to increase the participation of each member. The team leader was responsible for assigning tasks to the group members, arranging meetings and starting discussions. Sometimes we had problems to perform our meetings because of having different priorities. Then, we either try to perform online meetings or have sufficient participants. We have used Google Docs to share our outcomes with each other and have been in contact with our WhatsApp group.

We never want our course materials to be boring. After our discussion, we have decided to prepare our lectures with figures having all the information needed. We have also found different kinds of videos such as funny, professional or test-oriented to lure different kinds of students. Moreover, we have emphasized the importance of additional notes. Because some students can request from us for more information, thus we should be ready for them.

Lastly, we couldn't define our scope so easily. In the beginning, we thought to have a group of engineering students who can use our platform and give their feedbacks. We could make lectures, workshop, conferences, etc. with those students. However, because of our time limitation, we couldn't organize such a group, and then we utilize our group members as students who test the platform. We performed a small video conference to show how our platform is interactive.

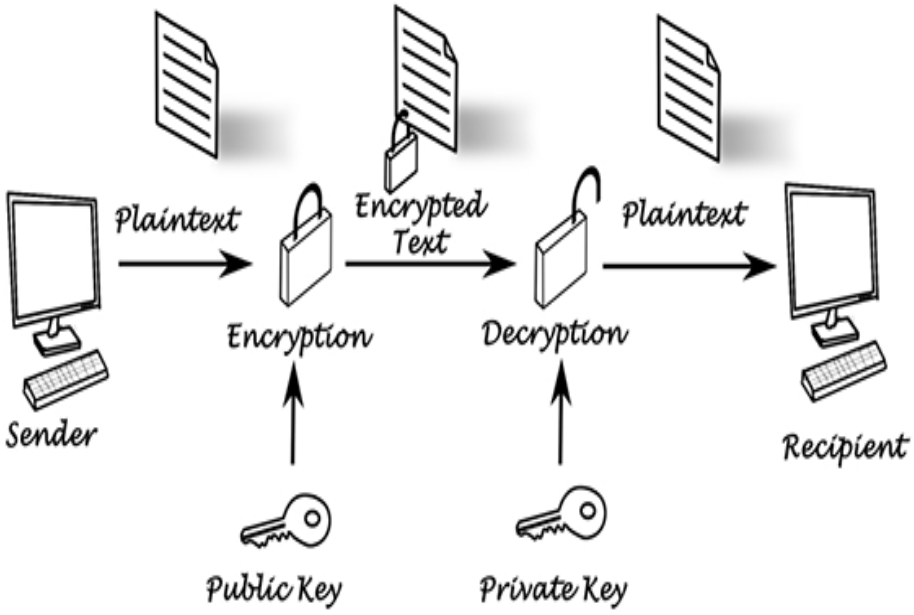
2. Course Contents

2-1. Application and Data Security

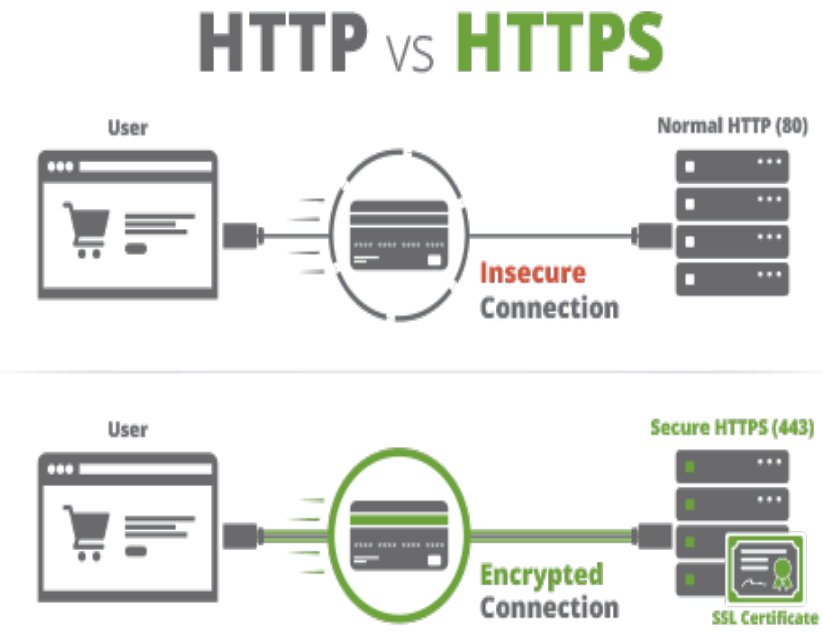
1) Lectures

It is the first topic of our course, which is talking about backup and recovery, the way of data storage, updates and patches, transmission and encryption, and protecting our operation system. In this topic, there are three main parts, which include lecture, videos, and additional note.

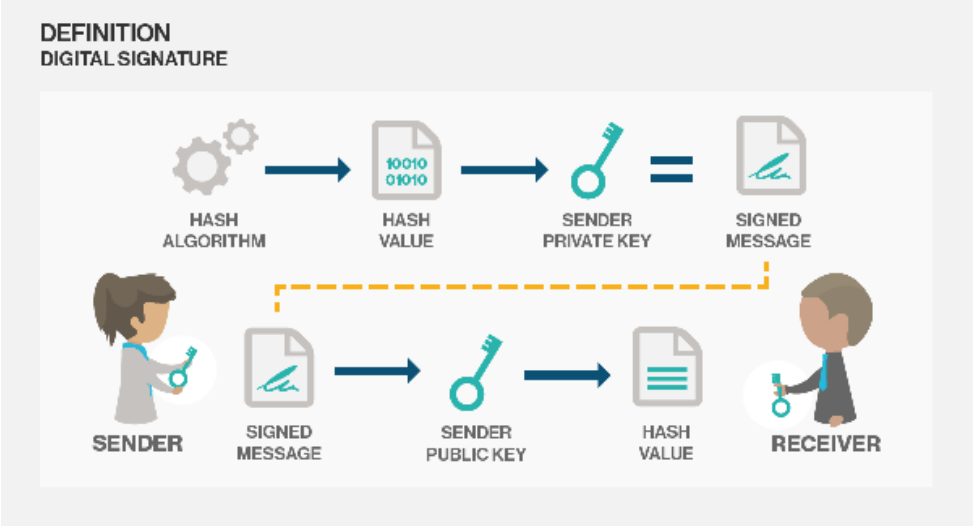
The lecture is used for the final exam which includes backup (online and offline) and recovery, the importance of updates and patches (WannaCry), what happen when we transmit (encryption, HTTP, HTTPS, and digital signatures) data in the Internet, the most vulnerable software in an operating system, how to have a secure coding (buffer overflow), and how to use log for management. It is a picture-based lecture which has a lot of straight forward image for learning sophisticated knowledge. For example, as shown in the pictures below.



Transmitting data with encryption



HTTP vs HTTPS



Definition of Digital Signature

By using a picture-based lecture, it can let the student learn those kinds of thing much more quickly and feel more enjoyable.

2) Additional Materials

a) Videos

Title	Links
Data Privacy	https://www.youtube.com/watch?v=Eh3wEtMGDRs
Data Backup	https://www.youtube.com/watch?v=rFO6NyLIP7M
What are Digital Signatures and How Do They Work?	What are Digital Signatures and How Do They Work?
Ethical Hacking: Buffer Overflow Basics	https://www.youtube.com/watch?time_continue=1&v=SOoJcrR4Ijo

b) Additional Notes

Title	Description
Online Data Storage	the benefits of online storage
What is encryption?	what is encryption and which algorithms are commonly used in our daily life
What's the Difference between HTTP and HTTPS?	More detail about HTTP and HTTPS
What happens when you run "WannaCry" Ransomware in Windows 10	It is an exciting video can let the student feel about what happens when a computer got the WannaCry virus
Bruce Schneier: Building Cryptographic Systems	Famous security guy Bruce talking about cryptographic systems

3) Exam Questions

1. Which security certification that the Secure HTTPS server have?
    a. SSL Certificate
    b. RSA Certificate
    c. DNS Certificate
    d. SDN Certificate

    Answer: a

2. During the process of asymmetric encryption, the public key is used for:
    a. Encrypt the plaintext
    b. Decrypt the encrypted text
    c. Encrypt the data on your computer
    d. Decrypt the data on your computer

    Answer: a

3. What Is Secure Coding?
    a. Secure coding is the practice of writing software that's protected from vulnerabilities.
    b. Secure coding is the practice of writing software that's protected from risks.
    c. Secure coding is the practice of writing software that's protected from bugs.
    d. Secure coding is the practice of writing software that's protected from threat.

    Answer: a

4. Which of the following is not included in Application and Data Security common sense?
    a. backup and recovery
    b. way of data storage
    c. updates and patches
    d. transmission and encryption
    e. protecting our operation system
    f. social media safety

    Answer: f

5. When encryption is using public and private keys, which type of encryption is correct?
    a. Symmetric encryption
    b. Asymmetric encryption

    Answer: b

6. Which of the following is not related to encryption?
    a. SSL
    b. Talnet
    c. TLS
    d. RSA

Answer: b

7. Which of the following ways of backup is the most safety way?
    a. Hard drive
    b. Cloud drive

    Answer: a

8. What is CIA triad?

    Answer: availability, integrity, confidentiality

9. Mac OS never have vulnerable software.
    a. True
    b. False

    Answer: b

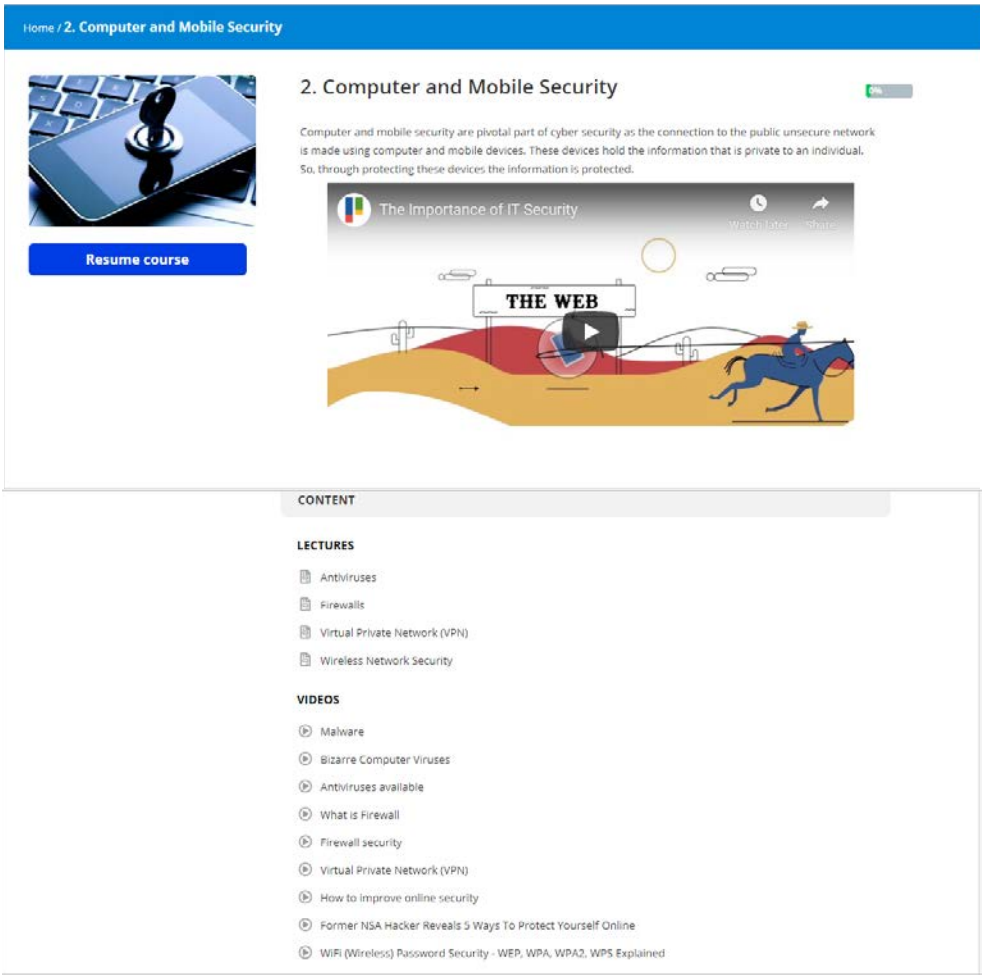
10. WannaCry ransomware attack is happened in which operating system?
    a. Mac OS
    b. Ubuntu
    c. Microsoft Window
    d. Android

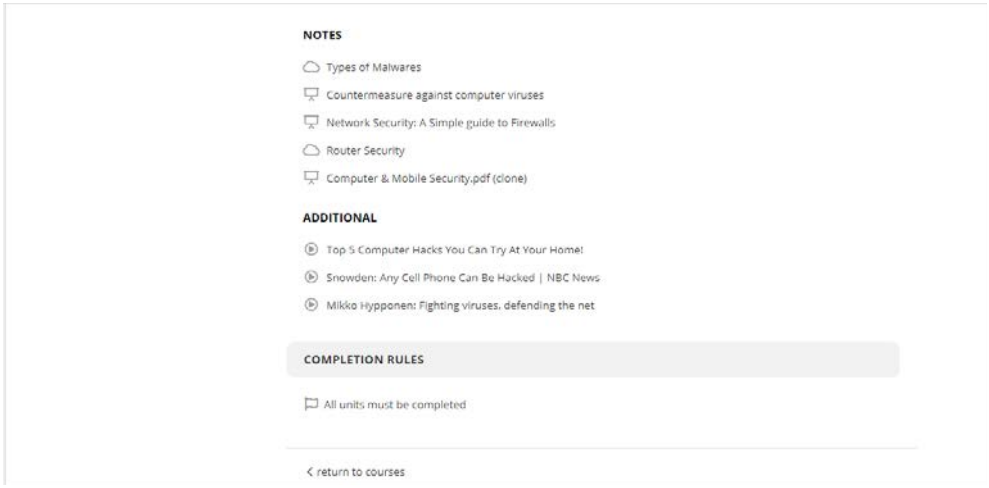
    Answer: c

2-2. Computer and Mobile Security

1) Lectures

The sole aim of cyber security is to ensure the security of the information that is saved or that is transmitted through our systems. By Computer and Mobile Security practices, we make sure that our gadgets are secured that in turn make our private information safe. By making the personal information safe, we mean that it is not accessed by any outsider and its originality is not lost. In the course, we have designed four ways in which we can make our systems safe. Each subtopic has the lectures and notes. Lectures provide concise information about a particular topic while the notes provide the elaborate information. Further, we have videos that closely coincide with the lectures and notes that are included to ensure that if someone does not want to learn by reading then they can opt for videos as it is very easy to understand something via videos. Furthermore, we have additional stuff also that is kept for students who have intend to gain further knowledge regarding cyber security.

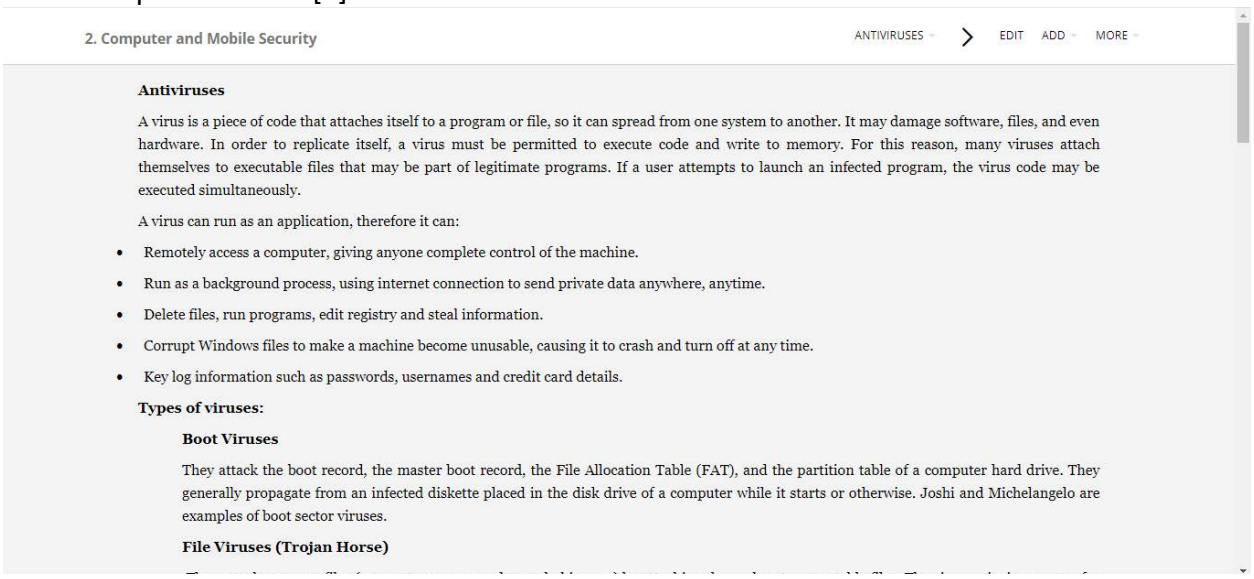




There are four subtopics under Computer and Mobile Security domain as follows:

a) Antiviruses

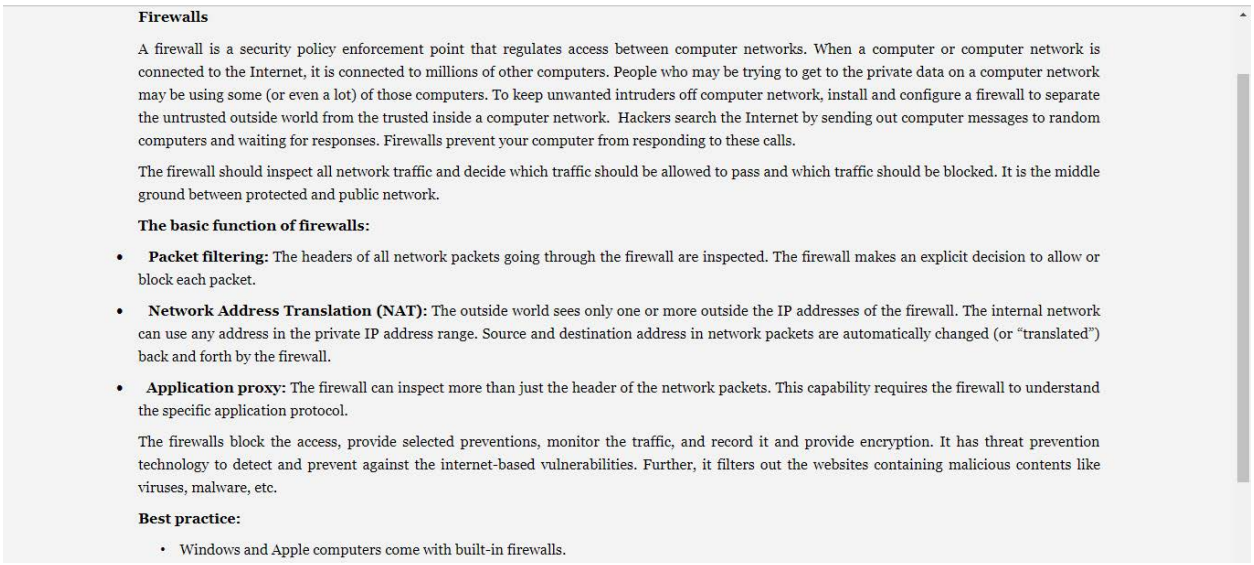
This subtopic is concerned with the issues of viruses. It includes the information like what is virus, how they affect the normal processing of the computer, its types, sources of viruses, symptoms of virus prone system and best practices that can be followed to avoid computer viruses [1].



Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2168

b) Firewalls:

This subtopic explains what firewalls are, there use and how they work. It further explains the basic functions of firewalls and best practices to use firewalls [2].



Firewalls

A firewall is a security policy enforcement point that regulates access between computer networks. When a computer or computer network is connected to the Internet, it is connected to millions of other computers. People who may be trying to get to the private data on a computer network may be using some (or even a lot) of those computers. To keep unwanted intruders off computer network, install and configure a firewall to separate the untrusted outside world from the trusted inside a computer network. Hackers search the Internet by sending out computer messages to random computers and waiting for responses. Firewalls prevent your computer from responding to these calls.

The firewall should inspect all network traffic and decide which traffic should be allowed to pass and which traffic should be blocked. It is the middle ground between protected and public network.

The basic function of firewalls:

- **Packet filtering:** The headers of all network packets going through the firewall are inspected. The firewall makes an explicit decision to allow or block each packet.
- **Network Address Translation (NAT):** The outside world sees only one or more outside the IP addresses of the firewall. The internal network can use any address in the private IP address range. Source and destination address in network packets are automatically changed (or "translated") back and forth by the firewall.
- **Application proxy:** The firewall can inspect more than just the header of the network packets. This capability requires the firewall to understand the specific application protocol.

The firewalls block the access, provide selected preventions, monitor the traffic, and record it and provide encryption. It has threat prevention technology to detect and prevent against the internet-based vulnerabilities. Further, it filters out the websites containing malicious contents like viruses, malware, etc.

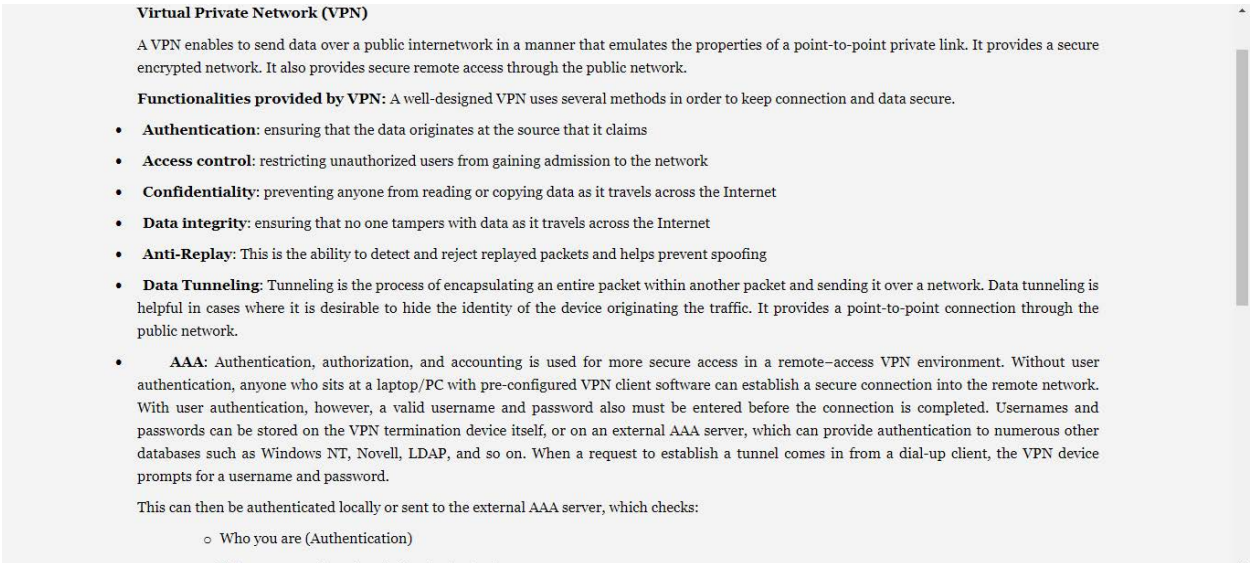
Best practice:

- Windows and Apple computers come with built-in firewalls.

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2169

c) Virtual Private Network

This subtopic includes the information about what are VPN's, functionalities provided by VPN like Authentication, Access control, confidentiality, Data integrity, Anti-replay, Data tunneling, AAA and Non-repudiation, types of VPN, and best practices **[3] [4] [5]**.



Virtual Private Network (VPN)

A VPN enables to send data over a public internetwork in a manner that emulates the properties of a point-to-point private link. It provides a secure encrypted network. It also provides secure remote access through the public network.

Functionalities provided by VPN: A well-designed VPN uses several methods in order to keep connection and data secure.

- **Authentication**: ensuring that the data originates at the source that it claims
- **Access control**: restricting unauthorized users from gaining admission to the network
- **Confidentiality**: preventing anyone from reading or copying data as it travels across the Internet
- **Data integrity**: ensuring that no one tampers with data as it travels across the Internet
- **Anti-Replay**: This is the ability to detect and reject replayed packets and helps prevent spoofing
- **Data Tunneling**: Tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. Data tunneling is helpful in cases where it is desirable to hide the identity of the device originating the traffic. It provides a point-to-point connection through the public network.
- **AAA**: Authentication, authorization, and accounting is used for more secure access in a remote–access VPN environment. Without user authentication, anyone who sits at a laptop/PC with pre-configured VPN client software can establish a secure connection into the remote network. With user authentication, however, a valid username and password also must be entered before the connection is completed. Usernames and passwords can be stored on the VPN termination device itself, or on an external AAA server, which can provide authentication to numerous other databases such as Windows NT, Novell, LDAP, and so on. When a request to establish a tunnel comes in from a dial-up client, the VPN device prompts for a username and password.

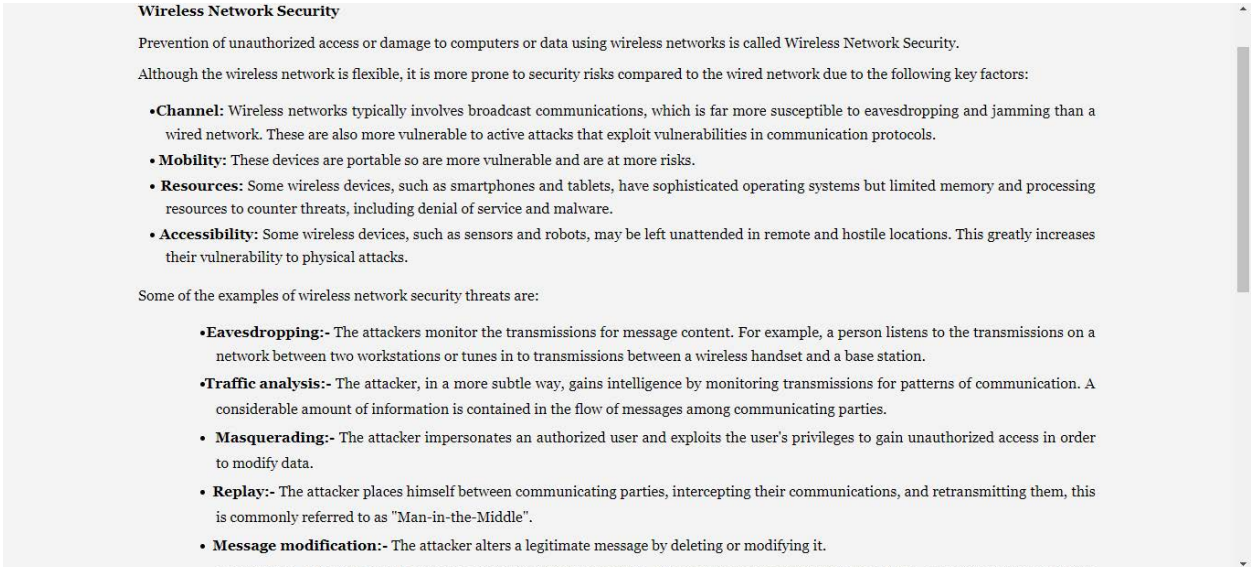
  This can then be authenticated locally or sent to the external AAA server, which checks:

  - Who you are (Authentication)

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2170

d) Wireless Network Security

This includes the explanation about the what is Wireless Network Security, why is this network insecure, potential Wireless Network threats, and best practices that need to follow in an effort to ensure the security of network [6].



Wireless Network Security

Prevention of unauthorized access or damage to computers or data using wireless networks is called Wireless Network Security.

Although the wireless network is flexible, it is more prone to security risks compared to the wired network due to the following key factors:

- **Channel:** Wireless networks typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than a wired network. These are also more vulnerable to active attacks that exploit vulnerabilities in communication protocols.
- **Mobility:** These devices are portable so are more vulnerable and are at more risks.
- **Resources:** Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources to counter threats, including denial of service and malware.
- **Accessibility:** Some wireless devices, such as sensors and robots, may be left unattended in remote and hostile locations. This greatly increases their vulnerability to physical attacks.

Some of the examples of wireless network security threats are:

- **Eavesdropping:-** The attackers monitor the transmissions for message content. For example, a person listens to the transmissions on a network between two workstations or tunes in to transmissions between a wireless handset and a base station.
- **Traffic analysis:-** The attacker, in a more subtle way, gains intelligence by monitoring transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages among communicating parties.
- **Masquerading:-** The attacker impersonates an authorized user and exploits the user's privileges to gain unauthorized access in order to modify data.
- **Replay:-** The attacker places himself between communicating parties, intercepting their communications, and retransmitting them, this is commonly referred to as "Man-in-the-Middle".
- **Message modification:-** The attacker alters a legitimate message by deleting or modifying it.

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2171

2) Additional Materials

a) Videos

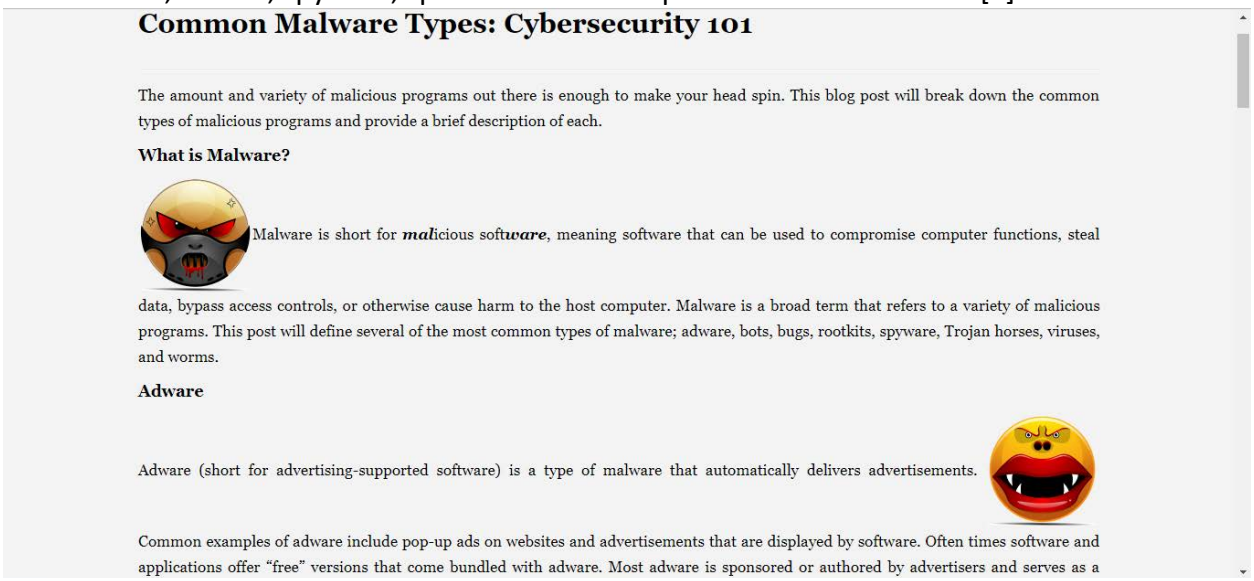
This section includes the following videos that are related to each of the subtopic:

Title	Link
Malware: Difference between computer Viruses, Worms, Trojans	https://cybersense.talentlms.com/unit/view/id:2172
Bizarre Computer viruses: the most destructive viruses in history	https://cybersense.talentlms.com/unit/view/id:2173
Antiviruses Available: the best antiviruses in market and which one to choose	https://cybersense.talentlms.com/unit/view/id:2174
Firewall: Introduction, importance	https://cybersense.talentlms.com/unit/view/id:2175
Firewall Security: how firewalls work and their importance	https://cybersense.talentlms.com/unit/view/id:2176
Virtual Private Network: what is VPN and how they work	https://cybersense.talentlms.com/unit/view/id:2177
How to improve online security	https://cybersense.talentlms.com/unit/view/id:2178
Former NSA Hacker reveals 5 ways to protect yourself online	https://cybersense.talentlms.com/unit/view/id:2179
WiFi: Password Security – WEP, WPA, WPA2, WPS	https://cybersense.talentlms.com/unit/view/id:2180

2) Additional Materials

This section includes the elaborative and in-depth information about each subtopic. It also includes the slides that include the images that can describe each subtopic making the learning and understanding interesting and easy.

a) Types of Malware: This includes the additional information on adware, bot, bug, ransomware, rootkit, spyware, spam and Malware prevention and removal [7].



Common Malware Types: Cybersecurity 101

The amount and variety of malicious programs out there is enough to make your head spin. This blog post will break down the common types of malicious programs and provide a brief description of each.

What is Malware?

Malware is short for ***mal***icious soft***ware***, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. This post will define several of the most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

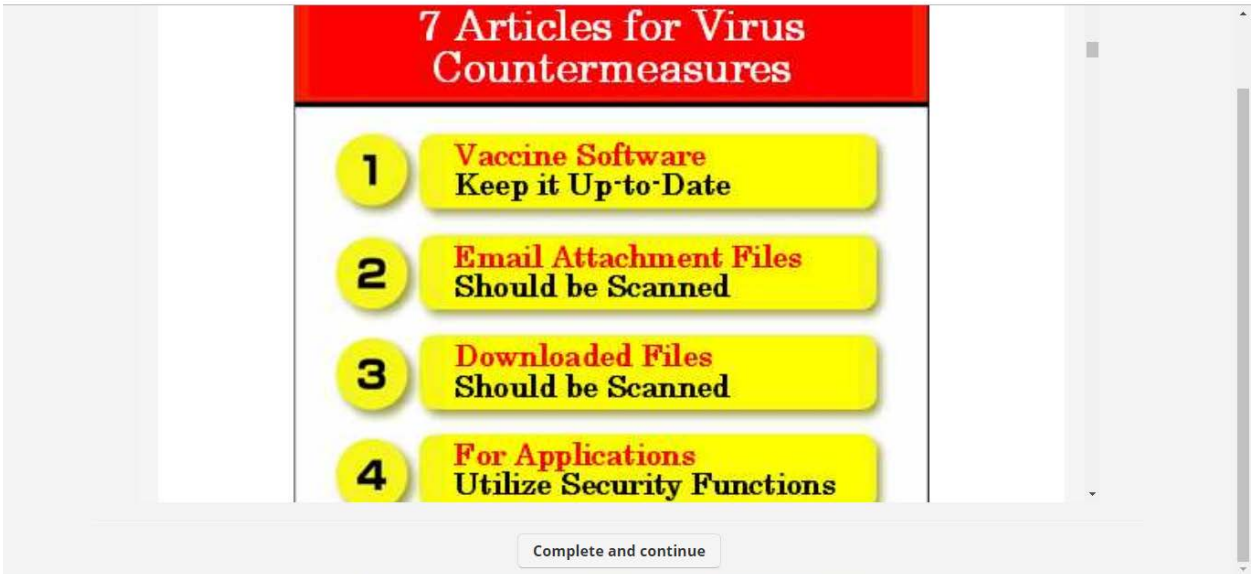
Adware

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.

Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer "free" versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2271

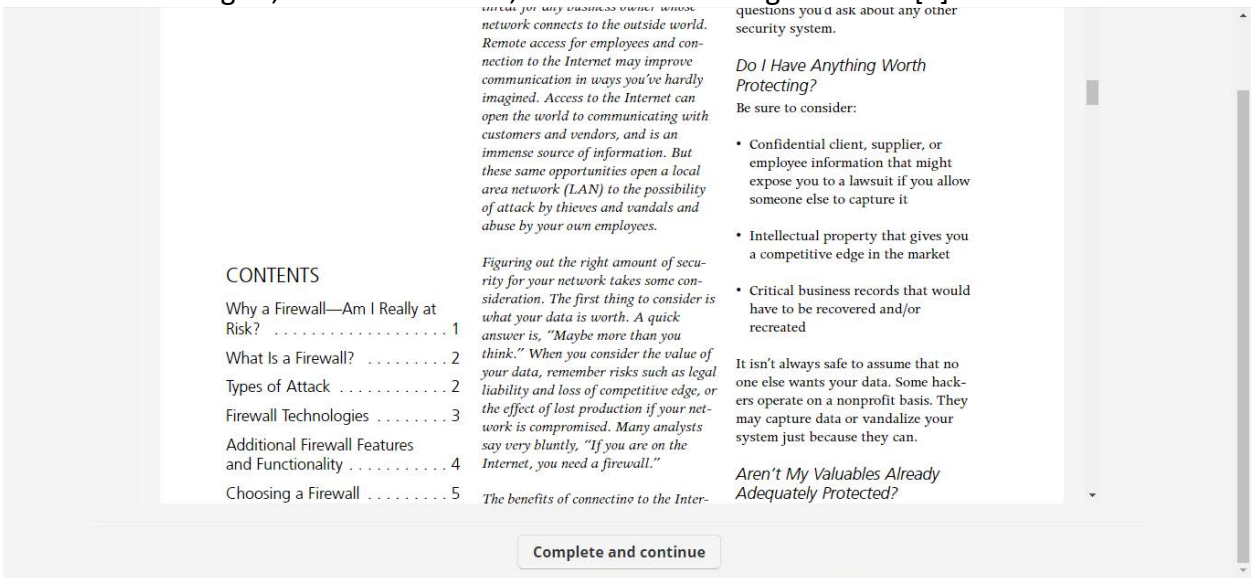
b) Countermeasures against computer viruses:
This article presented by Information-technology Promotion Agency, IT Security center includes step by step instructions on dealing with the viruses [8].



Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2183

c) Network Security: A simple guide to firewalls

This section includes the white paper by 3com corporation on network security like introduction on firewalls, types of attacks possible through weak network security, firewall technologies, its functionalities, and about choosing a firewall [9].



CONTENTS

network connects to the outside world. Remote access for employees and connection to the Internet may improve communication in ways you've hardly imagined. Access to the Internet can open the world to communicating with customers and vendors, and is an immense source of information. But these same opportunities open a local area network (LAN) to the possibility of attack by thieves and vandals and abuse by your own employees.

Figuring out the right amount of security for your network takes some consideration. The first thing to consider is what your data is worth. A quick answer is, "Maybe more than you think." When you consider the value of your data, remember risks such as legal liability and loss of competitive edge, or the effect of lost production if your network is compromised. Many analysts say very bluntly, "If you are on the Internet, you need a firewall."

The benefits of connecting to the Inter-

questions you'd ask about any other security system.

Do I Have Anything Worth Protecting?

Be sure to consider:

- Confidential client, supplier, or employee information that might expose you to a lawsuit if you allow someone else to capture it
- Intellectual property that gives you a competitive edge in the market
- Critical business records that would have to be recovered and/or recreated

It isn't always safe to assume that no one else wants your data. Some hackers operate on a nonprofit basis. They may capture data or vandalize your system just because they can.

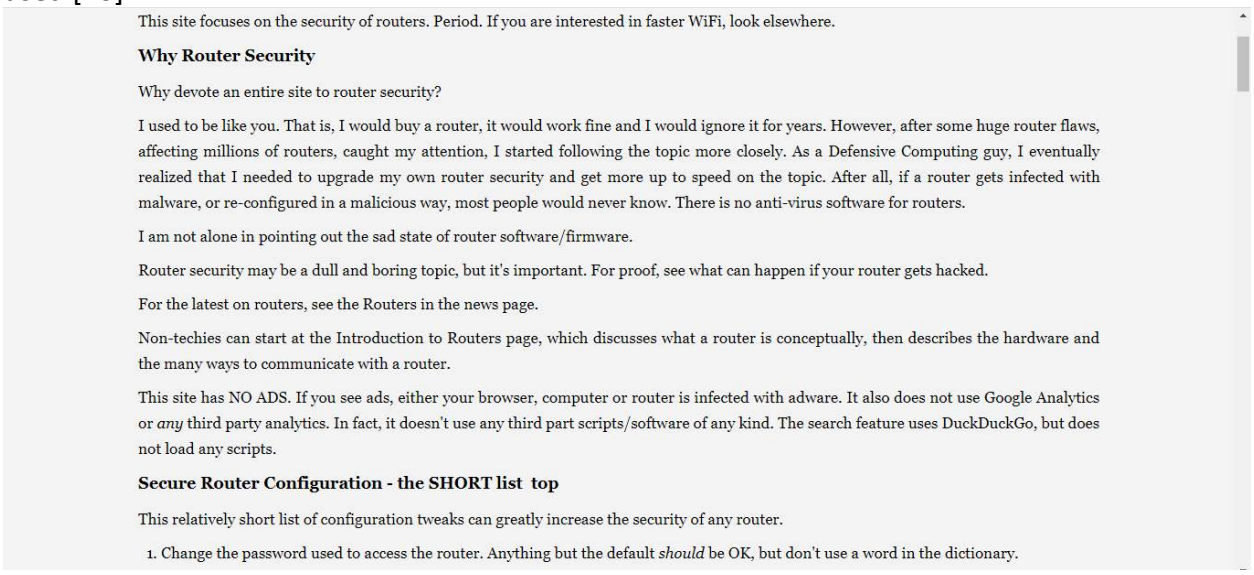
Aren't My Valuables Already Adequately Protected?

Complete and continue

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2182

d) Router Security:

This article includes the information on importance of router security, configuration of router to make it secure, recommendations on configuration and type of router to be used [10].



This site focuses on the security of routers. Period. If you are interested in faster WiFi, look elsewhere.

Why Router Security

Why devote an entire site to router security?

I used to be like you. That is, I would buy a router, it would work fine and I would ignore it for years. However, after some huge router flaws, affecting millions of routers, caught my attention, I started following the topic more closely. As a Defensive Computing guy, I eventually realized that I needed to upgrade my own router security and get more up to speed on the topic. After all, if a router gets infected with malware, or re-configured in a malicious way, most people would never know. There is no anti-virus software for routers.

I am not alone in pointing out the sad state of router software/firmware.

Router security may be a dull and boring topic, but it's important. For proof, see what can happen if your router gets hacked.

For the latest on routers, see the Routers in the news page.

Non-techies can start at the Introduction to Routers page, which discusses what a router is conceptually, then describes the hardware and the many ways to communicate with a router.

This site has NO ADS. If you see ads, either your browser, computer or router is infected with adware. It also does not use Google Analytics or *any* third party analytics. In fact, it doesn't use any third part scripts/software of any kind. The search feature uses DuckDuckGo, but does not load any scripts.

Secure Router Configuration - the SHORT list top

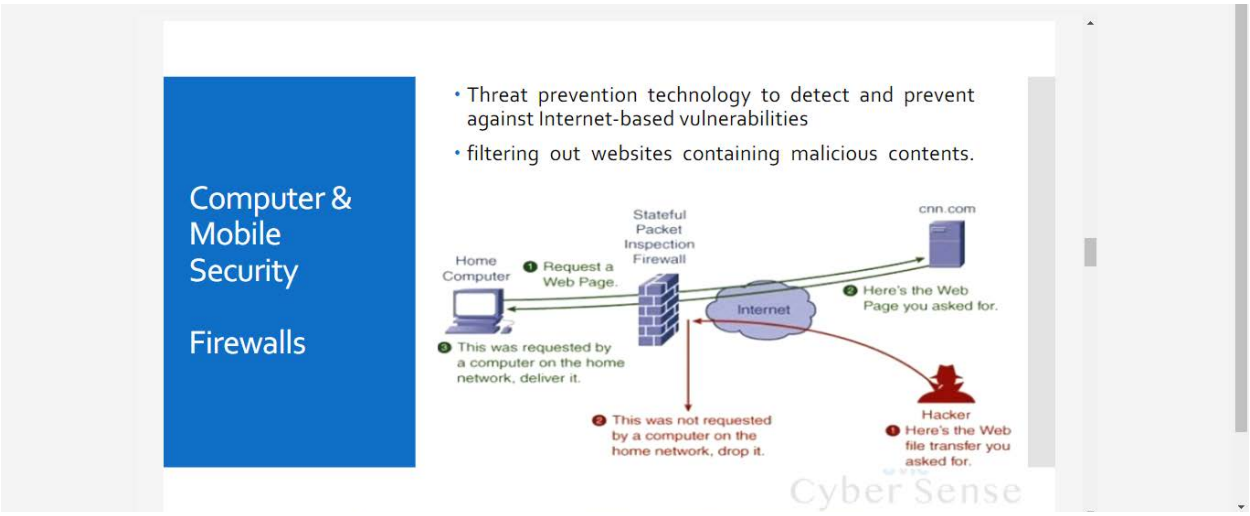
This relatively short list of configuration tweaks can greatly increase the security of any router.

1. Change the password used to access the router. Anything but the default *should* be OK, but don't use a word in the dictionary.

Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2184

e) Computer and Mobile Security

This section includes the images that describe use of each subtopic very easy.



Link to the subtopic: https://cybersense.talentlms.com/unit/view/id:2279

2-2.4 Additional

This section includes some additional videos that are very useful for acquiring additional knowledge.

Title	Link
Top 5 computer hacks you can try at your home	https://cybersense.talentlms.com/unit/view/id:2146
Snowden: any cell phone can be hacked | NBC news	https://cybersense.talentlms.com/unit/view/id:2150
Mikko Hypponen: fighting viruses, defending the net	https://cybersense.talentlms.com/unit/view/id:2156

3) Exam Questions

1. Using VPN, we can access _____
   a) Access sites that are blocked geographically
   b) Compromise other's system remotely
   c) Hide our personal data in the cloud
   d) Encrypts our local drive files while transferring

Ans: a

2. _____ are also used for hides user's physical location.
   a) Firewall
   b) Antivirus
   c) Incognito mode
   d) VPN

Ans: d

3. _____ masks your IP address.
   a) Firewall
   b) Antivirus
   c) VPN
   d) Incognito mode

Ans: c

4. A _____ can hide a user's browsing activity.
   a) Firewall
   b) Antivirus
   c) Incognito mode
   d) VPN

Ans: d

5. For secure connection, Remote access VPNs rely on _____ and _____
   a) IPSec, SSL
   b) L2TP, SSL
   c) IPSec, SSH
   d) SSH, SSL

Ans: a

6. _____ is the kind of firewall is connected between the device and the network connecting to internet.
   a) Hardware Firewall
   b) Software Firewall
   c) Stateful Inspection Firewall
   d) Microsoft Firewall

Ans: a

7. _____ is software that is installed using internet connection or they come by-default with operating systems.
   a) Hardware Firewall
   b) Software Firewall
   c) Stateful Inspection Firewall
   d) Microsoft Firewall

Ans: b

8. Firewall examines each _____ that are entering or leaving the internal network.
   a) emails users
   b) updates

c) connections
d) data packets

Ans: d

9. Packet filtering firewalls are deployed on _____
   a) routers
   b) switches
   c) hubs
   d) repeaters

Ans: a

10. In the _____ layer of OSI model, packet filtering firewalls are implemented.
    a) Application layer
    b) Session layer
    c) Presentation layer
    d) Network layer

Ans: d

11. Which of the following is a type of program that either pretends to have, or is described as having, a set of useful or desirable features but actually contains damaging code.
    A) Trojans
    B) Viruses
    C) Worm
    D) Adware
    E) Bots

Ans: a

12. Which of the following is the type of software that has self-replicating software that causes damage to files and system?
    A) Viruses
    B) Trojan horses
    C) Bots
    D) Worms
    E) Backdoors

Ans: d

13. Which of the following is a program capable of continually replicating with little or no user intervention?
    A) Virus
    B) Troja1n horses
    C) Rootkit

D) Worms
E) Bots

Ans: a

14. Which of the following is a software that, once installed on your computer, tracks your internet browsing habits and sends you popups containing advertisements related to the sites and topics you've visited?
    A) Backdoors
    B) Adware
    C) Malware
    D) Bots
    E) Spyware

Ans: b

15. What is the software called that's designed to exploit a computer user and is a broad term covering computer viruses, worms, Trojan, adware, etc.?
    A) Backdoors
    B) Key-logger
    C) Malware
    D) Bots
    E) Spyware

Ans: c

16. Which among them has the strongest wireless security?
    a) WEP
    b) WPA
    c) WPA2
    d) WPA3

Ans: d

17. Which among the following is the least strong security encryption standard?
    a) WEP
    b) WPA
    c) WPA2
    d) WPA3

Ans: a

18. WPS stands for _____
    a) WiFi Protected System
    b) WiFi Protected Setup

c) WiFi Protocol Setup
d) Wireless Protected Setup

Ans: b

19. It is recommended to use WPA2 or WPA3 encryption standard as they are strong and more secure.
    a) True
    b) False

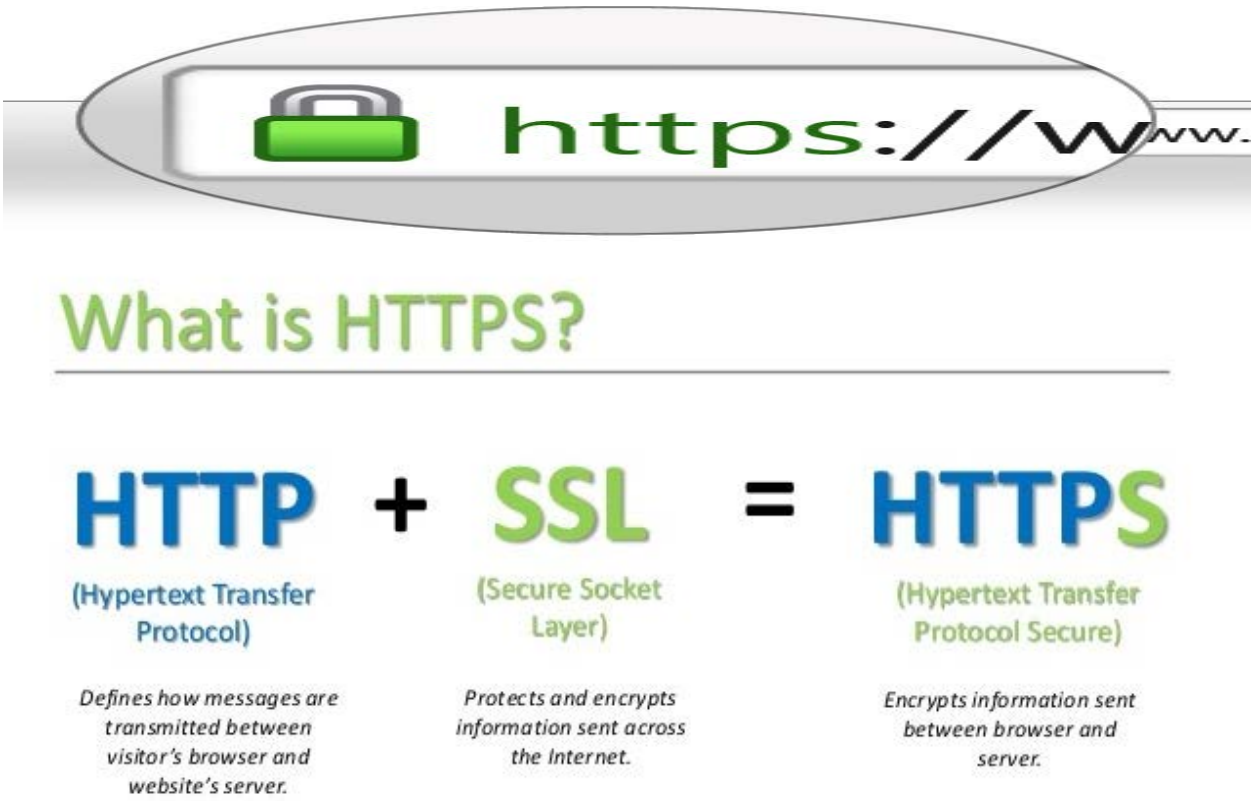
Ans: t

20. _____ began to show up few years back on wireless access points as a new way of adding or connecting new devices.
    a) WPA2
    b) WPA
    c) WPS
    d) WEP

Ans: c

2-3.Error! Bookmark not defined.Internet Safety

1) Lectures



Why HTTPS is important?

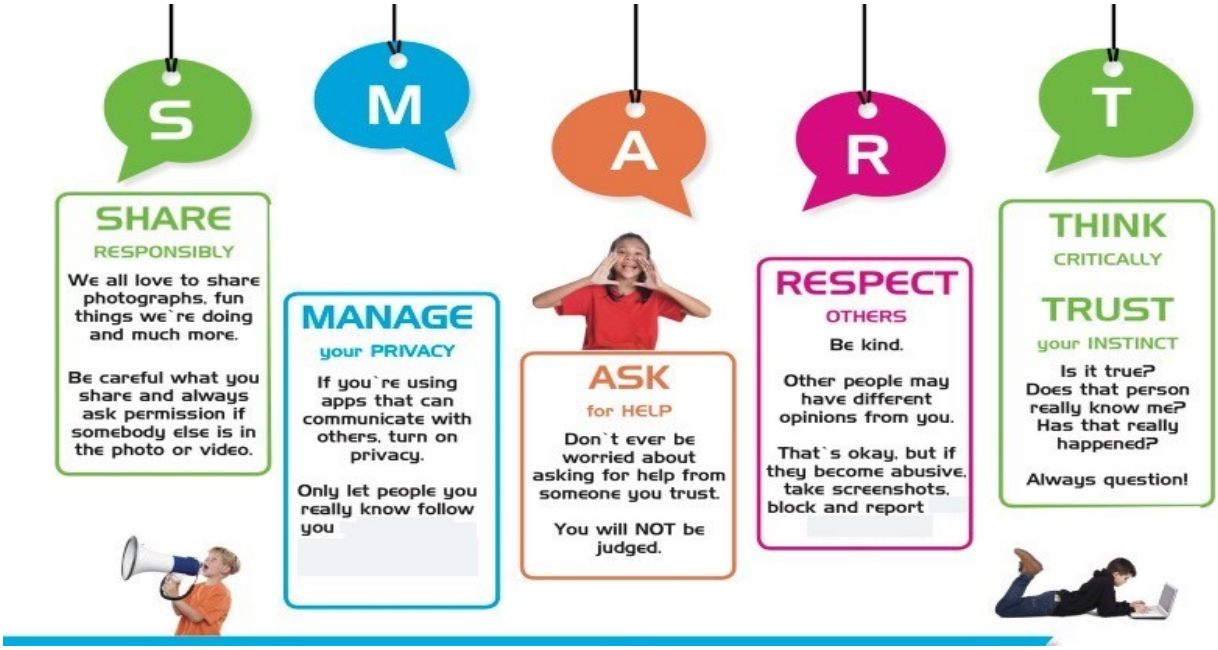
When visiting a webpage, pay close attention to the page's URL, because the suspicious websites almost look similar to the genuine website which you are looking for. Before you enter any personal information on a webpage such as your credit card information, your passwords and even your date of birth, check the URL to make sure it starts with https and is proceeded by a locked headlock icon. This makes you secure while browsing and using internet.

HTTP + SSL = HTTPS

HTTP is the Hypertext Transfer Protocol which defines how messages are transmitted between visitor's browser and website's server.

SSL is Secure Socket Layer which protects and encrypts information sent across the internet.

HTTPS is Hypertext Transfer Protocol Secure which encrypts information sent between browser and server.



Be SMART while using internet. These are the 5 key steps which you should always keep in mind while using internet to keep yourself secure.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Phishing takes place mainly through emails. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

"Phish" is pronounced just like it's spelled, which is to say like the word "fish" — the analogy is of an angler throwing a baited hook out there (the phishing email) and hoping you bite.

Spear phishing

When attackers try to craft a message to appeal to a specific individual, that's called *spear phishing.* (The image is of a fisherman aiming for one specific fish, rather than just casting a baited hook in the water to see who bites.) Phishers identify their targets (sometimes using information on sites like LinkedIn) and use spoofed addresses to send emails that could plausibly look like they're coming from co-workers.

Whale phishing

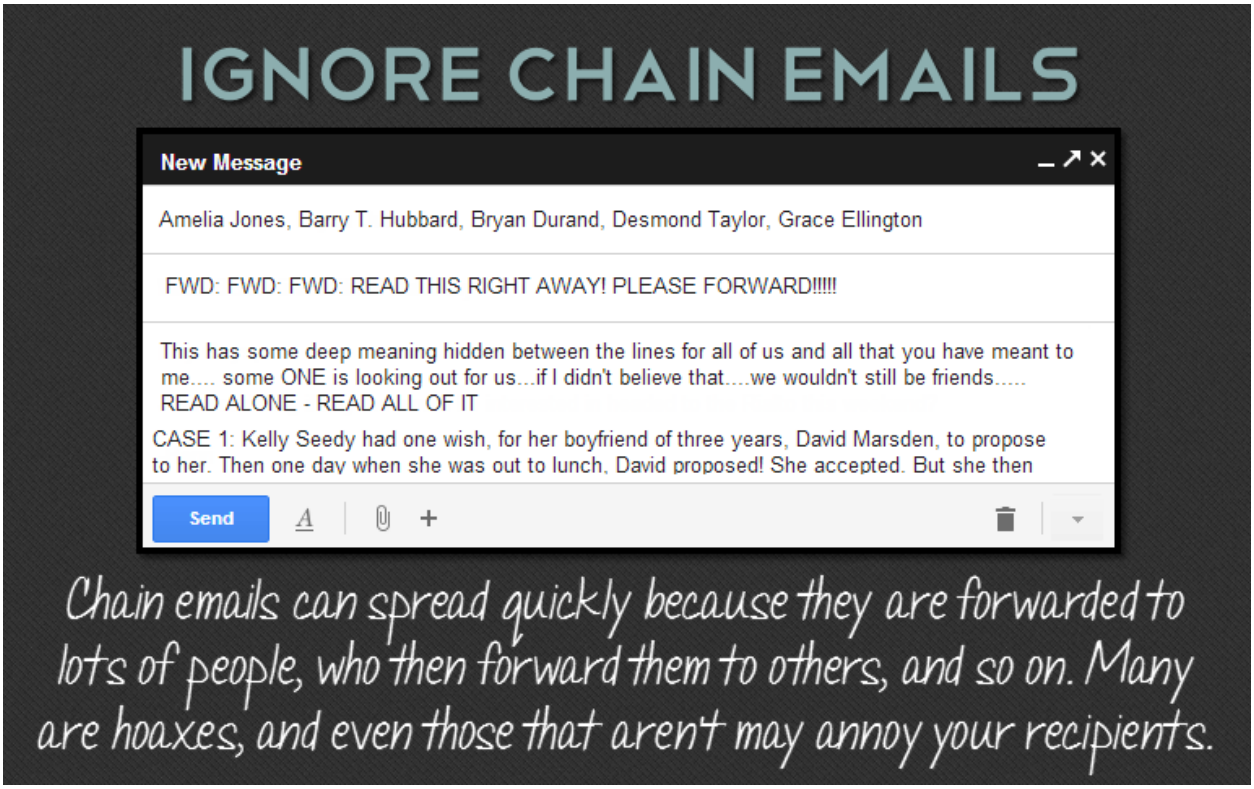
Whale phishing, or *whaling*, is a form of spear phishing aimed at the very big fish — CEOs or other high-value targets.

How to prevent phishing?

1. Always check the spelling of the URLs in email links before you click or enter sensitive information
2. Watch out for URL redirects, where you're subtly sent to a different website with identical design
3. If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply
4. Never click on links given in that email or download an attachment, as it may be some malware which may harm your computer.


spear Phishing
SPEAR PHISHING:
a targeted scam directed at a specific person or department
STOP
WHEN YOU RECEIVE A SUSPICIOUS EMAIL
Do not 'reply,' 'reply to all,' or 'forward' the email
Do not open any attachments in the email
Do not click any website links provided in the message
CAREFULLY EXAMINE THE EMAIL
Beware of unknown senders or sensational subject lines
Look at the hyperlinks in the email carefully
If the message claims it's from your financial institution, call them to verify
LOOK
RECOGNIZE
RECOGNIZE THE RED FLAGS
Misspelled words and poor grammar
Urgent, sensational subject lines
Promises of free gifts or prizes
Requests to verify your password or account


EMAIL SAFETY
1 WHO SENT IT?
FROM: A PERSON <APERSON@YOUR.ORG>
recognized
FROM: A PERSON <SOMEONELSE@DMAIL.COM>
unrecognized
2 WAS IT EXPECTED?
expected
unexpected
3 ACTION REQUESTED?
click link,
view attachment,
reply/call,
make payment,
send info
no action
OK!
4 VERIFY WITH SOURCE
USE ONLY KNOWN
CONTACT INFORMATION

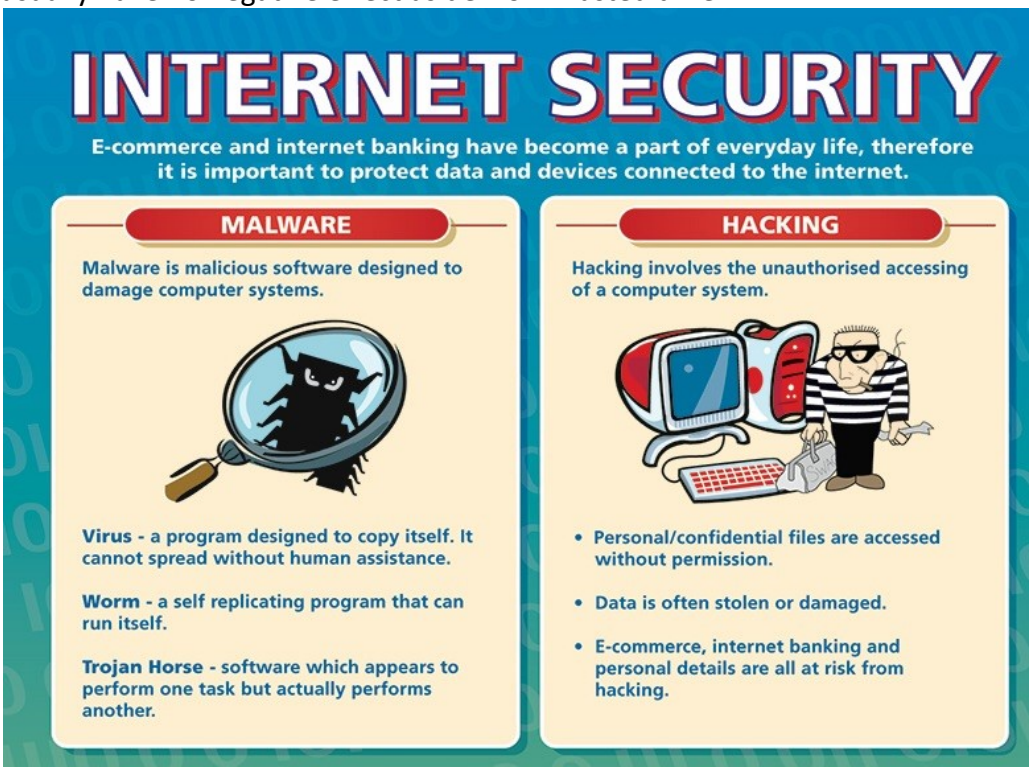


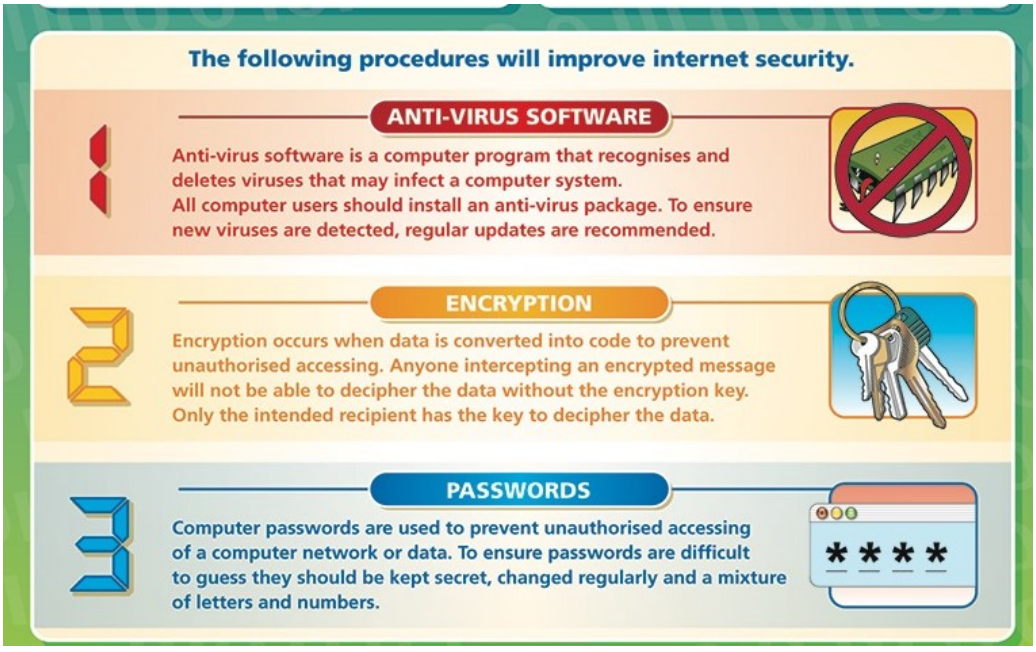
Chain emails

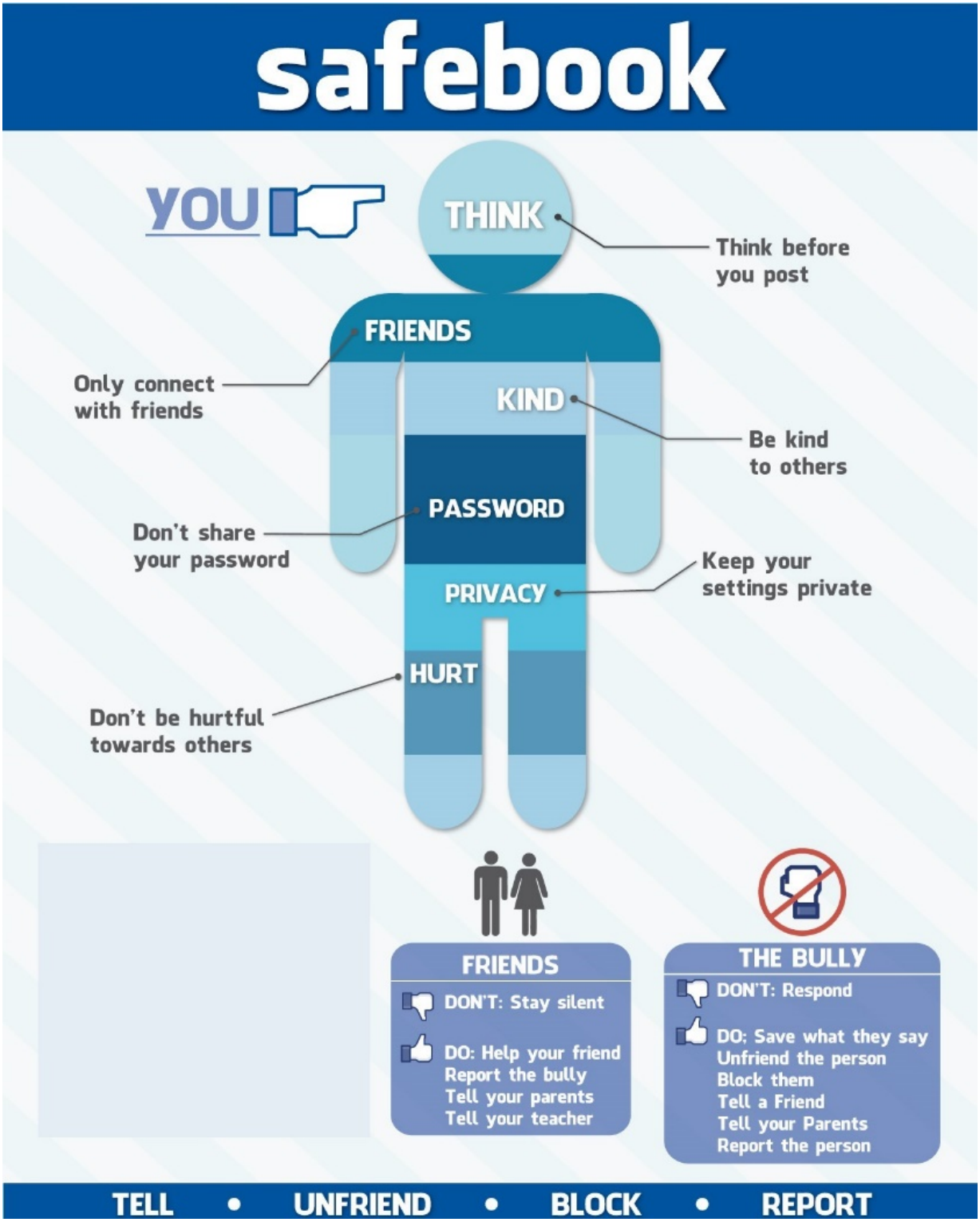
A **chain email** is a message that attempts to convince the recipient to forward this email on to a certain number of recipients (either a predefined number or as many as possible). The "chain" is actually an exponentially growing pyramid (a tree graph) that cannot be sustained indefinitely. Common methods used in chain emails include emotionally manipulative stories, get-rich-quick pyramid schemes, and the exploitation of superstition to threaten the recipient with bad luck or even physical violence or death if he or she "breaks the chain" and refuses to adhere to the conditions set out in the email. Chain emails are often sent via email messages, postings on social network sites, and text messages.
There are two main **types** of chain emails:

Hoaxes: Hoaxes attempt to trick or defraud users. A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus. It could also be a scam that convinces users to spread the email to other people for a specific reason, or send money or personal information. Phishing attacks could fall into this.

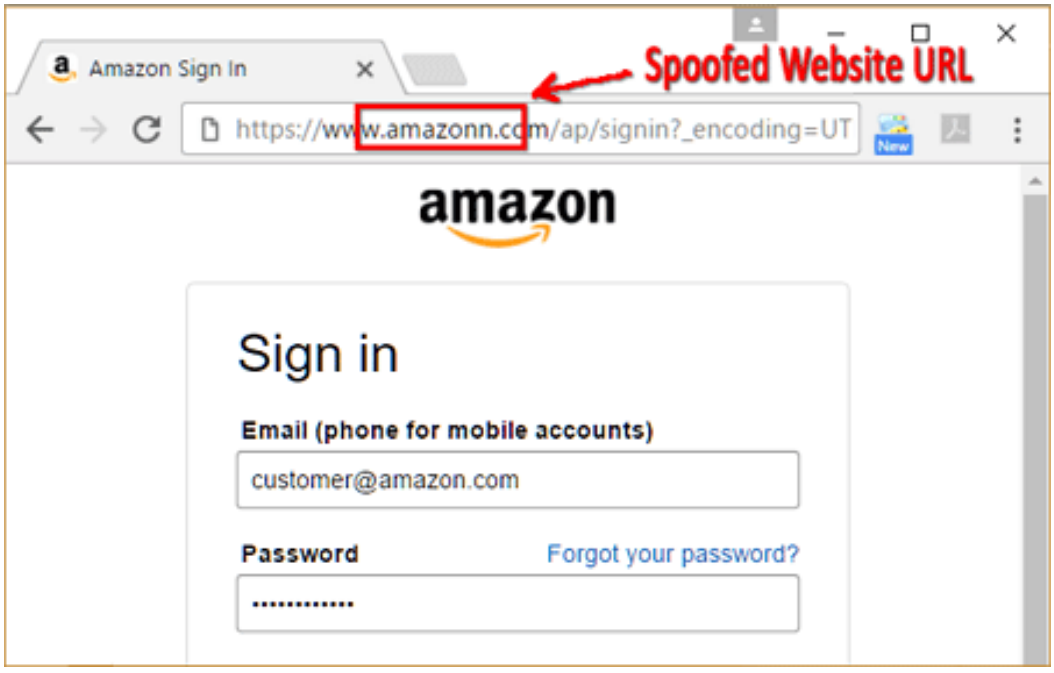
Urban legends: Urban legends are designed to be redistributed and usually warn users of a threat or claim to be notifying them of important or urgent information. Another common form are the emails that promise users monetary rewards for forwarding the message or suggest that they are signing something that will be submitted to a particular group. Urban legends usually have no negative effect aside from wasted time.






safebook
YOU
THINK
Think before you post
FRIENDS
Only connect with friends
KIND
Be kind to others
PASSWORD
Don't share your password
PRIVACY
Keep your settings private
HURT
Don't be hurtful towards others
FRIENDS
DON'T: Stay silent
DO: Help your friend
Report the bully
Tell your parents
Tell your teacher
THE BULLY
DON'T: Respond
DO: Save what they say
Unfriend the person
Block them
Tell a Friend
Tell your Parents
Report the person
TELL • UNFRIEND • BLOCK • REPORT


SAFETY TIPS FOR
SHOPPING ONLINE
Use a strong and unique password.
Do your shopping with a secure device.
Beware of discount deals that seem too good to be true.
Check the specifications of an item before making a purchase.
Check the legitimacy of the website you're viewing.
SALE!
BUY


Amazon Sign In
Spoofed Website URL
https://www.amazonn.com/ap/signin?_encoding=UT
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your password?

2) Additional Materials

a) Videos

Title	Links
Phishing awareness	https://www.youtube.com/watch?v=wZwxxdXmazs
Social Engineering	https://www.youtube.com/watch?v=VkTH6BPMMFA
Wi-Fi Security	https://www.youtube.com/watch?v=lY9Dy7xNuDU

b) Additional Notes

Title	Description
10 steps to staying secure on public Wi-Fi	https://www.welivesecurity.com/2015/09/02/10-steps-staying-secure-public-wi-fi/
Bruce Schneier: The battle for power on the internet	https://www.youtube.com/watch?v=h0d_QDgl3gI
Identity theft	https://www.youtube.com/watch?v=MGqIoMggb30
Guide to ID theft awareness and avoidance	https://www.monster.com/career-advice/article/protect-against-identity-theft
How to avoid Internet scams	https://www.whoishostingthis.com/resources/online-fraud/

3) Exam Questions

1. If someone do cyber-bullying to you

a) No one can do that to you, be rude to them as well and argue

b) Ask them to meet in person

c) No need to argue, save what they say

d) Continue texting them, and be kind

Answer: c

Explanation: You have to keep record of such things, which will help you while reporting as you will have evidence of what they said to you. Don't give them chance to record your bad behavior by arguing with them.

2. You need to be kind to others on internet.

a) True

b) False

Answer: a

Explanation: Treat others in same way like you want to be treated.

3. It is OK to shop from a website with minor difference in URL, only if you get good discounts

a) True

b) False

Answer: b

Explanation: It can be a spoofed website which will steal your personal information or even harm your computer.

4. Holiday status updates/snaps should be uploaded on social media

a) Not uploaded, to protect your property from burglars

b) Uploaded, so that your friends can see and know where you are

c) Few of them can be uploaded

Answer: a

5. Chain emails should

a) Be forwarded, so that important message could reach everyone

b) No need to forward, should be deleted

c) Sometimes OK to forward to few friends

d) Should be replied to warn them, to not send such emails in future

Answer: b

Explanation: It can be hoaxes, don’t spread them to others.

6. When you click a link given in a phishing email

a) It takes you to original website

b) It will be a fun

c) Nothing will happen, waste of time

d) It takes you to hacker's website which looks similar to original

Answer: d

7. _____ is saying bad words or saying things that other people could feel bad about it.

a) Cyber bullying

b) Flaming

c) Trickery

d) Netiquette

Answer: a

8. Pair up the following, keeping in mind the internet safety rules:

a) Ask	a) Respect
b) Give	b) Responsibly
c) Think	c) help
d) Share	d) Critically

Answer: ac , ba , cd , db

9. The website URL must starts with 'https' along with

a) Close headed lock

b) Open headed lock

Answer: a

10. It is always good to download software from any website, if it is free.

a) True

b) False

Answer: b

Explanation: you should check the legitimacy of the website, it can be a Trojan or other malicious software.

11. Phishing is

a) Fraudulent act by sending emails to users in order to reveal their personal information

b) An online sporting event

c) An online game, where you can win 1000's of dollars by catching fishes in ocean.

Answer: a

12. Is it acceptable to write in all capital letters?

a) Yes, It doesn't matter whether capital or small

b) Not acceptable, as it is an internet code for shouting and is rude

Answer: b

13. What is Hacking?

a) Sending some bait e-mails to users

b) Unauthorized accessing of a computer system

c) Protecting your personal information from hackers

Answer: b

14. What should be chosen for a status update when revealing information about your location?

a) Everyone

b) All users

c) My friends only

Answer: c

15. If a flashing pop-up appears saying that you are the 1000th visitor and it wants you to 'click here' to claim your prize. What do you do?

a) I'm so lucky. Go for it.

b) Send it to your friend because you are skeptical about it.

c) I'll close the advertisement.

Answer: c

Explanation: Be cautious if something seems too god to be true.

16. Since the internet is loaded with educational information, I should use it as much as I like and go to ALL the sites I want to see.

a) You're the coolest, surf away

b) I would check the legitimacy of the website I'm viewing

c) The internet has very few 'bad' sites. I don't have to worry about that kind of stuff

Answer: b

17. I'm online and I meet someone my age in a chat room. Is it OK to give him or her my address or phone number so we can get together?

a) Yes

b) No

Answer: b

18. When targeting victims, dangerous criminals disguise their identities on social network sites.

a) True

b) False

Answer: a

19. What should you do if someone you do not know wants to chat?

a) Be cautious and don't give them any personal information

b) E-mail them a picture of yourself

c) Tell them to chat with your friend

d) Send them a text message

Answer: a

20. What does SSL stands for?

a) Software Security Layer

b) Secure Socket Layer

c) Socket Surface level

d) Secure Shipping level

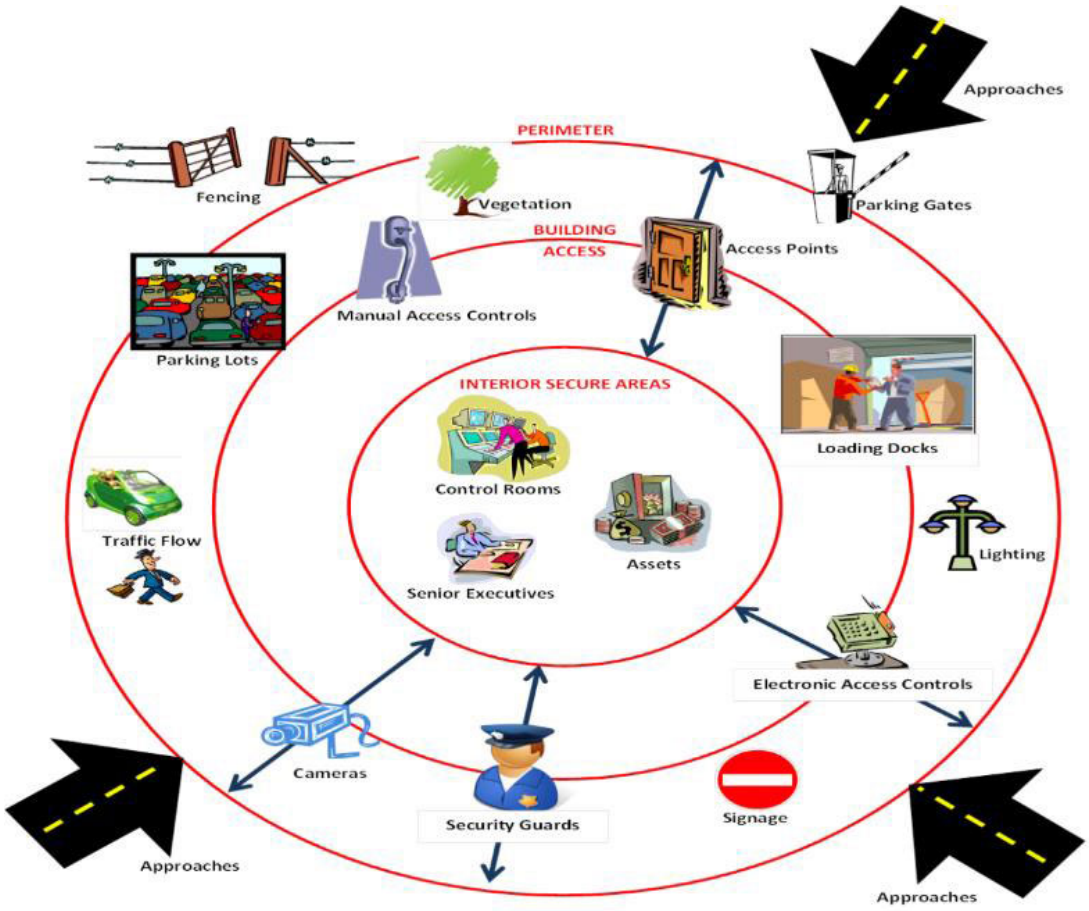
Answer: b

2-4. Physical Security Error! Bookmark not defined.

1) Lectures

Information security professionals tend not to take physical security seriously. Most IT organizations often overlook physical security because they focus on technology-centric security measures to prevent hacking. Users should have physical security mechanisms to prevent malicious attackers from stealing confidential information through physical access. In the modern era, cyber and physical systems are becoming more and more integrated. Engineering students may use a variety of devices, including laptops, USB drives, tablets, and smartphones. If electronic devices are stolen or destroyed, students may be subject to unexpected personal information infringement or financial loss.

Organizations are basically building basic physical security control mechanisms to protect their members. Firstly, perimeter security methods include Mantraps, gates, and fences. Secondly, organizations also use badges, ID cards, etc. to identify their identity; identification is important in physical security, and UVic identifies the student using an ID card that contains a photograph of the individual. Lastly, motion detectors are often used in conjunction with an alarm system to perform intrusion detection for malicious attackers.



Source: www.bayometric.com/best-practices-physical-security-management/

UVic basically provides physical security measures, but it cannot always take the appropriate security measures in the context of each student. Students should take physical security measures against computer equipment that they own or use. We recommend some best practices for physical security that engineering students should follow in their lives

- **Activate a screen lock:** Students should set their devices to be automatically screen locked when the desktop or notebook is not in use for a certain amount of time (5 minutes). It is very important to set up the screen lock function, especially when students are participating in important research projects and use their computing devices off campus.

- **Attach a label to your devices:** Students should attach labels to their desktops or laptops to prepare for loss or theft. For smartphones, it is recommended to set up a function to detect the location of lost smartphones.
- **Don't leave your devices in a public place:** Students should not leave their computing devices in public places (library coffee shops, cafeterias, etc.) for a long time to prevent malicious theft. Students are encouraged to ask for a trusted friend to watch their devices for the duration of their departure if they need to leave the devices for a short time.
- **Report a lost or stolen device quickly:** Students should report critical incidents to the relevant organization (UVic's security office or the police) without delay; for example, if a desktop or notebook computer contains confidential information, such as important research results (patents, confidential information, etc.), students must report the theft and be supported.

2) Additional Materials

a) Videos

Title	Links
Physical & Information Security Awareness	https://youtu.be/tmOGJVDvJaQ
Physcial Security - Awareness	https://youtu.be/ORS9DPKJlks

b) Additional Notes

Title	Description
Physical Security	Winning Initiatives and Best Practices for Physical Security(IFMA)

3) Exam Questions

1. Which of the following is not considered as a delaying mechanism?

A. Locks
B. Defense-in-depth measures

C. Warning signs
D. Access controls

Answer: C
Every physical security program should have delaying mechanisms, which have the purpose of slowing down an intruder so security personnel can be alerted and arrive at the scene. A warning sign is a deterrence control, not a delaying control.

2. Physical security has a different set of threats, vulnerabilities, and risks when compared to other security issues we address in this series.
True
False

Answer: True

3. Physical threats to companies include: (choose all that apply.)
A. Theft
B. Accidents
C. Cyber crimes
D. Fraud

Answer: A, B, and D
Physical security threats to companies include interruption of services, theft, fraud, sabotage, vandalism, and accidents.

4. _____ are short-term solutions to power failure.
A. Generators
B. UPSs
C. Batteries
D. Power supplies

Answer: B
UPSs are usually short-term solutions compared to generators.

5. What is a mantrap?
A. A trusted security domain
B. A mechanism for logical accessing control

C. A double-door room used for physical access control
D. A device for fire suppression

Answer: C
A mantrap is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility.

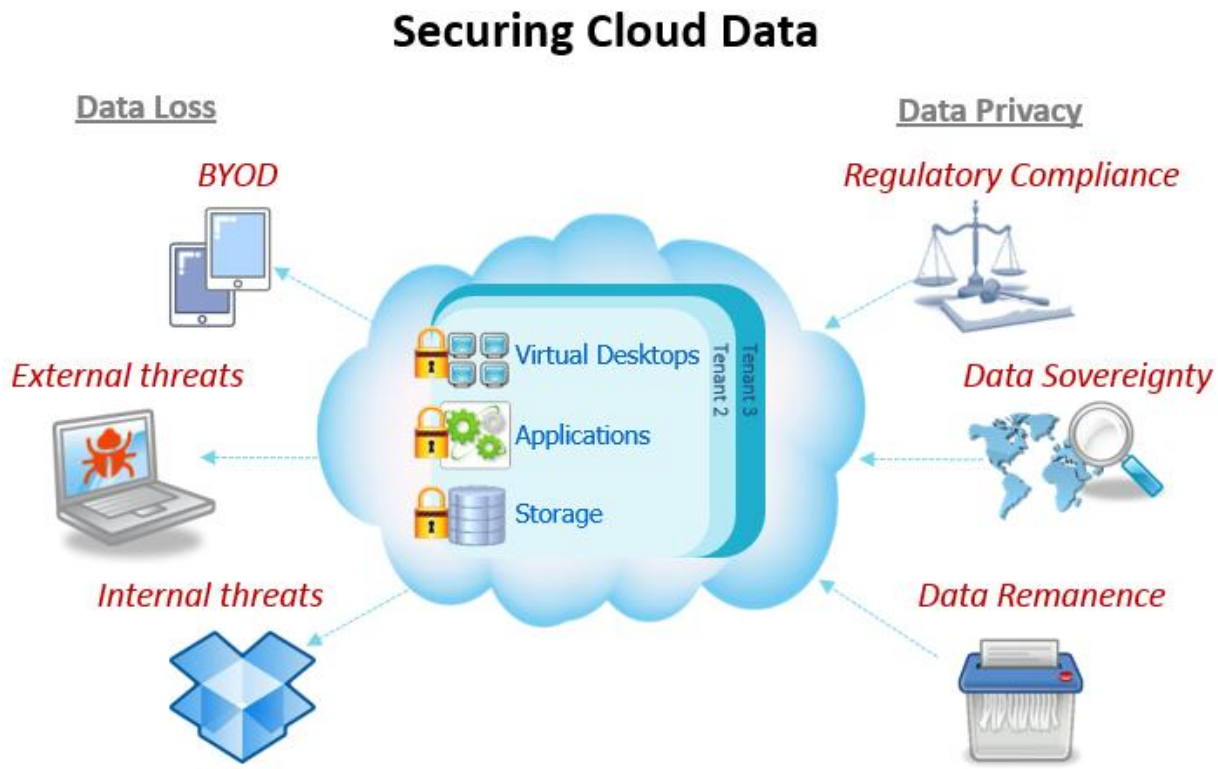
6. Which of the following is not a control category in a physical security program?
A. Deterrence and delaying
B. Response and detection
C. Assessment and detection
D. Delaying and lighting

Answer: D
The categories of controls that should make up any physical security program are deterrence, delaying, detection, assessment,
and response. Lighting is a control itself, not a category of controls.

2-5.Error! Bookmark not defined.Cloud and IoT Security

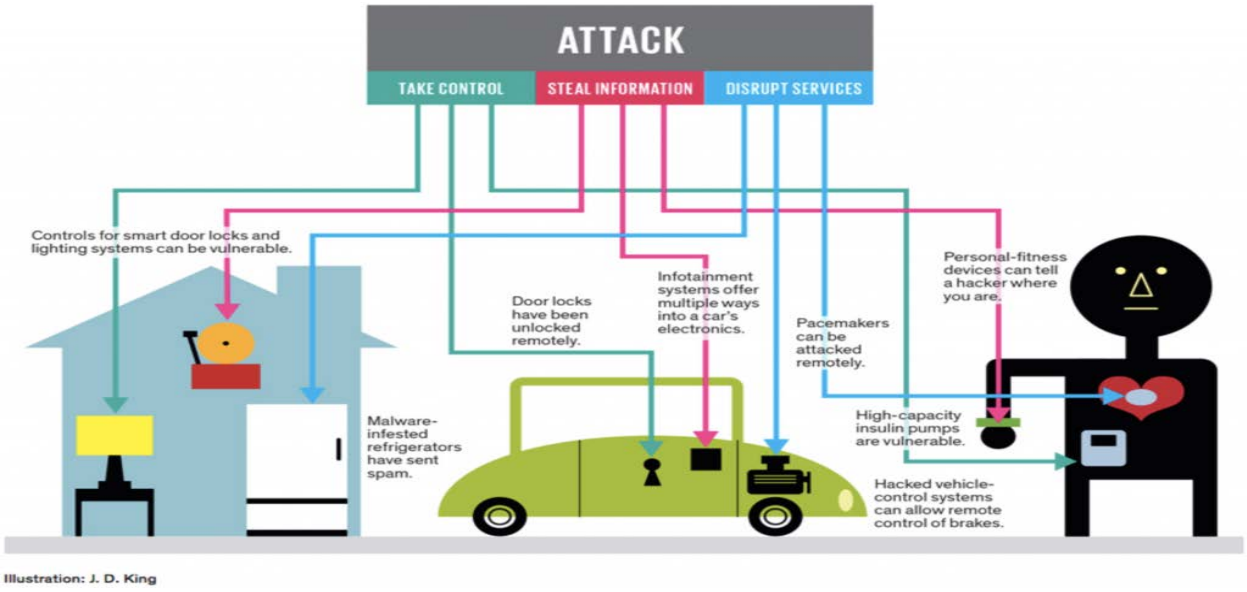
1) Lectures

- **Infrastructure-as-a-service (IaaS)**: where a third party provides highly automated and scalable IT infrastructure – server, storage, networking, and virtualization.
- **Platform-as-a-service (PaaS):** where a third party provides a developer with everything they need to develop and deploy an application, including server, storage, networking, and virtualization, operating system, middleware. However, the third party does not provide a developer with data and application.
- **Software-as-a-service (SaaS):** where a third party's software can be accessed over the web and is generally charged on a subscription basis per user or 'seat'. So, the third party provide a developer with everything, including data and application.



In the cloud environment, various issues are raised, such as security capabilities of cloud service providers, accountability between service providers and users in case of security incidents such as information leakage.

With the cloud environment, IoT (Internet of Things) devices with network and computing capabilities are also expanding the attack surface of malicious attackers. IoT devices with sensor and network capabilities include smart home appliances, security devices, cleaning robots for household use, reconnaissance drones for industrial and military use, and autonomous vehicles. In addition, IoT devices include various smart watches, motion sensors with sensors, etc., which are used by individuals in daily life as the development of wearable technology. IoT is used anywhere in everyday life, so IoT is also called Internet of everything (IoE). The following figure shows a variety of Iot devices which are connected to the network and sharing information through three kinds of cloud services



However, Internet of everything means Internet of vulnerability: Everything is being connected to the internet, so everything can be hacked. IoT devices and services have various security vulnerabilities and threats. IoT are not commonly designed with security and privacy in mind, which are often sold by companies who don't care about privacy and security in the stage of production. IoT devices may not use passwords, have weak password, or have default, generic, or undocumented accounts. Moreover, IoT devices have various vulnerabilities: insecure network services, insecure ecosystem interfaces, lack of secure update mechanism, insufficient privacy protection, insecure or outdated components, and lack of physical hardening.

We recommend some best practices for cloud and IoT security that engineering students should follow in using IoT devices on campus and in their daily lives.

- **No default password**: IoT service providers commonly provide a default username and password when selling IoT devices to consumers. Therefore, after purchasing the IoT device, students must change the default password to a complex password that is difficult for a malicious attacker to easily guess.
- **Securely store credentials and sensitive data**: Students can inherently possess credentials and sensitive personal information on vulnerable IoT devices. In particular,

wearable devices may include sensitive medical information of users. Therefore, students must store their credentials in encrypted form when they need to store their credentials on IoT devices, and backup important information frequently to prepare for theft or hacking.

- **Keep software updated:** Students should regularly perform updates to the software on their IoT devices whenever possible. If an IoT service provider provides a security alert or provides a security patch online, students should make a security patch without delay. Especially when using IOT devices connected to the student's UVic information system, a quick security patch should be implemented to ensure that their IoT devices are not used as a pathway for malicious attackers.
- **Monitor the activity (logs or traffic):** Students should check to see if their IoT devices have logging capabilities and periodically check their log records to see if a malicious actor has attempted illegal access to an asset's IoT device. Students should also check the status of their normal communication traffic on their IoT devices. If students detect anomalous behavior, such as when their devices send or receive excessive traffic, they should promptly consult security experts to check for and remove malware.

2) Additional Materials

a) Videos

Title	Links
Cloud Computing Security - Simply Speaking	https://www.youtube.com/watch?v=WiFnz5XdaQM
What is the Internet of Things (IoT) and how can we secure it?	https://youtu.be/H_X6IP1-NDc

b) Additional Notes

Title	Description
The 10 Challenges of Securing IoT Communications	https://www.pubnub.com/blog/10-challenges-securing-iot-communications-iot-security/

3) Exam Questions

1. Which of the following service provider provides the least amount of built in security ?

a) SaaS

b) PaaS

c) IaaS

d) All of the mentioned

Answer: c

Explanation: You get the least amount of built in security with an Infrastructure as a Service provider, and the most with a Software as a Service provider.

2. Point out the correct statement:

a) Different types of cloud computing service models provide different levels of security services

b) Adapting your on-premises systems to a cloud model requires that you determine what security mechanisms are required and mapping those to controls that exist in your chosen cloud service provider

c) Data should be transferred and stored in an encrypted format for security purpose

d) All of the mentioned

Answer: d

Explanation: When you identify missing security elements in the cloud, you can use mapping to work to close the gap.

4. The following flowchart is intended to evaluate _____ in any cloud.

cloud-computing-questions-answers-cloud-security-q4

a) risk

b) errors

c) inconsistencies

d) none of the mentioned

Answer: a

Explanation: Your risks in any cloud deployment are dependent upon the particular cloud service model chosen and the type of cloud on which you deploy your applications.

6. Which of the following area of cloud computing is uniquely troublesome ?

a) Auditing

b) Data integrity

c) e-Discovery for legal compliance

d) All of the mentioned

Answer: d

Explanation: Storing data in the cloud is of particular concern.

7. Using virtualization, we can make one server appear to be many, a desktop computer appears to be running multiple operating systems simultaneously, a network connection appear to exist, or a vast amount of disk space or a vast number of drives to be available. → True

8. Common cloud deployment models include:
A. Community clouds
B. Private clouds
C. Public clouds
D. Hybrid clouds
E. All of the above → E. All of the above

9. Which of these is not a major type of cloud computing usage?

A. Hardware as a Service

B. Platform as a Service

C. Software as a Service

D. Infrastructure as a Service

Answer: A

10. What is the name of the organization helping to foster security standards for cloud computing?

A. Cloud Security Standards Working Group

B. Cloud Security Alliance

C. Cloud Security WatchDog

D. Security in the Cloud Alliance

Answer: B

11. Virtual Machine Ware (VMware) is an example of

A. Infrastructure Service

B. Platform Service

C. Software Service

Answer: A

12. Amazon Web Services is which type of cloud computing distribution model?

A. Software as a Service

B. Platform as a Service

C. Infrastructure as a Service

Answer: C

13. Which of the following is true of cloud computing?

A. It's always going to be less expensive and more secure than local computing.

B. You can access your data from any computer in the world, as long as you have an Internet connection.

C. Only a few small companies are investing in the technology, making it a risky venture.

Answer: B

14. Google Docs is a type of cloud computing.

A. True

B. False

Answer: A

15 This is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

A. Platform as a Service (PaaS)

B. Infrastructure as a Service (IaaS)

C. Software as a Service (SaaS).

Answer: C

16. _____ empowers IoT by bringing together everyday objects.
a) Intelligence
b) Connectivity
c) Dynamic Nature
d) Enormous Scale

Answer: b
Explanation: Connectivity empowers IoT by bringing together everyday objects. Connectivity of these objects is pivotal because simple object level interactions contribute towards collective intelligence in IoT network.

17. _____ in IoT as one of the key characteristics, devices have different hardware platforms and networks.
a) Sensors
b) Heterogeneity

c) Security
d) Connectivity

Answer: b
Explanation: Heterogeneity in IoT as one of the key characteristics, devices have different hardware platforms and networks. And can interact with other devices or services platforms through different networks.

18. IoT devices are naturally vulnerable to _____ threats.
a) Sensors
b) Heterogeneity
c) Security
d) Connectivity

Answer: c
Explanation: IoT devices are naturally vulnerable to security threats. There is a high level of transparency and privacy issues with IoT.

19. Which of the following issues are considered in IoT?
a) Security Issue
b) Reliability Issue
c) Standard Issue
d) All issues

Answer: d
Explanation: We should be very careful while building IoT as it has the following issues:
Security Issue
Reliability Issue
Standard Issue.

2-6. Policy and Law ComplianceError! Bookmark not defined.

1) Lectures

The law is a top-level requirement that an organization or individual must adhere to, and the state enacts information security laws that organizations and individuals must adhere to. Canada has enacted and implemented a variety of information security laws at federal and state levels.

A policy is an official statement that outlines the principles, direction, and intent of a control over the organization's services, actions, and ways in which it conducts its mission. An information security policy is an organization's position on important decisions or issues, decides on a specific action plan, and decides how the members of the organization should act. Policies may include Code of Conduct.

Procedures describe a step-by-step process for the set of actions, processes, and responsibilities required to achieve a specific policy goal. Procedures describe how an organization performs its expected performance and behavior in order to effectively perform its functions and are designed to specifically enforce the provisions required by law or policy.

The guidelines determine the laws that an organization must perform, and the precise way in which the university operates its policies. The guidelines describe the details necessary to carry out the procedures of the organization and provide various best practices for users to refer to as necessary. Guidelines aim to rationalize business processes and ensure the security quality of the organization in accordance with the requirements of the expected practices. Guidelines are generally presented in the form of recommendations.

In Canada, important information security laws at the federal level include the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Information Protection Act (PIPA). While the FIPPA is a law for the public sector the PIPA is a law for the private sector.

- **FIPPA** is to establish an individual's right to access records in the custody or control of a Public Body, including access to one's own Personal Information.
- **PIPA** is to govern the collection, use and disclosure of personal information in private sectors.

In addition, there are laws related to information security.

- **Copyright Act** protects original literary, artistic, musical and dramatic works, including software.
- **Canadian Patent Act** protects certain new, useful and inventions, giving the owner of the Canadian patent the exclusive right to use his works.

In particular, engineering students who are interested in information security or who are looking for information security related jobs in the future should be aware of information security laws and policies.

As an organization, UVic has established and implemented information security policies: Information Security Policy and Information Security Policy. Information Security Policy define authorities, responsibilities, and accountabilities for information resources and information systems security and has associated procedures and guidelines as the followings:

- Procedures for Responding to an Information Security Incident

- Procedures for Addressing Security Vulnerabilities of University Electronic Information Resources and Information Systems
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device Payment Card Acceptance Procedures
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Protection of Privacy Policy articulates how the university complies with privacy components of the Freedom of Information and Protection of Privacy Act (FIPPA) and associated procedures as the followings:

- Procedures for Responding to a Privacy Incident or Privacy Breach
- Procedures for the Management of University Surveillance Systems
- Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
- Procedures for the Management of Personal Information
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device

When UVic students work part-time in school, they must observe and adhere to the school's information security policies, procedures and guidelines when using the university's equipment in the school's laboratory. If students ignore information security policies, procedures, and guidelines, they can cause intentional or unintended security problems. Therefore, students must be familiar with information security related policies, procedures, and guidelines before beginning the new work on campus.

2) Additional Materials

a) Videos

Title	Links
Cybersecurity Policies, Standards, Procedures	https://youtu.be/5DIxmz0k0PU
Privacy Legislation in Canada	https://youtu.be/Cx4g7eX3Fv4

b) Additional Notes

Title	Description
UVic Information Security Policy	UVic Information Security Policy(Procedures)

3) Exam Questions

1. GDPR is designed to help people protect and control use of their "personal data". But what does that cover?

a) Your name, email address, date of birth and passport number - but nothing else

b) All the above plus your bank details, social network posts, medical information and computer IP address - but nothing else

c) All of the above and, under some circumstances, images of your face and information about your relatives among other data

Answer: C

2 FIPPA is to establish an individual's right to access records in the custody or control of a Public Body, including access to one's own Personal Information.

Answer: True

3. PIPA is to govern the collection, use and disclosure of personal information in private sectors.

Answer: True

4. UVic has established and implemented information security policies including:

a) Procedures for Responding to an Information Security Incident

b) Procedures for Addressing Security Vulnerabilities of University Electronic Information Resources and Information Systems

c) University Information Security Classification Procedures

d) Procedures for Responding to the Loss or Theft of a Mobile Computing Device Payment Card Acceptance Procedures

e) Guidelines for the Secure Destruction and Deletion of University Records and Information

f) All of the above

Answer: f

2-7. Authentication

1) Lectures

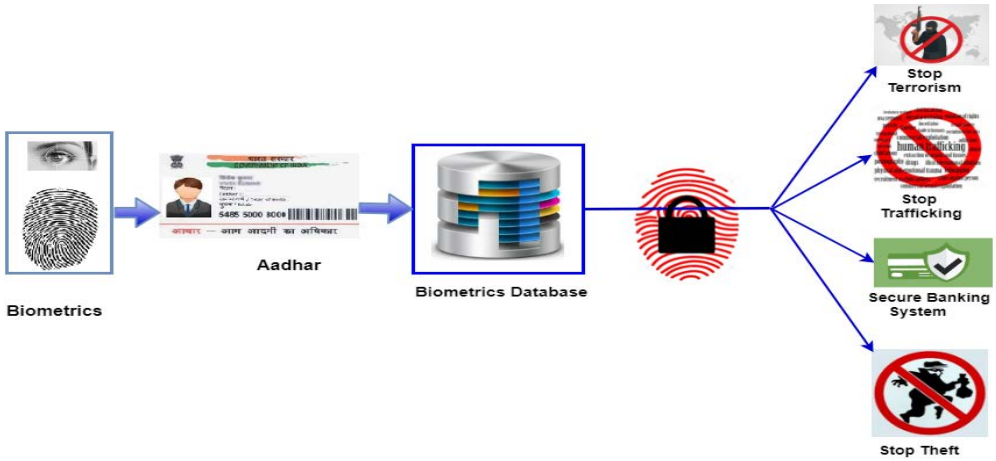
Passwords are the most important part of authentication systems. Complex and long passwords enforce attackers to spend so much time and effort, then cause to give up their intent. We should keep passwords between 10 and 32 characters long along with using characters in different character sets.

Type	No. of characters	Character sets	Examples
Short	10-15	3 or more sets	Ex@shorTest
Intermediate	16-19	2 or more sets	ShortJustTwoSets
Easy to type	20-32	1 set (or more)	examplelongerbuteasy

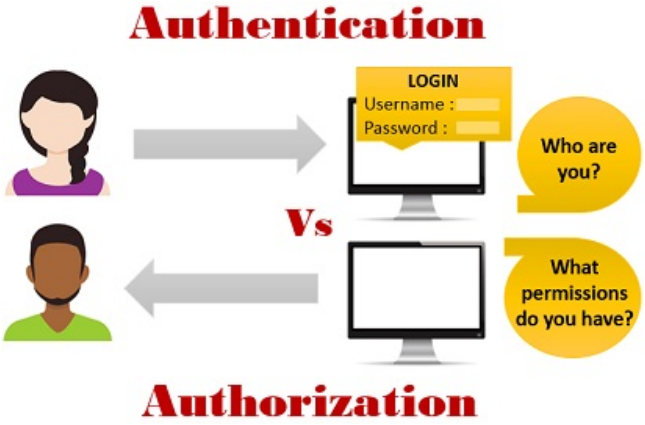
The following picture [11] is very interesting comparing online security practises of non-experts and experts. It seems that ordinary people need to upgrade their some habits to become more safety.

Two factor authentication means your account can only be opened if you supply something you know with something you have or something you are. Online accounts almost always start with a password. Your password is something you know. Your phone is something you have since everyone always has their phone. The second factor does not have to be a number. It is also possible to set up two factor authentication with something you are: your fingerprint, facial recognition, retina or iris scans, etc.

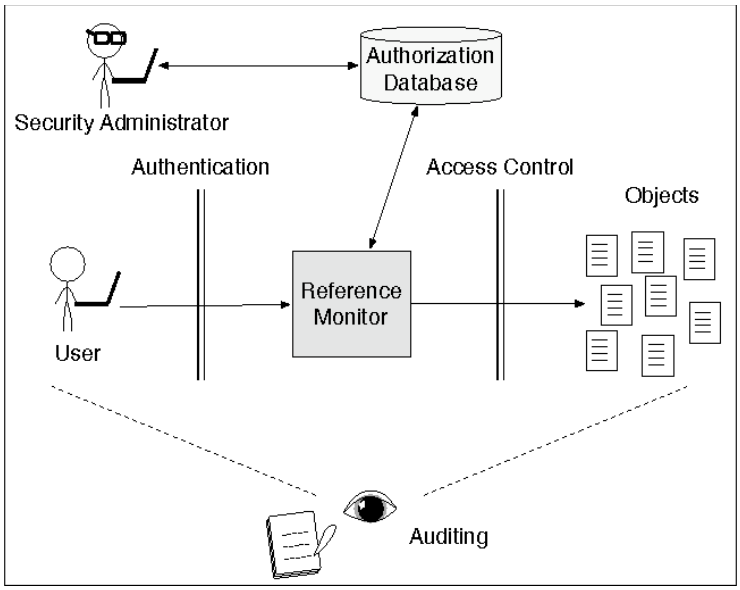
For example, Biometrics information can be used for identification by matching against database. There are many vital areas utilizing this information in the first place.



The authentication and authorization are interchangeably used but are distinct. The identity of a person is assured by authentication. On the other hand, the authorization includes the permissions that a person has given [12]



Lastly, you can see the whole architecture of Access Control (AC). Actually, there are 2 types of AC: logical and physical. Logical AC systems perform identification, authentication and authorization of users. A widely used AC system is role-based AC that restricts access to computer resources based on individuals or groups (roles). The audit process gathers data about activity in the system and analyze it to discover security violations or diagnose their cause.



2) Additional Materials

a) Videos

Title	Links
Password Security Awareness Video	https://www.youtube.com/watch?v=VqEMlofu47k
Be Smart with Passwords (Security Awareness Video)	https://www.youtube.com/watch?v=Mc7simZ_aqU

b) Additional Notes

Title	Description
Everything with Authentication	https://searchsecurity.techtarget.com/definition/authentication
This is How Hackers Crack Passwords	https://www.youtube.com/watch?v=YiRPt4vrSSw
Edward Snowden on secure passwords	https://www.youtube.com/watch?v=SuaNGOx4ZSc

2-8. Security Awareness

This course does not have slides since it has large scope. The purpose is here to review all other courses and learn about related popular internet tutorials. We believe that knowing about mindset of security make learning all other courses easier and meaningful. At the end, cybersecurity is only human security that we need to increase our awareness in different ways.

1) Security Awareness

The purpose of this section is all about having a quick review of the other courses. The videos in this section only focus on some significant areas of security that we need to know in our daily life.

a) Security Awareness Videos

Title	Links
Why is Information Security important?	https://www.youtube.com/watch?v=7L9JerWIT3Y
Pause, Think and Act	https://www.youtube.com/watch?v=o_58rBduAqQ
Phishing awareness training	https://www.youtube.com/watch?v=-0Ql6xnNj7g
Stay Safe from Phishing and Scams	https://www.youtube.com/watch?v=R12_y2BhKbE
Phishing and Spear Phishing	https://www.youtube.com/watch?v=ygON2B9-xTw
How attackers track you online?	https://www.youtube.com/watch?v=4afJOlYNbBc
Credit Card Security Awareness	https://www.youtube.com/watch?v=A6OTQGp7a10
Advanced Persistent Threats	https://www.youtube.com/watch?v=Gin4PUi0wYc
Security Awareness 7 Tips	https://www.youtube.com/watch?v=i0iLy8racHI

2) Additional Materials

The purpose of this section is to introduce you some important people, websites, courses, channels along with their ideas. We are sure that you will be fond of some of those and continue to follow for a long time.

a) Additional Notes

Title	Description
Cyberthreat Real-Time Map	https://cybermap.kaspersky.com/tr
Worlds biggest data breaches hacks	https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Security Weekly	https://securityweekly.com
Weekly Update	https://www.troyhunt.com/
Cyber Security News Podcast	https://www.youtube.com/channel/UCIOrawT0QyfjAUeVTQg9bew

b) Youtube Channels&Videos

Title	Description
What Is SecureNinjaTV?	https://www.youtube.com/watch?v=dnRVXZeuJNg
Hashtag Awareness	https://www.youtube.com/watch?v=6QQ7tgg58m8
Sophos Videos	https://www.youtube.com/user/SophosLabs
Bruce Schneier: The Security Mindset	https://www.youtube.com/watch?v=eZNzMKS7zjo
Bruce Schneier on the Future of Cybercrime	https://www.youtube.com/watch?v=kUwceKE7cL8
Reconceptualizing Security	https://www.youtube.com/watch?v=CGd_M_CpeDI
How to start your career in cybersecurity?	https://www.youtube.com/watch?v=ZKXAyHFTvks
Living in a surveillance state	https://www.youtube.com/watch?v=lHj7jgQpnBM
Hackers -> curiosity, and security -> feeling	https://www.youtube.com/watch?v=HW9hH0vlPEM
How Israel Rules The World Of Cyber Security	https://www.youtube.com/watch?v=ca-C3voZwpM
Kevin Mitnick: How to Troll the FBI	https://www.youtube.com/watch?v=Nn3O8XD1z0w

3) Exam Questions

20. It is recommended to reuse your password top multiple sites to make it easier to remember.

a) True

b) False

21. Which is not included in a strong password policy?

a) Verify users can change their password.

b) Verify that user set passwords are at least 10 characters in length.

c) Verify that password change functionality requires the user's current and new password.

d) Verify password hints or knowledge-based authentication (so-called "secret questions") are present.

e) Verify that password change functionality requires the user's current and new password.

Answer: d

Explanation: Security questions are like a second password prompt. Just like passwords, users tend to create weak or easy to guess answers. Unlike passwords, security questions usually do not have policies to enforce complexity, uniqueness and guessability.

22. It is okay to share my password with

a) Nobody

b) Spouse/Partner

c) Children

d) Help Desk Staff

e) Co-workers/Friends

Explanation: a

23. Pick three passwords they are stronger than others

a) Kl@escaTest

b) Rs*d$3

c) Tb3544*V

d) longerbuteasierisgoodbelieveme

e) PickmeDOntWoRRY

Answer: a, d, e

24. Which of the following combination is the best implementation of 2 factor authentication on Internet?

a) Password Authentication + SMS Verification

b) Biometric Authentication + SMS Verification

c) Password Authentication + Push technology

d) Password Authentication + Public Key Infrastructure

e) SMS Verification + Email Verification

Answer: c

Explanation: Online accounts almost always start with a password. Push Technology are new technology implemented by Google, Microsoft, etc. It uses message-oriented

(publish&subscribe) technology implementing fully end-to-end encryption with strong key management.

25. Which statements are true?

a) Biometry is utilized mainly for identification process.

b) Firewalls are used to protect against internal users.

c) Two factor authentication is an implementation of defense in depth strategy.

d) A sniffer on the network can monitor the plaint-text data during SSH login process.

e) The main purpose of PKI is data encryption.

Answer: a,c

26. Which examples are a violation of Integrity

a) Denying access to users

b) An unencrypted CD-ROM that is stolen

c) A working program is modified

d) Messages are read

e) An unauthorized copy of software

Answer: c

27. Which examples are a violation of Availability.

a) Deleted Files

b) Unauthorized read of data

c) Messages that are modified or duplicated

d) Equipment that is stolen

e) Not working communication lines

Answer: a,d,e

28. Can you order the secure network participants from external towards internal.

a) Internet

b) Router

c) IPS/IDS

d) Firewall

e) Secure Zone

29. Which attacks below are usually utilized by using e-mails?

a) whaling

b) phishing

c) vishing

d) smishing

e) spearphishing

30. Which ones below are implemented by Digital Signature process?

a) Hash algorithms

b) Non-repudiation

c) Authentication

d) Authorization

e) Data integrity

Answer: a,b,c,e

31) Which thread actor is the least sophisticated one?

a) nation states

b) insiders

c) juveniles

d) hacktivists

e) cyber terrorists

Answer: c

32) Which statements are true?

a) IoT are not commonly designed with security and privacy in mind

b) Everything connected to the internet can be hacked.

c) Information security professionals tend to take physical security seriously.

d) Procedures describe a step-by-step process for the set of actions, processes, and responsibilities

e) As a cloud consumer, on SaaS platform, we are responsible for application security.

Answer: a,b,d

33) What is Cyberbullying?

a) Downloading cyber bullying programs and giving the computer a virus.

b) Sending, posting, or sharing negative, harmful, false, or mean content about someone else.

c) Cyberbullying is a way for advertisement media to reach its customers and ask them about internet safety problems.

d) Harassing the victim during a live chat.

Answer: b

34) What prefix indicates your communication are being encrypted during transit?

a) Http://

b) Https://

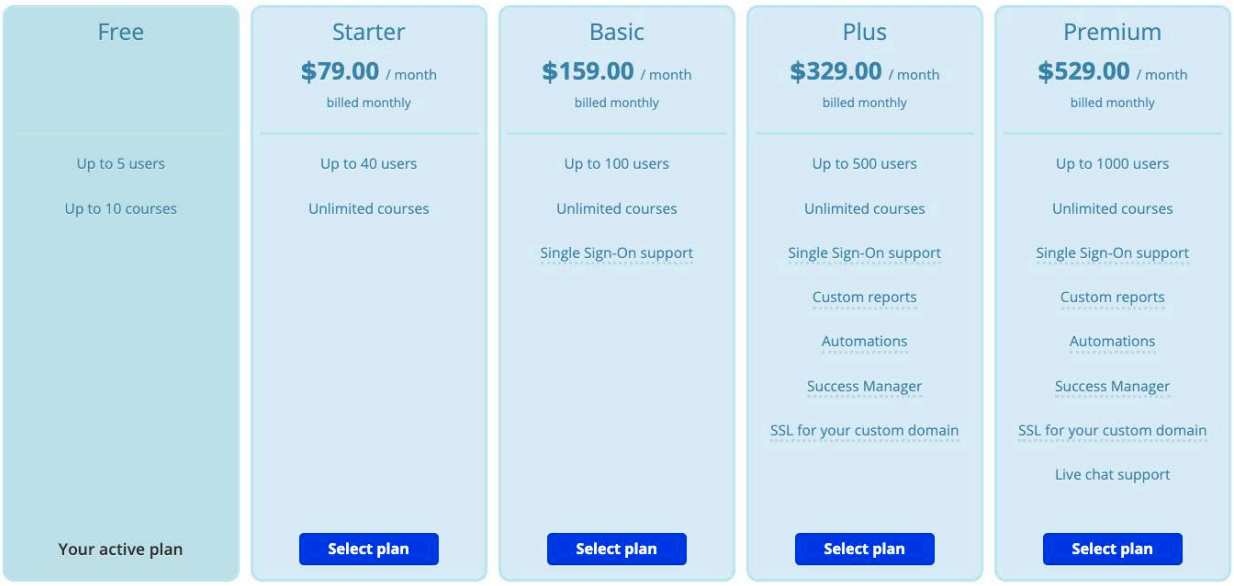
c) Ftp://

d) Tcp://

Answer: b

3. Course Website

We are using a commercial website called TalentLMS. If we would like to have up to 500 users for using this course, we have to pay US$329 per month which include SSO support, SSL for our custom domain, etc. as shown in the picture below.



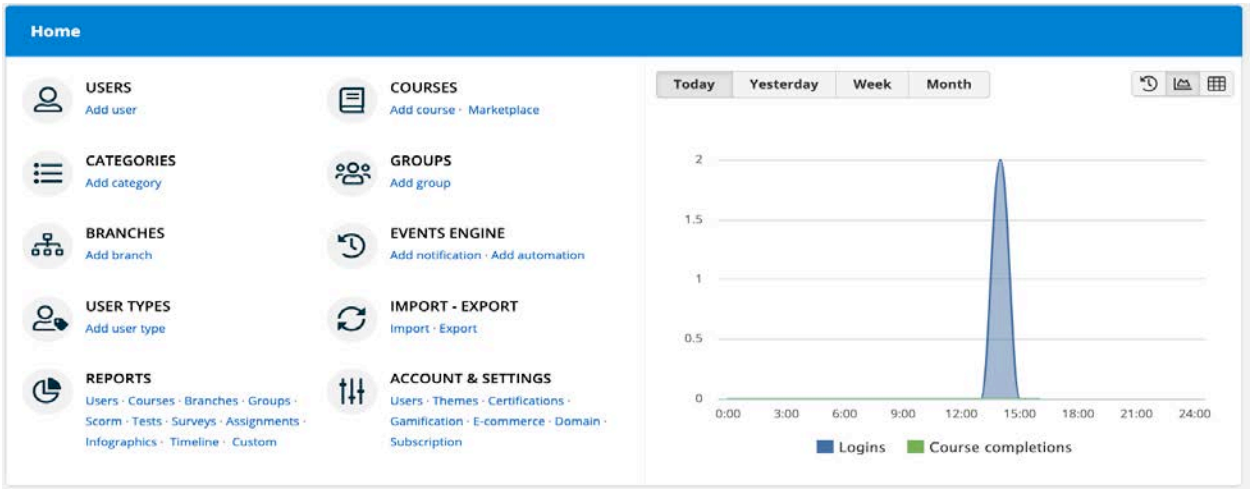
Our website link is https://cybersense.talentlms.com since we are in a free trial version; there are only five users that we can use. As shown in the table below, it is the account name and password of these five users.

User account	User password	User type
ansonleong	testing	Administrator, Instructor
t1	testing	Learner
t2	testing	Learner
t3	testing	Learner
t3	testing	Learner

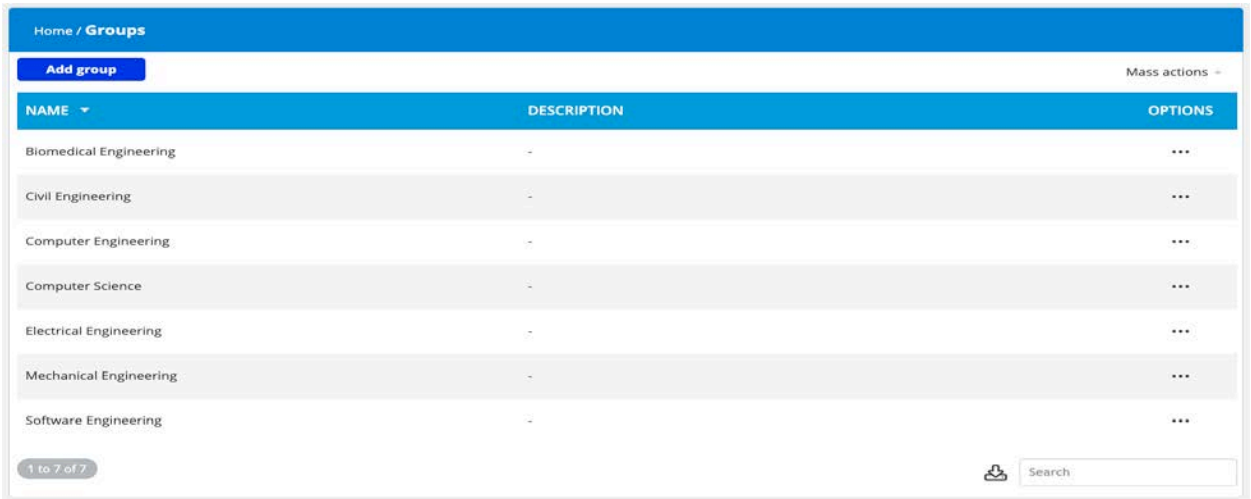
There are three different roles on this website, which is administrator, instructor, and learner.

1. Administrator

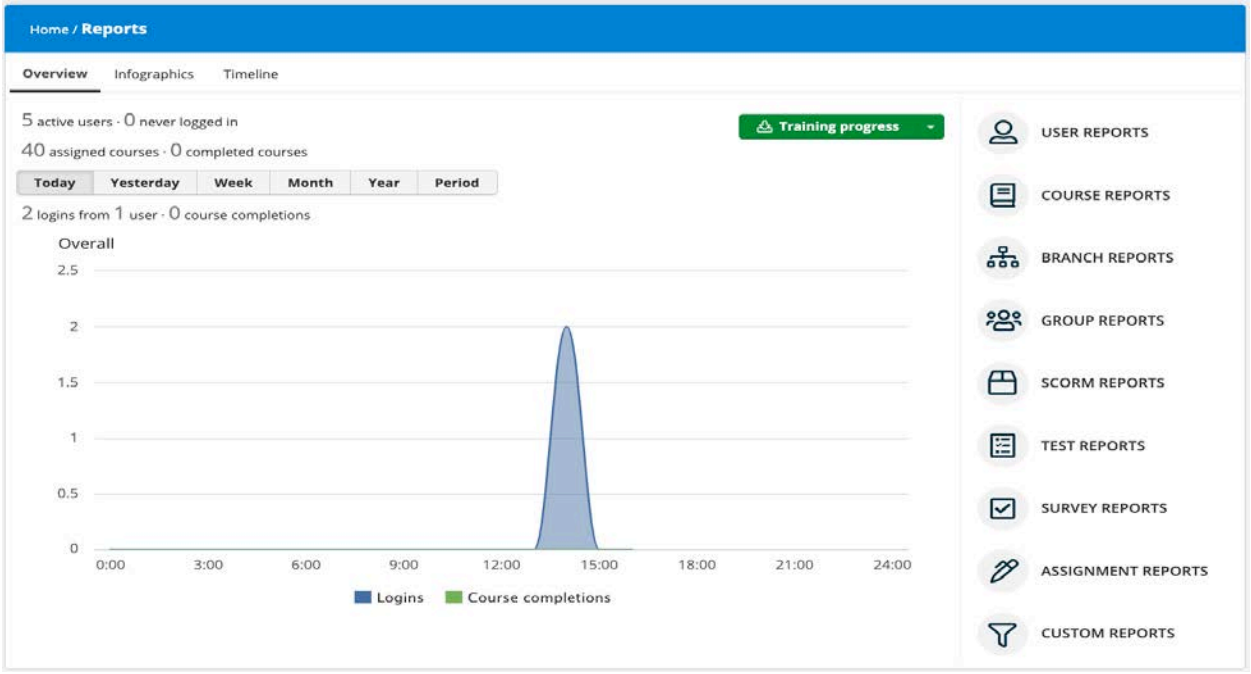
Administrator can set up all the background setting which include adding users, adding courses, having categories for courses, adding group to separate different department, adding notification, add user type, importing and exporting data for backing up, having report to see what happen of all courses, and setting up all detail of the account and background setting. As shown in the picture below, it is the home page of the administrator.



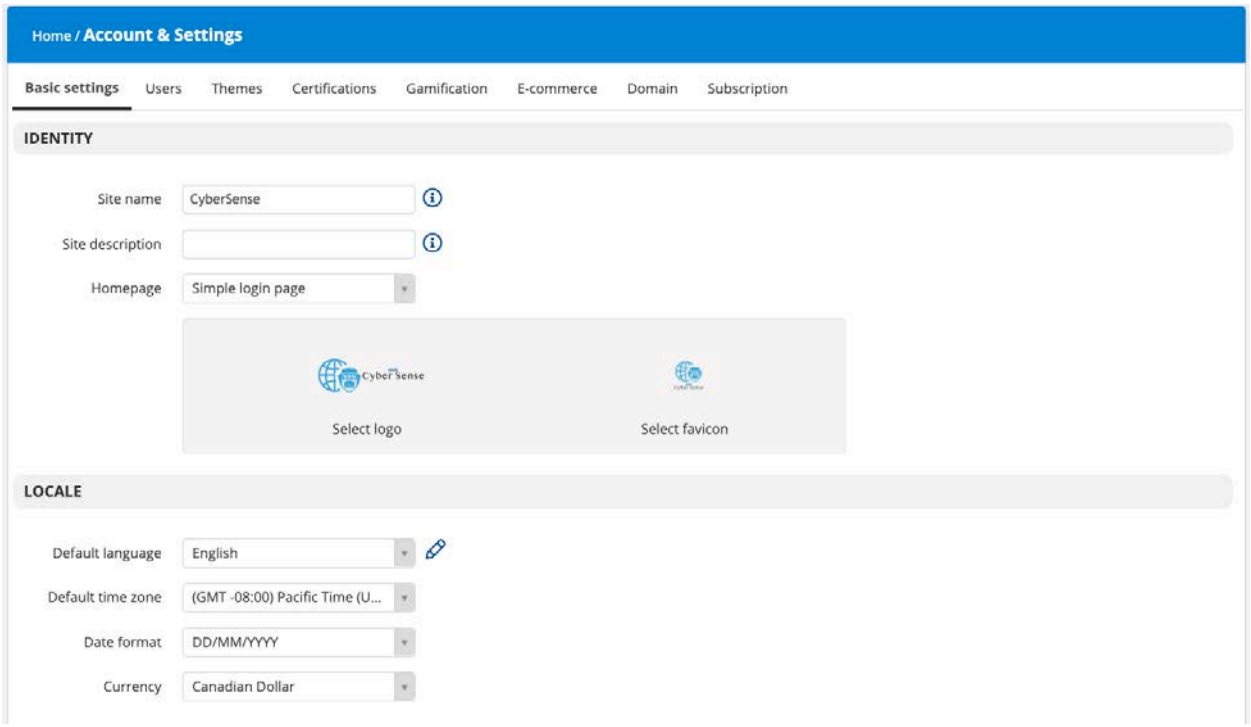
In the group, we can easily to separate different department for having proper maintenance of all engineering students.



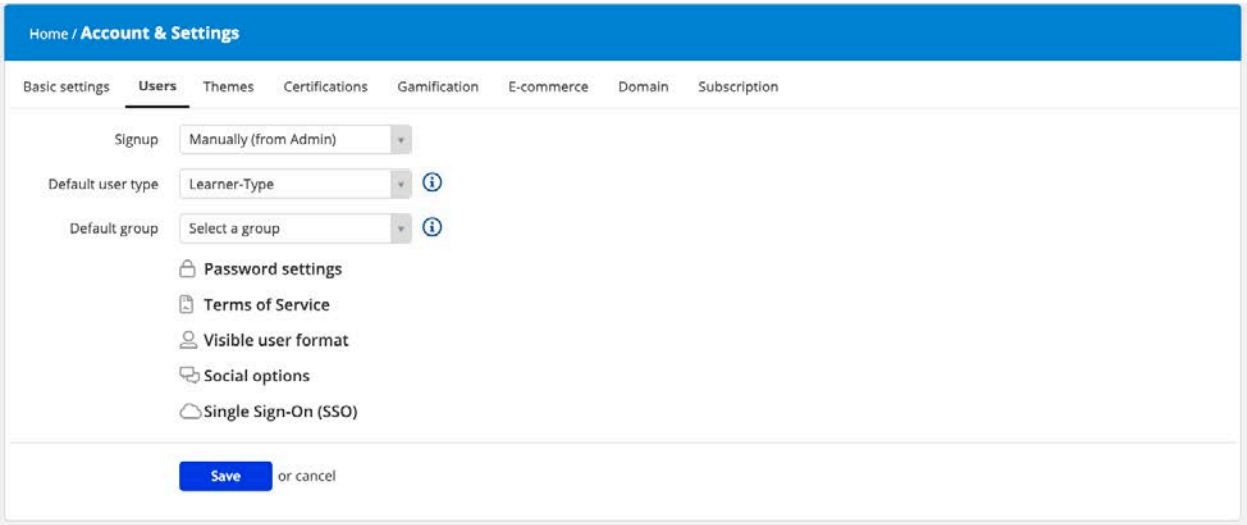
In the report part, we can see what going on about the user, course, group, test, assignment, etc.



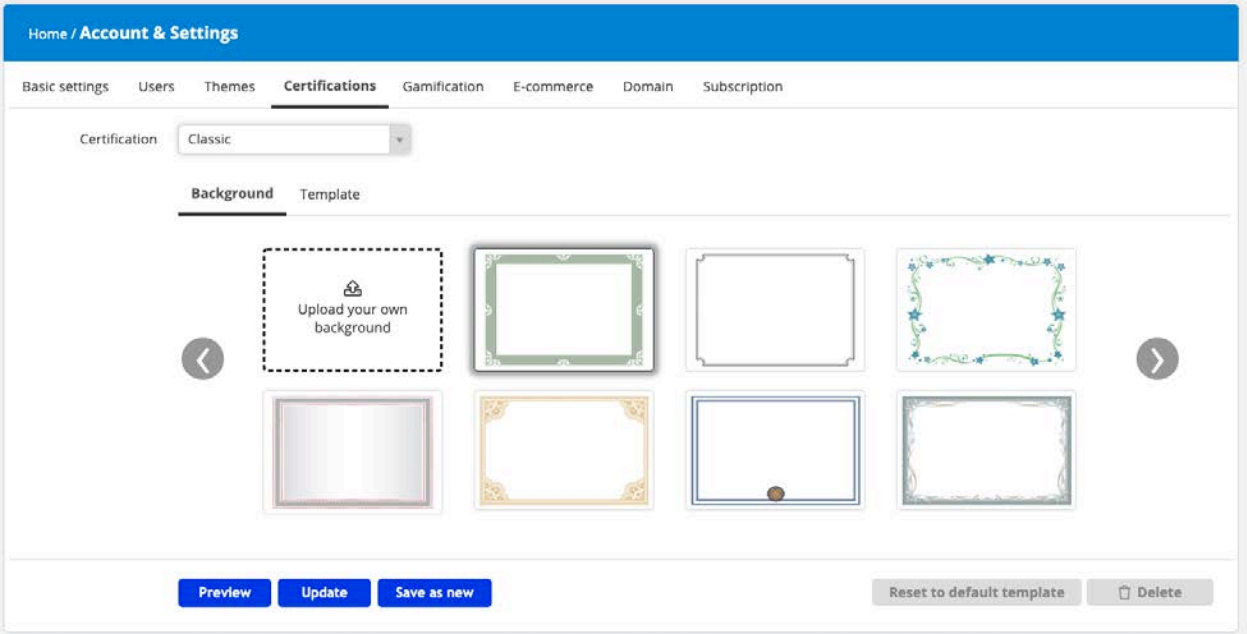
In the account & settings part, we can upload our logo, set up our site name, time zone, language, some security setting in the subpart of basic setting.



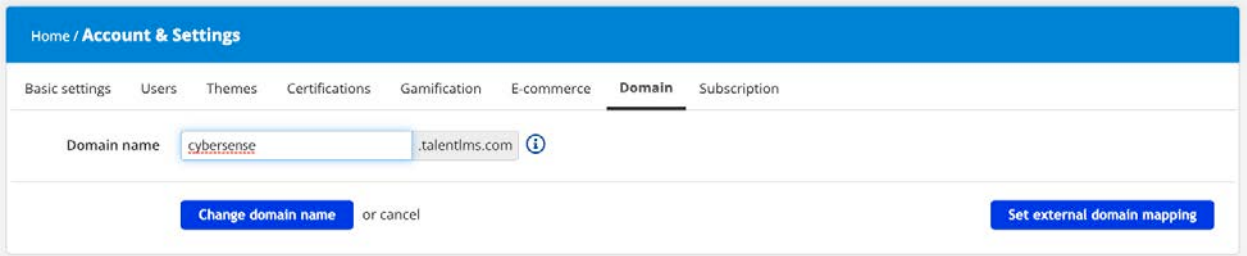
In the users part, we can set up the signup method (manually, direct, captcha, email verification), user type, group, also, password settings, terms of service, SSO, etc.



Also, we can set up the color of the course themes. Additionally, the format of the certifications, as shown in the picture below.

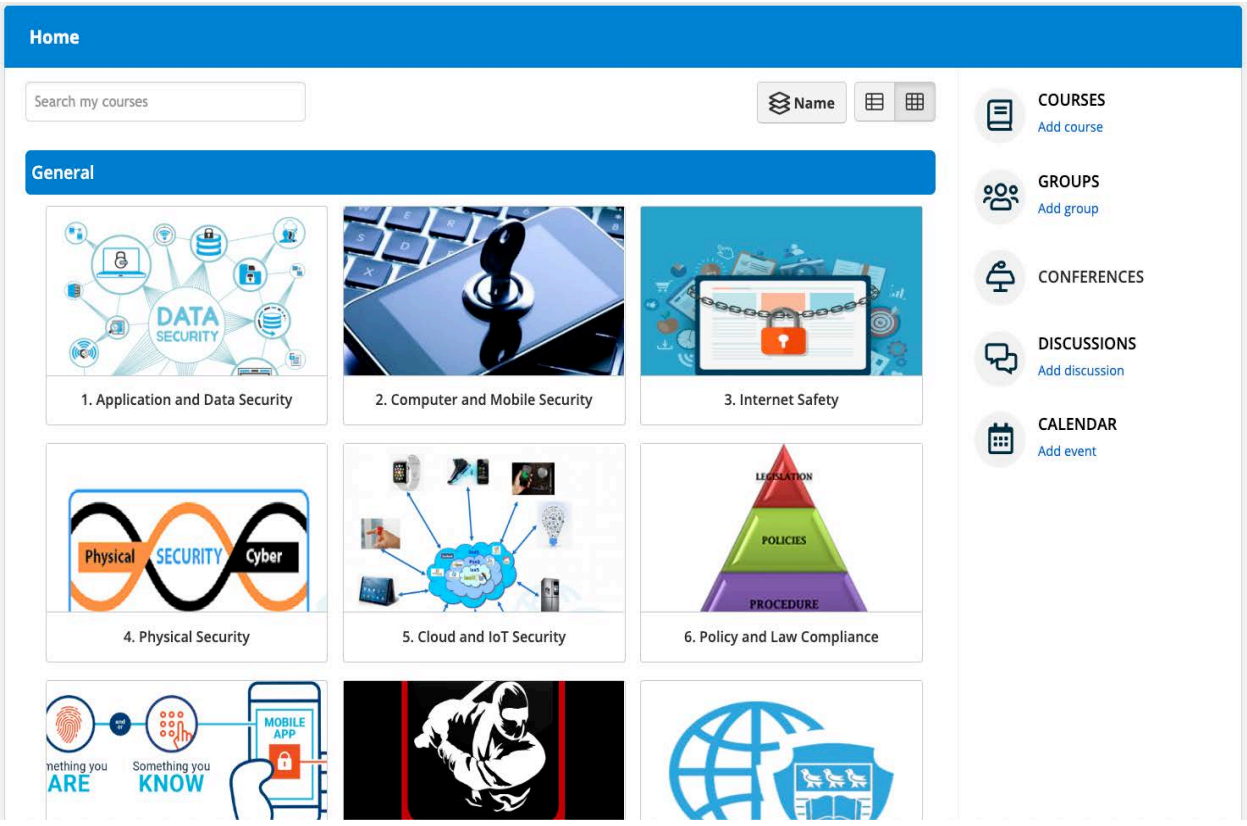


Then, the gamification and e-commerce which are not useful for our courses, therefore, we do not explain for these two parts. Finally, we also can set up our course website domain name.



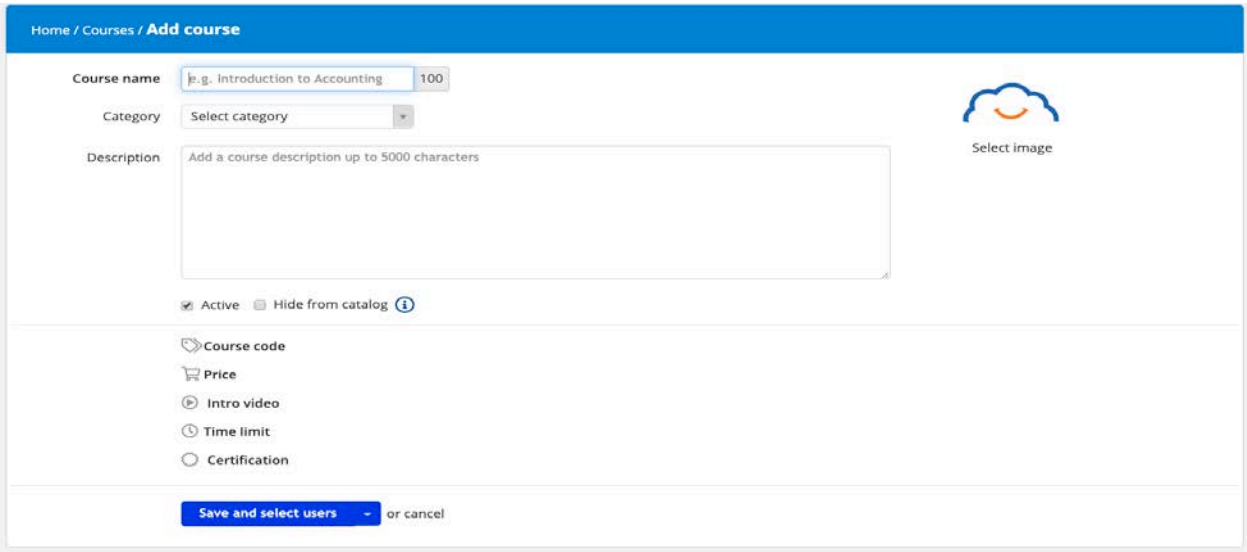
2. Instructor

As shown in the picture below, this is the home page of the instructor point of view. There are five functions that an instructor can use, which is adding courses, adding a group, having a conference, having discussions, and adding an event.

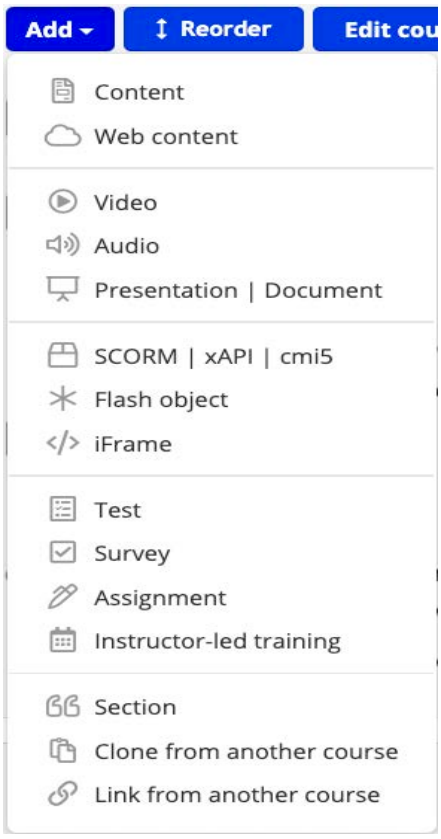


- Adding course

We can set up course code, price, certification, adding intro video, and time limit for a course.

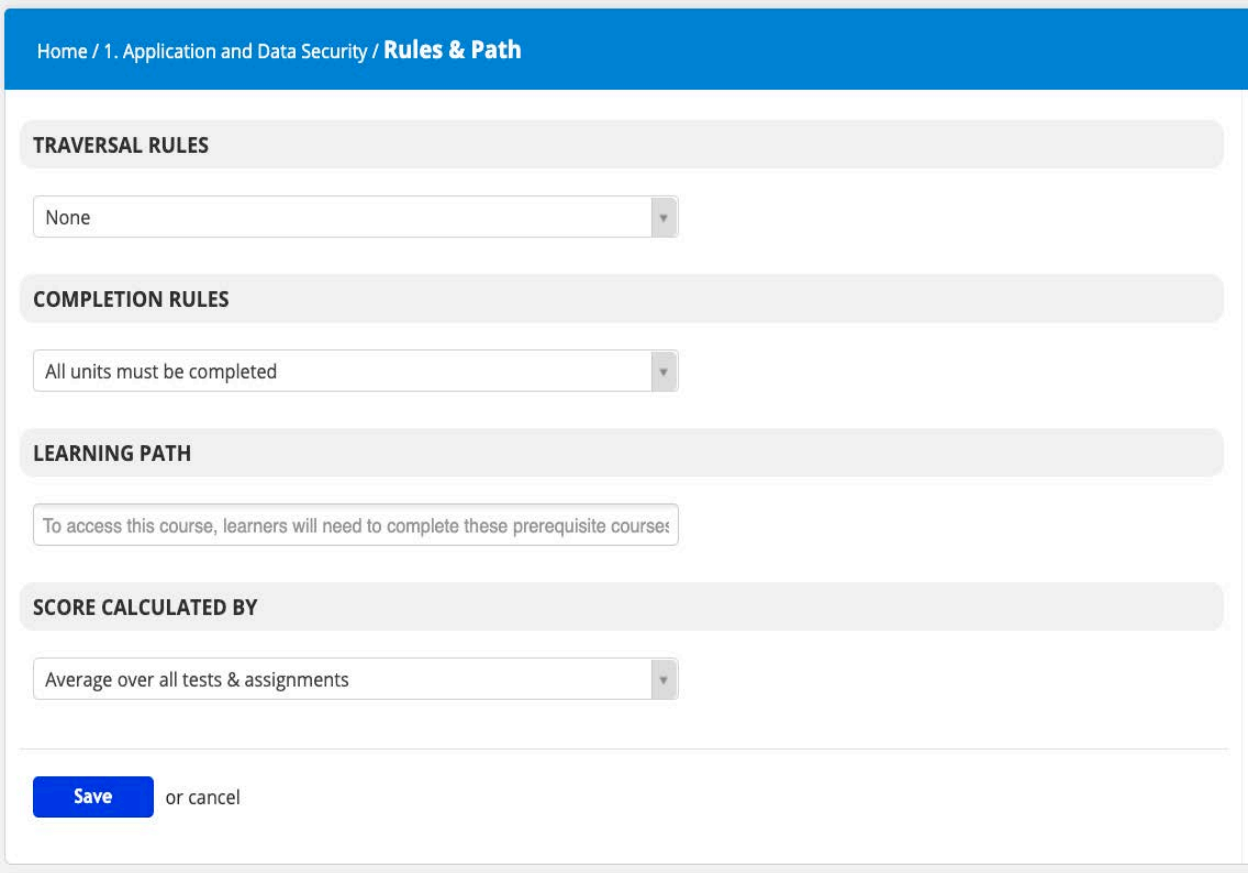


After adding a course on our website, we can add material in the course. We can add text content, web content, video, audio, PowerPoint slide, flash, iFrame, test, survey, assignment, section, etc. as shown in the picture below.

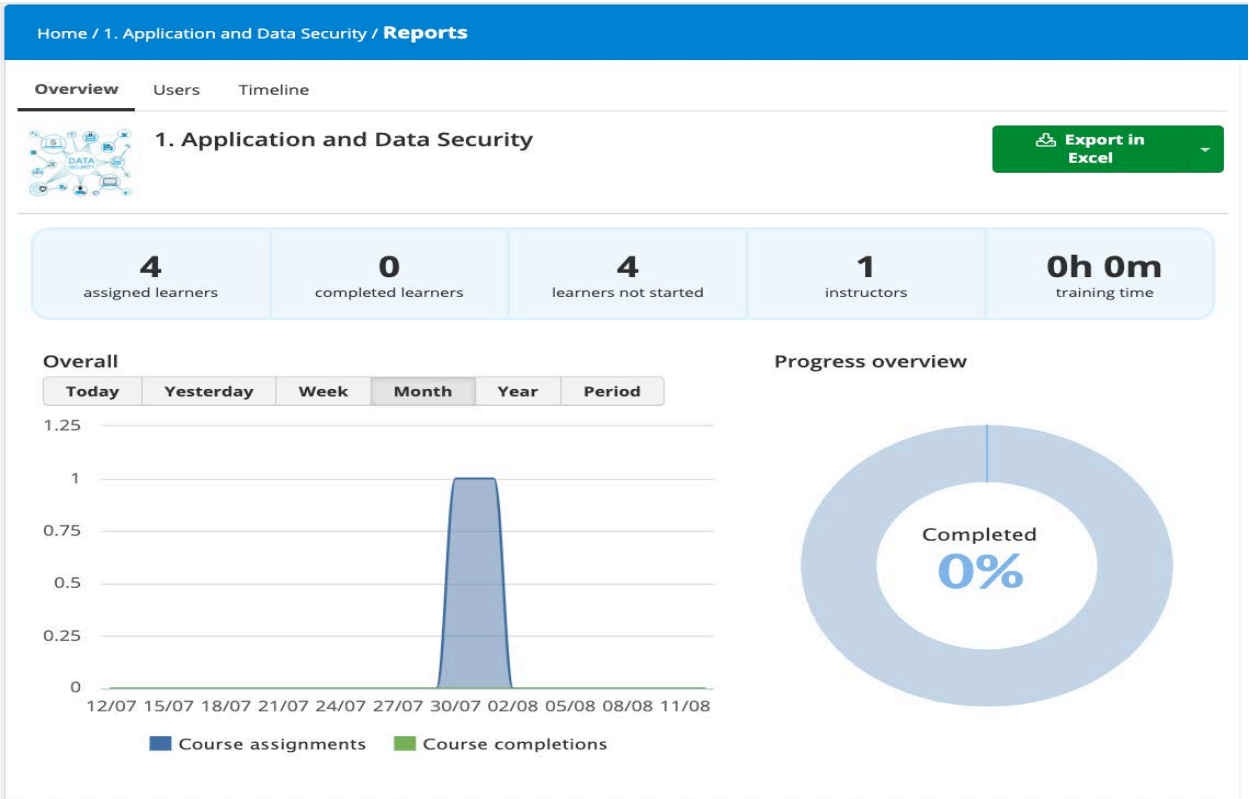


Also, we can set up the rules of a course. For example:

1. Traversal rules
   - None, or
   - Units must all be seen and completed sequentially
2. Completion rules
   - All units must be completed, or
   - Certain units must be completed, or
   - A percentage of units must be completed
3. Score calculated by
   - Average over all tests & assignments, or
   - Only tests, or
   - Specific tests & assignments

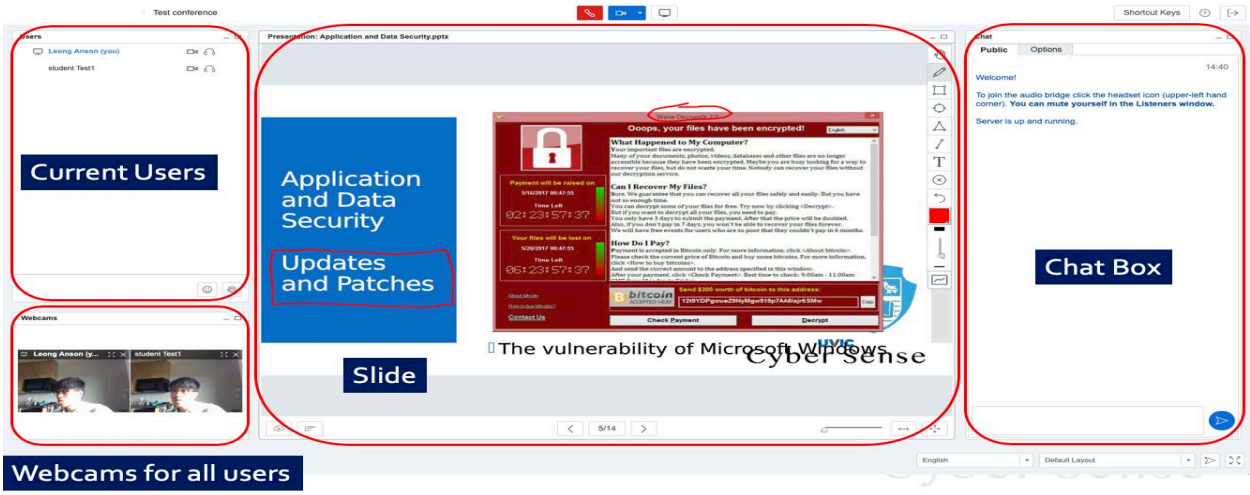


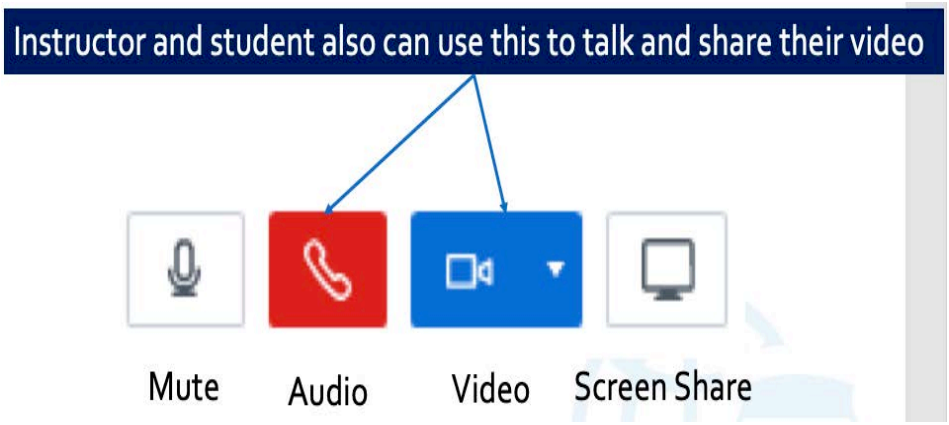
Also, the instructor can view the report, but the data is only related to the learner.



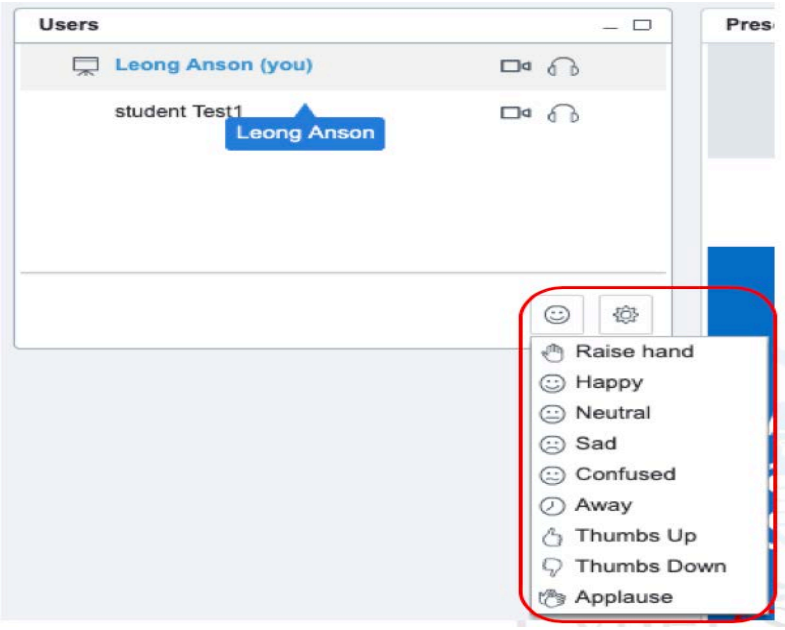
- Conferences

This function can be used for interacting with the student by using video, audio, presentation, chatbox, and poll system, as shown in the figure below. In our opinion, we do not only provide online courses. We want to let the student learn more and learn enjoyably.

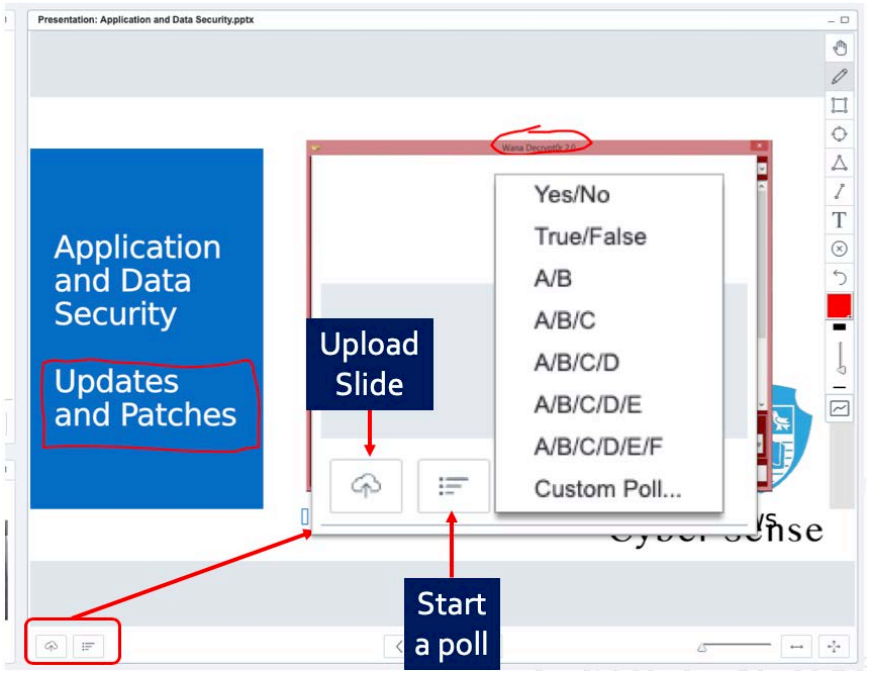




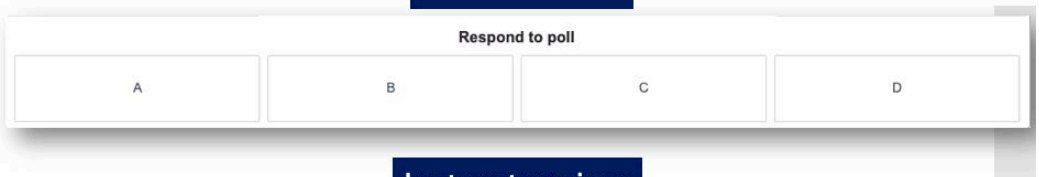
As shown in the figure below, the user can raise a hand to ask a question, also can share their feeling like happy, neural, thumbs up, and so on.



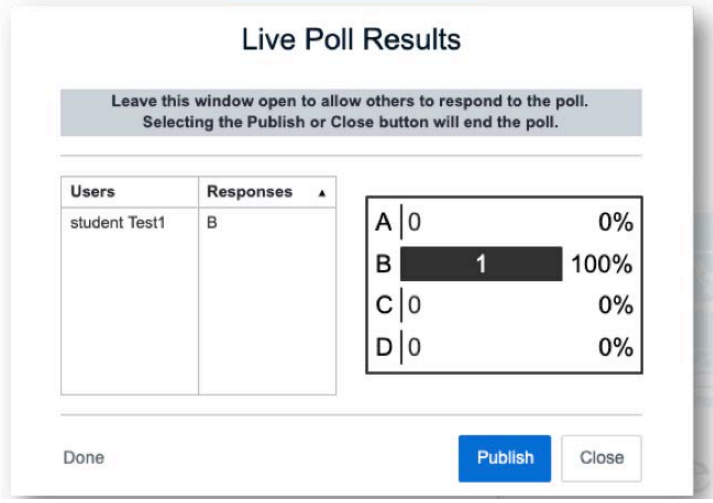
Additionally, there is an essential function which is polling. We can use this function to keep track of the student what they are learned at this moment.



Student view



Instructor view

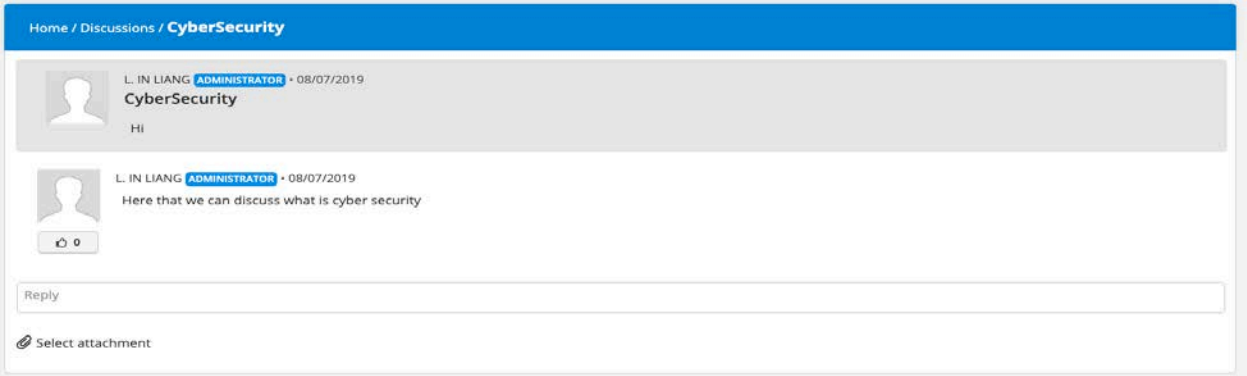


Finally, it is a video to introduce how the conference function work.

https://www.youtube.com/watch?v=kSVp82UqWtQ&feature=youtu.be

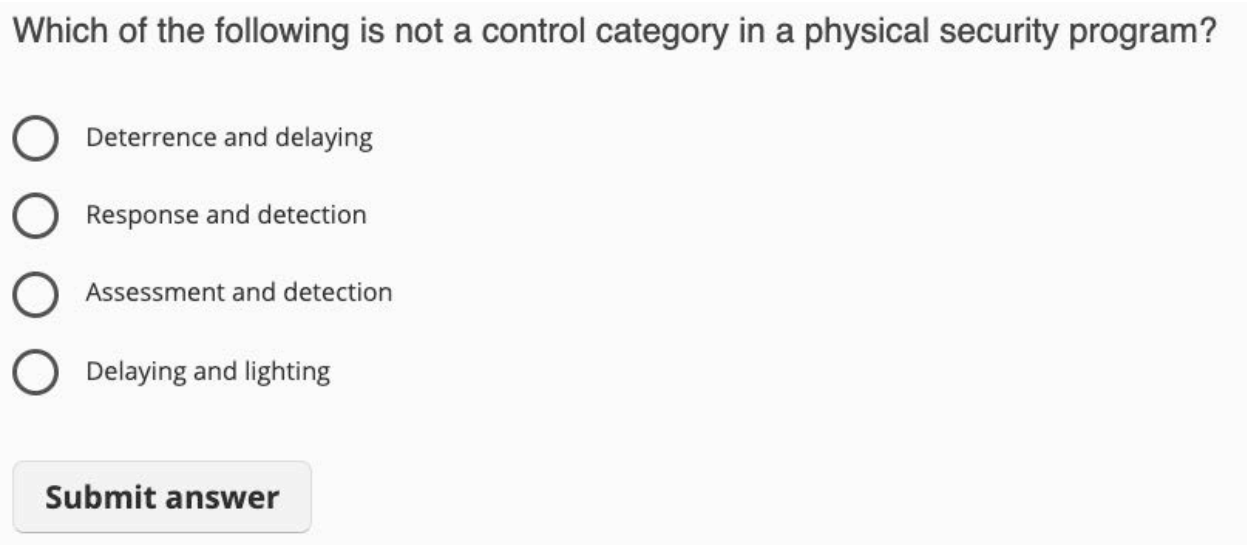
- Discussions

We can use the function of the discussion to let the student ask a question or make them discuss some topic.

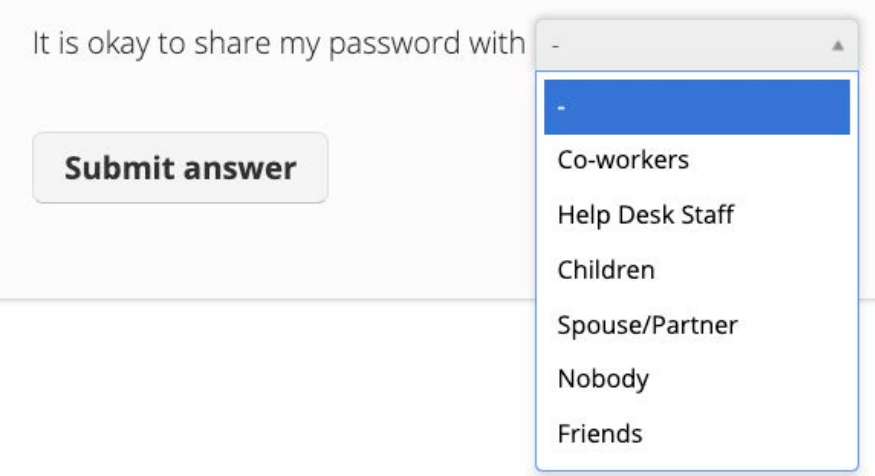


- Final Exam

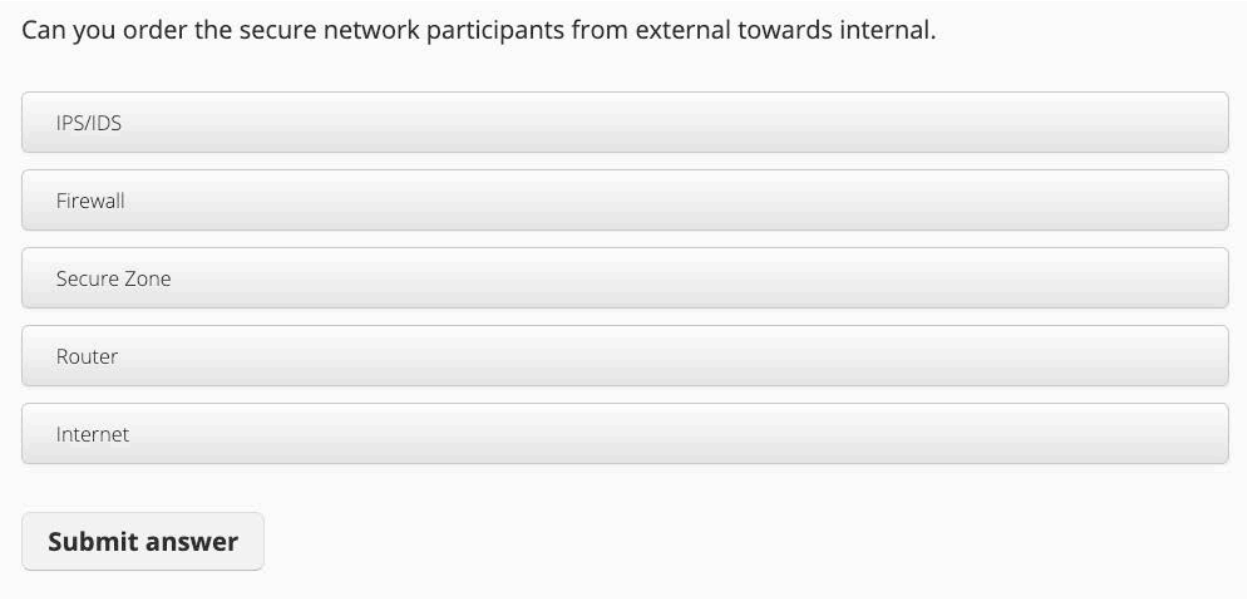
We created a question pool which includes 120 questions which related to our eight guidelines. There are six types of questions inside our question pool, for instance, multiple-choice, fill the gap, ordering, drag-and-drop, free text, and randomized. For the final exam, we randomly choose 50 questions in our pool, and we choose at least four questions on each guideline.



Example of Multiple choice

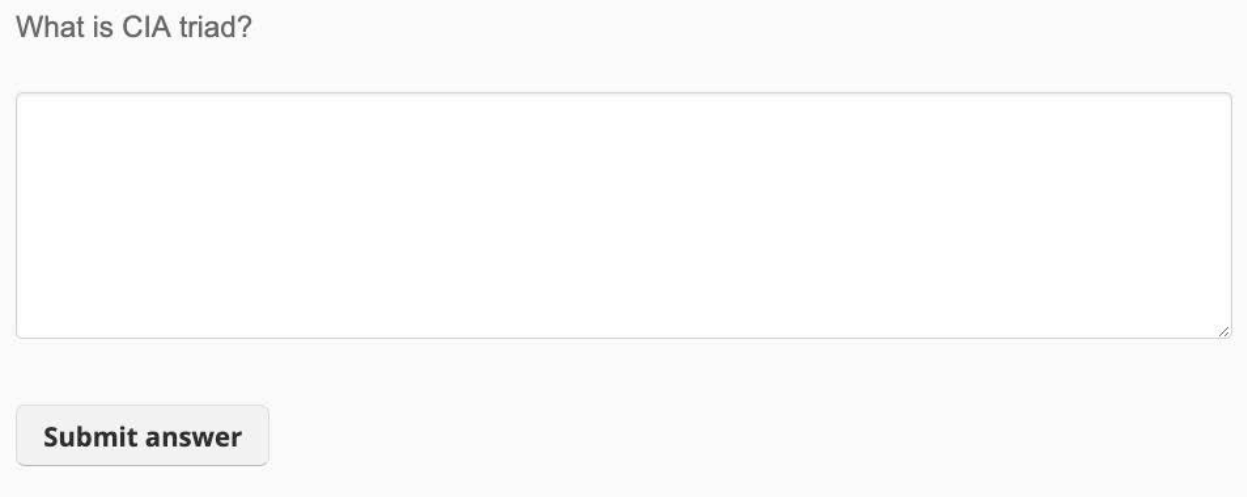


Example of Fill the gap



Example of ordering

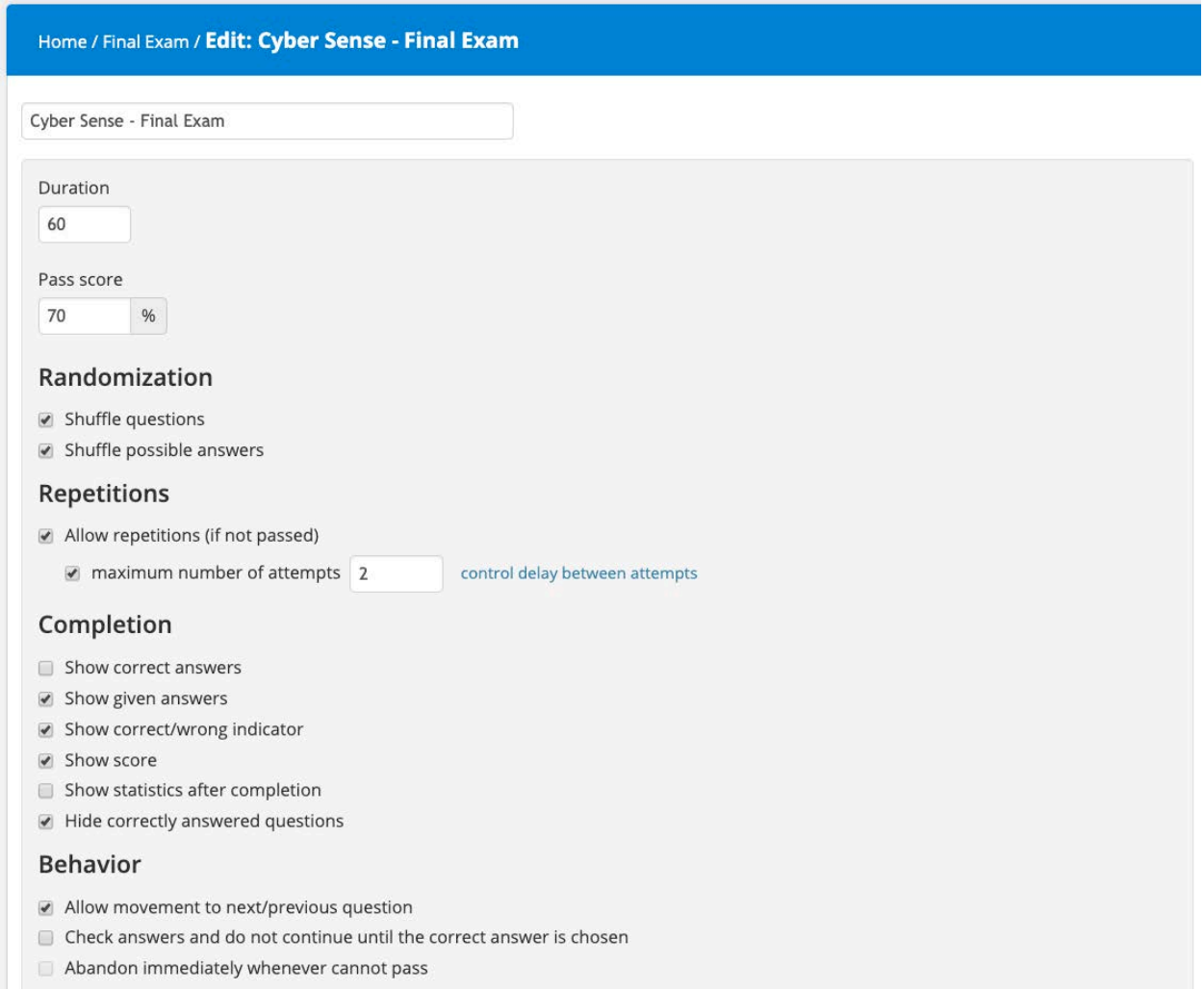
Example of drag-and-drop



Example of free text

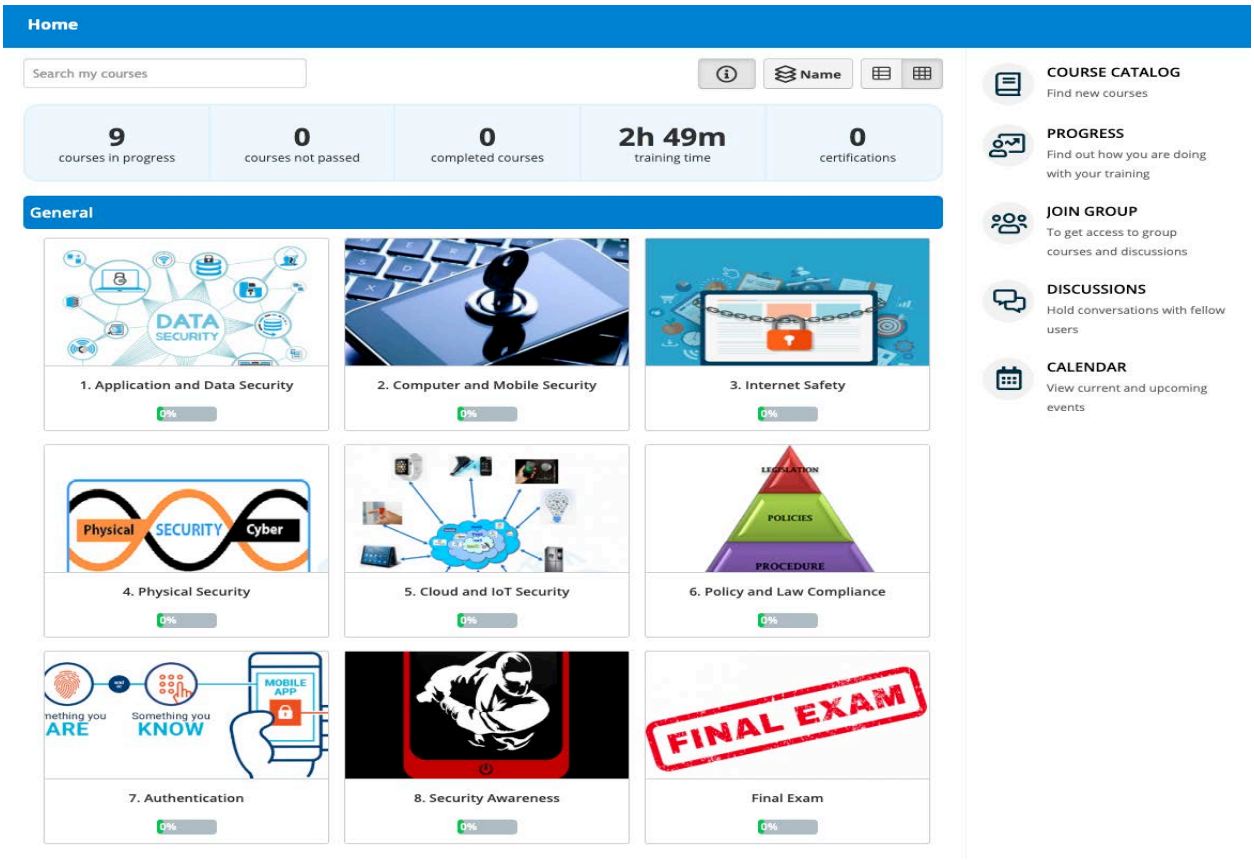
Additionally, we can set up the question weight on each of them.

In the test option, we set up the duration is 60 minutes, and the passing score is 70%. Also, shuffle questions and possible answers. There are only two attempts if the student not passed it. When they complete the exam, it will show the given answers, correct/wrong indicator, score, and hide the correctly answered questions. It is because we do not want student can know the correct answer and question, then make a screenshot and share with another classmate. As shown in the picture below is the test setting.

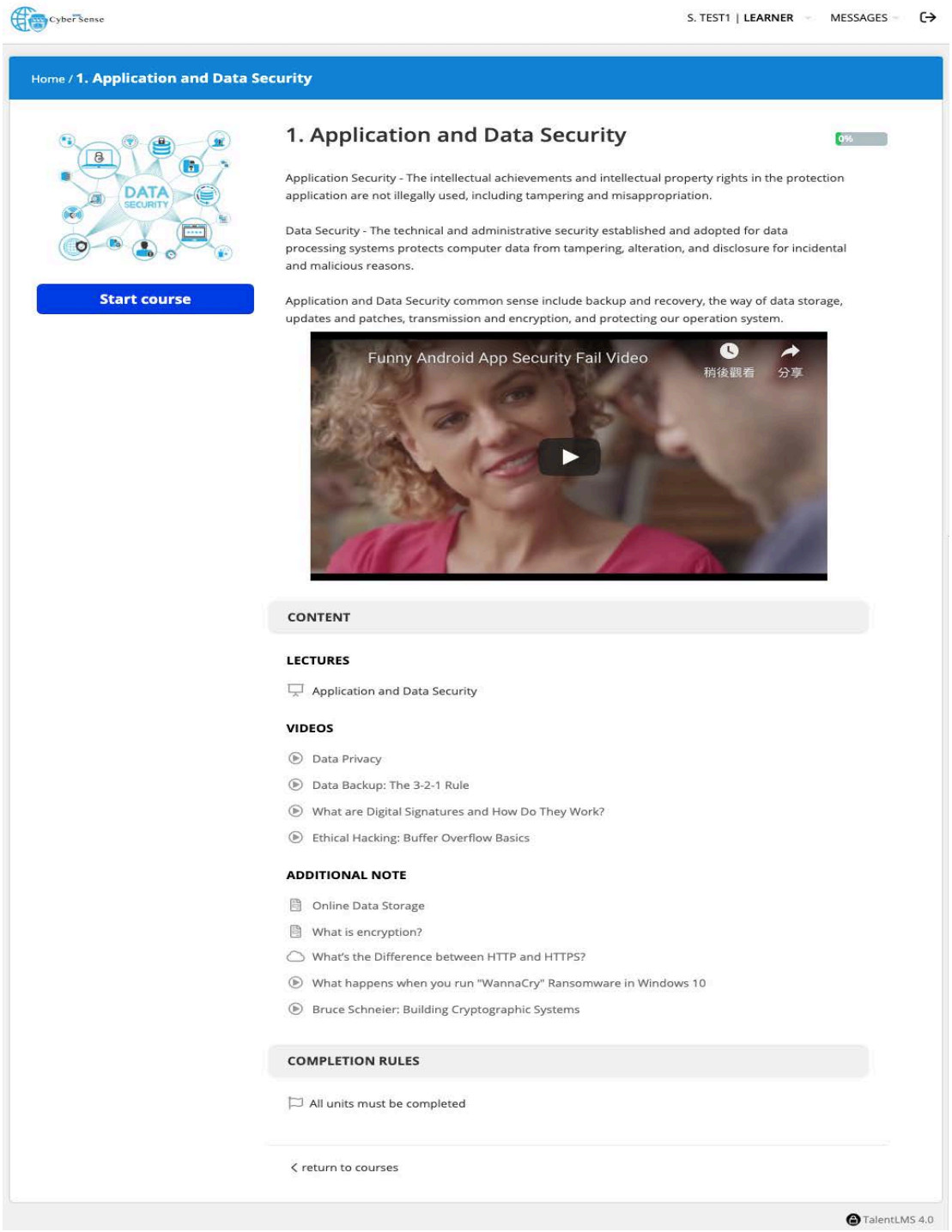


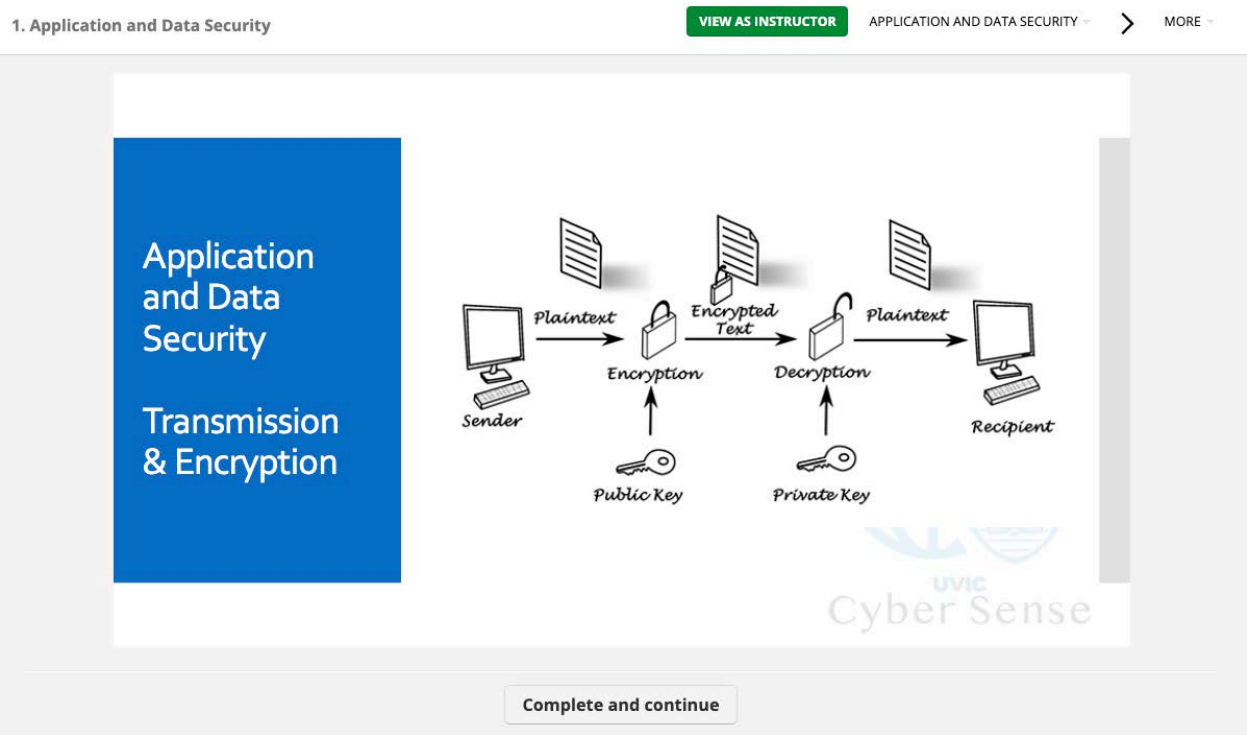
3. Learner

We will introduce the point of view of the learner. As shown in the picture below, it is the home page of the learner, which includes eight courses and one final exam.

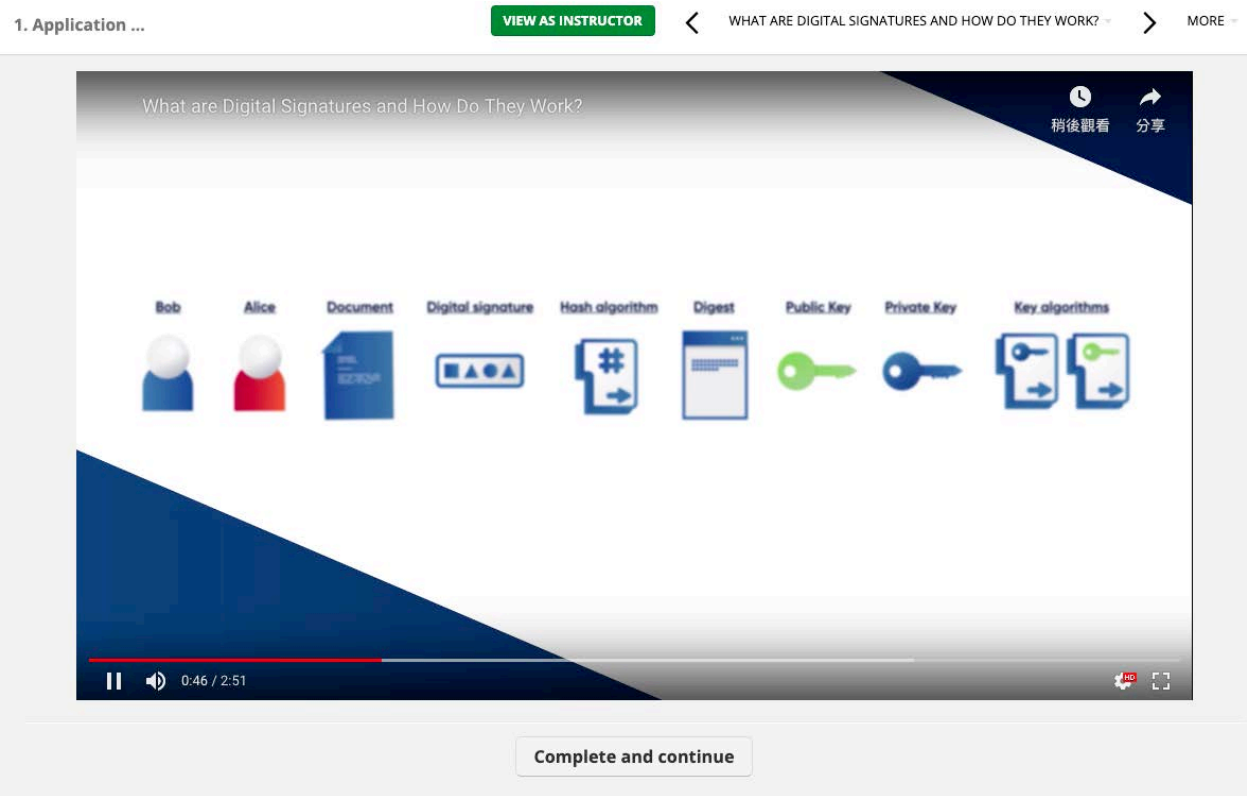


After we click one course, there is a brief introduction on the top with a funny intro video which talking about Android app security. Then, the content which includes three parts, lecture, videos, and additional note.

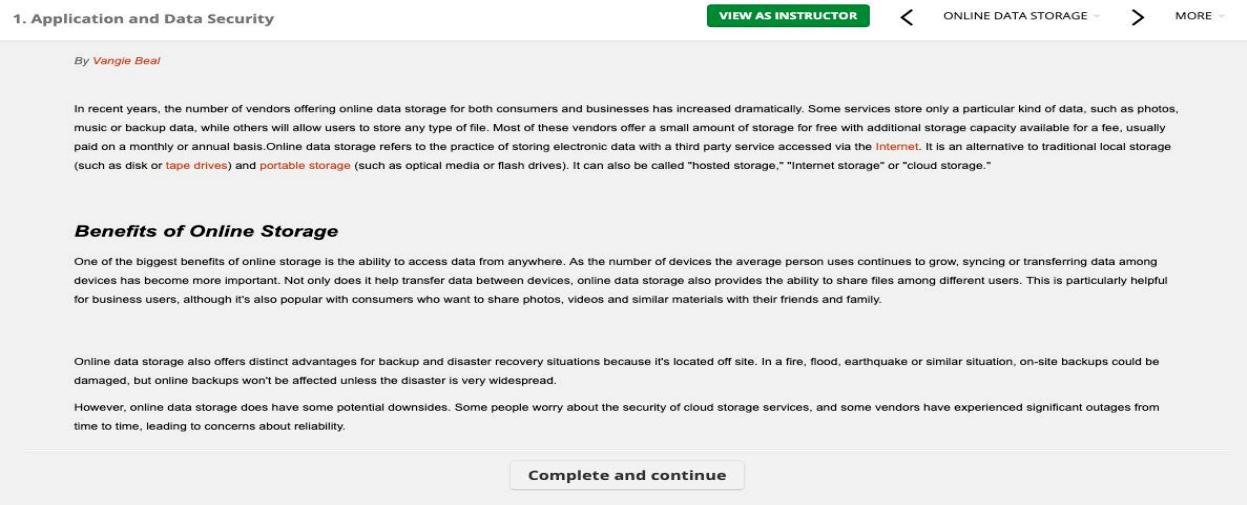




Learner view of the presentation (PowerPoint slide)



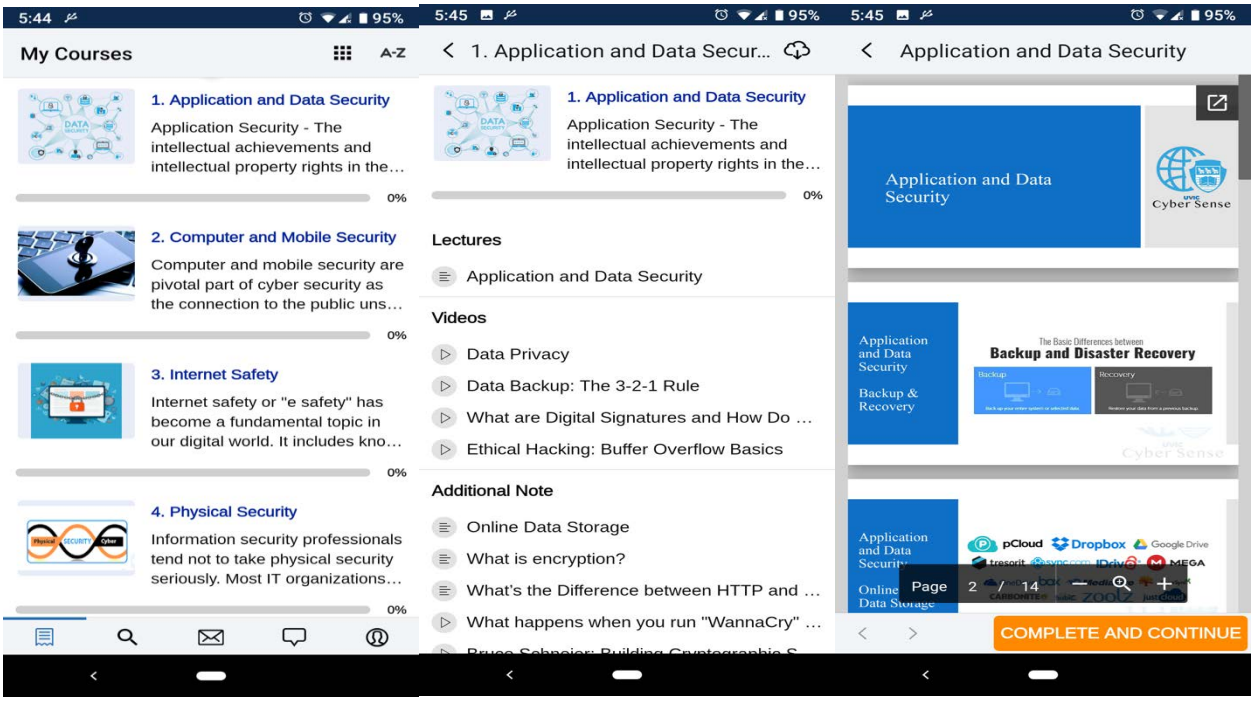
Learner view of a video



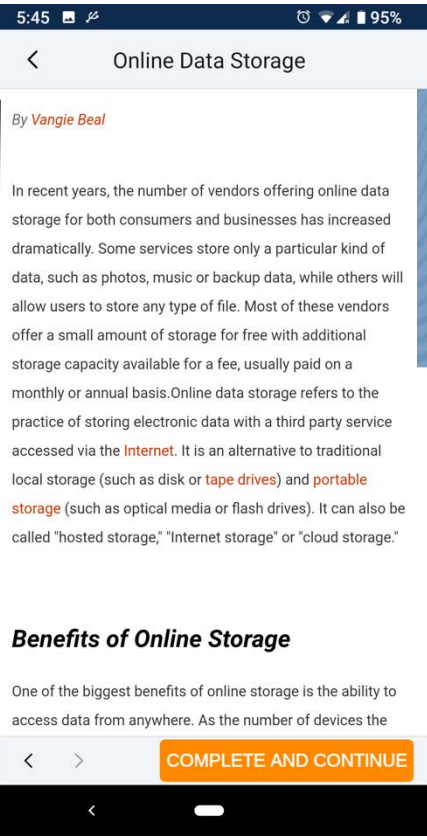
Learner view of a document / Website

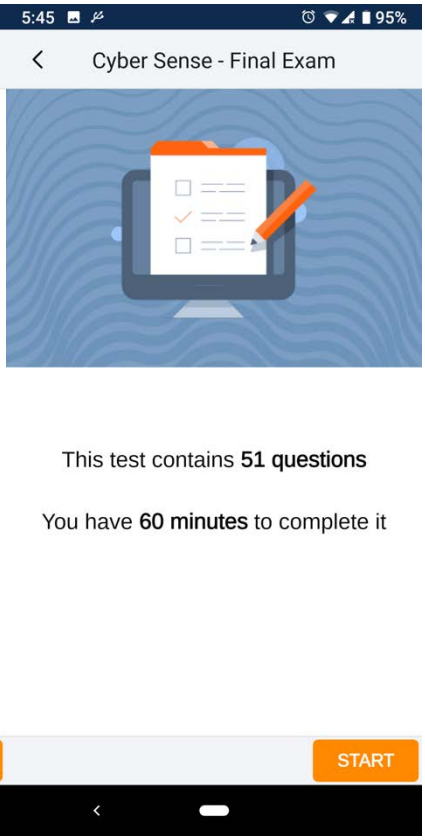
4. Mobile application

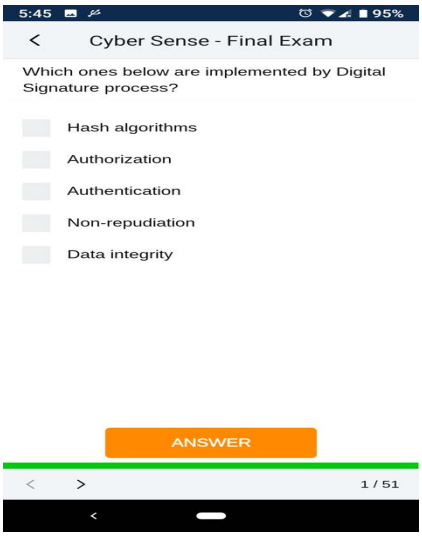
Finally, we will introduce the TalentLMS mobile application. It is an excellent application that can let the student learn our courses everywhere and any places. As shown in the figures below, there are several screenshots of the mobile app.




5:45
95%
Ethical Hacking: Buffer Over...
Ethical Hacking: Buffer O...
COMPLETE AND CONTINUE


5:45
95%
Online Data Storage
By Vangie Beal
In recent years, the number of vendors offering online data storage for both consumers and businesses has increased dramatically. Some services store only a particular kind of data, such as photos, music or backup data, while others will allow users to store any type of file. Most of these vendors offer a small amount of storage for free with additional storage capacity available for a fee, usually paid on a monthly or annual basis.Online data storage refers to the practice of storing electronic data with a third party service accessed via the Internet. It is an alternative to traditional local storage (such as disk or tape drives) and portable storage (such as optical media or flash drives). It can also be called "hosted storage," "Internet storage" or "cloud storage."
Benefits of Online Storage
One of the biggest benefits of online storage is the ability to access data from anywhere. As the number of devices the
COMPLETE AND CONTINUE


5:45
95%
Cyber Sense - Final Exam
This test contains 51 questions
You have 60 minutes to complete it
START


5:45
95%
Cyber Sense - Final Exam
Which ones below are implemented by Digital Signature process?
Hash algorithms
Authorization
Authentication
Non-repudiation
Data integrity
ANSWER
1 / 51

4. Conclusion

All in all, the CyberSense Cyber Security course is made to enlighten the first-year students about the potential issues that can arise due to being naïve to the cybersecurity field. To cover every aspect that can arise any security issue, we have jotted down eight different domains like application security, mobile securities, etc. Through each domain, we have made an effort to convey the importance of that specific domain in ensuring cybersecurity. For each domain, we have marked some guidelines and best practices that are a type of recommendation to be safe if any such situation arises.

While designing the online course, we decided to use a Talent Learning management system, so that we can focus more on making course content rather than just designing the course. This platform is very interactive and flexible to use. In each domain of the course, we have included lectures, notes, videos, presentation slides, and some additional stuff also. Adding different course material have made the course very easy to understand and it gives freedom to the user for selecting their best-suited study material. This makes the course quite intriguing and it does not feel monotonous to the students. Further, the platform provides the facility to interact with the students through the conference and chat. Once the student covers all the course material, the user is headed towards the exam of at least 50 questions, that are selected randomly for each student out of a pool of questions.

The course is not only limited to the course content, but we have also made our best efforts to provide the best recommendations on various aspects for the students who would like to pursue their career in Cyber Security field. One of our domains called Security Awareness is solely made for future recommendations to keep the students engaged and aware. It consists of a set of videos that we have selected very carefully especially for the very inquisitive students. This domain is not held mandatory to cover for the course exam. Lastly, our main purpose was to encourage the students for practicing awareness so that they can avoid any mishappening in future.

References

[1] Cisco, [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.pdf

[2] ctp, [Online]. Available: www.ctp.bilkent.edu.tr/~ctp204/CanerErcanDOC.doc

[3] Heimdalsecurity, [Online]. Available:

https://heimdalsecurity.com/blog/home-wireless-network-security/

[4] IPA, [Online]. Available:
https://www.ipa.go.jp/security/english/virus/antivirus/pdf/Virus_measures_eng.pdf.

[5] ncb, [Online]. Available:
http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Anti%20Virus%20Best%20Practices.pdf

[6] Router Security, [Online]. Available: https://routersecurity.org/

[7] sdtimes, “Google’s top 5 online security practices,” [Online]. Available:
https://sdtimes.com/antivirus-software/googles-top-5-online-security-practices-from-experts-and-users/

[8] Slideplayer, [Online]. Available: https://slideplayer.com/slide/13774175/

[9] techdifferencem, “The difference of authentication and authorization,” [Online]. Available:
https://techdifferences.com/difference-between-authentication-and-authorization.html

[10] Veracode, [Online]. Available:

https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

[11] UKY, [Online]. Available: http://www.uky.edu/~dsianita/390/firewall1.pdf

[12] UVic, “protection of privacy policy,” [Online]. Available:
https://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf

[13] UVic,”information security policy,” [Online]. Available:
https://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf

[14] UVic, “campus security,” available on https://www.uvic.ca/security/home/contact/index.php

[15] Uvic, “Logins and passphrases,” [Online]. Available:
https://www.uvic.ca/systems/services/loginspasswords/index.php

[16] Wikihow, [Online]. Available: https://www.wikihow.com/Use-a-VPN