Network Device

Shih-Yi (James) Chien
Assistant Professor
Dept. of Management Information Systems
National Chengchi University, Taiwan
sychien@nccu.edu.tw

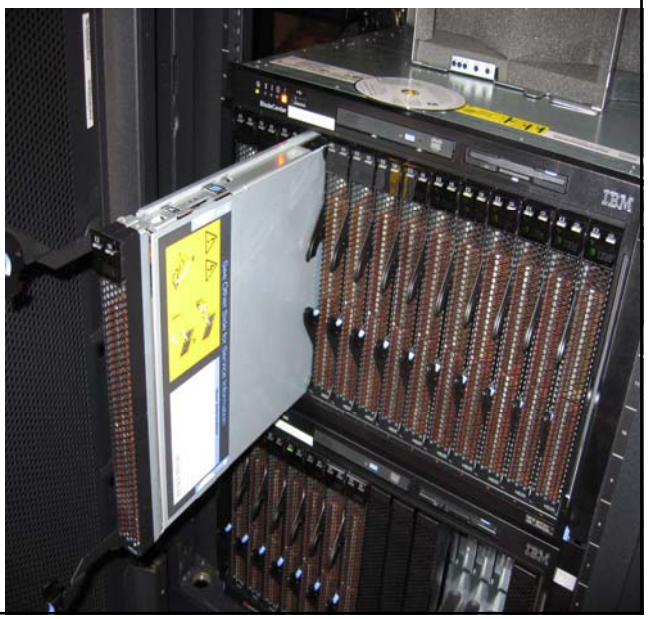
Servers

A **server** is a computer dedicated to providing services to other computers or devices on a network

- Tower server
  - Desktop or laptop can be
- Rack server
  - Require more spaces for the machines
  - Better scalability (more memory slots)
    - Might strengthen the computing power
- Blade server
  - Save space but cooling can be an issue
  - Limited spaces for scalability
  - Support hot plugging

Photo credit: https://www.youtube.com/watch?v=bhT1rV5JUQc&ab_channel=ITSimplifiedinHINDI

Rack server vs. Blade server



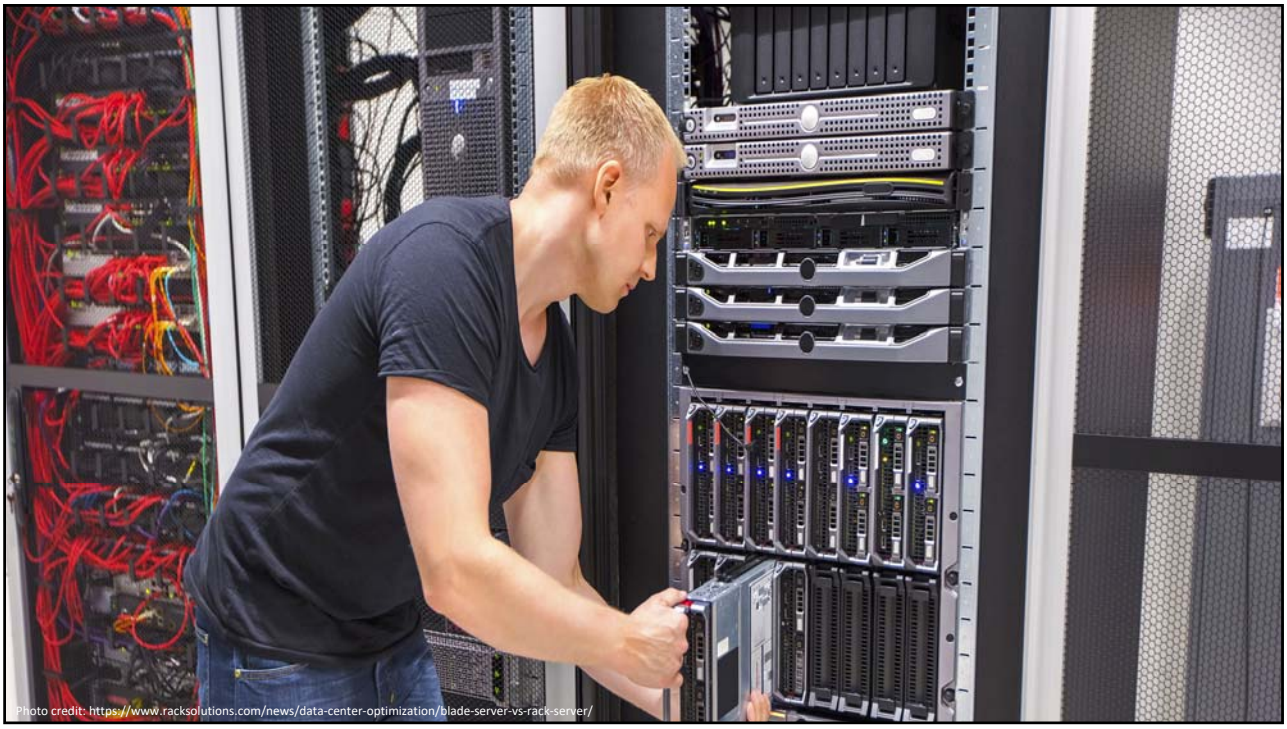


Photo credit: https://www.racksolutions.com/news/data-center-optimization/blade-server-vs-rack-server/

Dedicated Servers

Dedicated servers perform a specific service

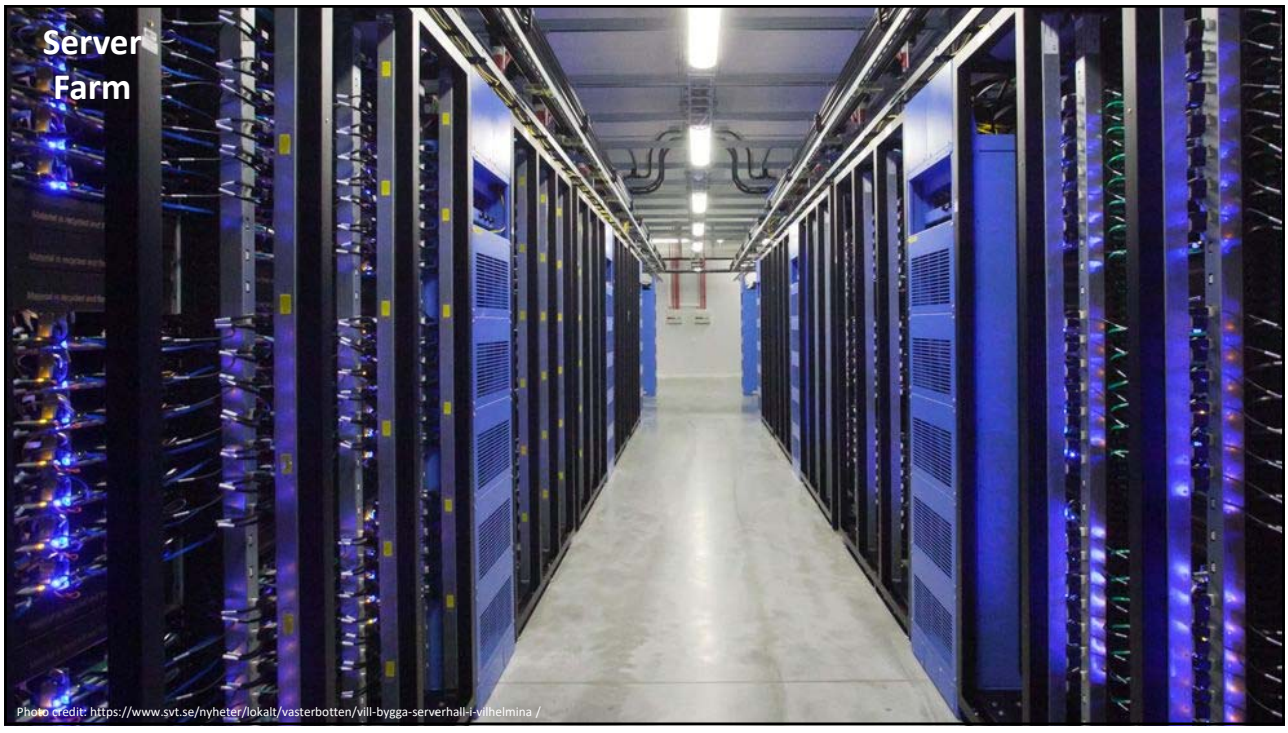
Type	Main Service Provided
Application server	Stores and runs apps
Backup server	Backs up and restores files, folders, and media
Database server	Stores and provides access to a database
Domain name server	Stores domain names and their corresponding IP addresses
File server	Stores and manages files
FTP server	Provides a central location for online gaming
Mail server	Stores and delivers email message
Print serer	Managers printers and documents being printed
Web server	Stores and delivers requested webpages to a computer via a browser

Servers

- Virtualization is the practice of sharing or pooling computing resources, such as servers and storage devices
  - Server virtualization uses software to enable a physical server to emulate the hardware and computing capabilities of one or more servers, known as virtual servers
- Mainframes are large, expensive, powerful server that can handle high-volume online transaction processing simultaneously
  - Finance and banking industries
  - High learning curve for most administrators
- A **server farm** is a network of multiple servers in a single location
  - Better scalability, cost-effective, agile and innovative environments
  - Easy to maintain the machines (with universal OS, such as Linux and Windows)

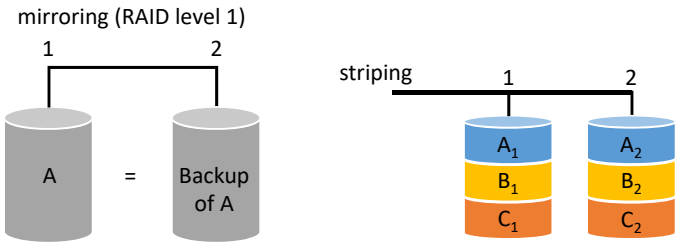
Clip: https://www.youtube.com/watch?v=V9AiN7oJaIM


Mainframe
IBM
IBM
Photo credit: https://en.wikipedia.org/wiki/Mainframe_computer#/media/File:IBM_z13_and_LinuxONE_Rockhopper.jpg


Server Farm
Photo credit: https://www.svt.se/nyheter/lokalt/vasterbotten/vill-bygga-serverhall-i-vilhelmina /

Enterprise Storage - RAID

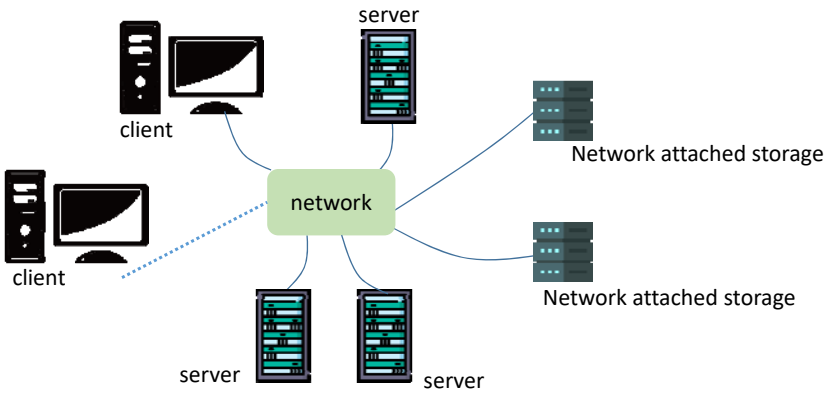
- Enterprise hardware allows large organizations to manage and store data and information with equipment designed for heavy use, maximum efficiency, and maximum availability
- **RAID** (redundant array of independent disks) is a group of two or more integrated hard drives
  - RAID duplicates data, instruction, and info to improve data reliability
  - RAID 0, 1, 5, and 10



Clip: https://www.youtube.com/watch?v=U-OCdTeZLac

Enterprise Storage – NAS

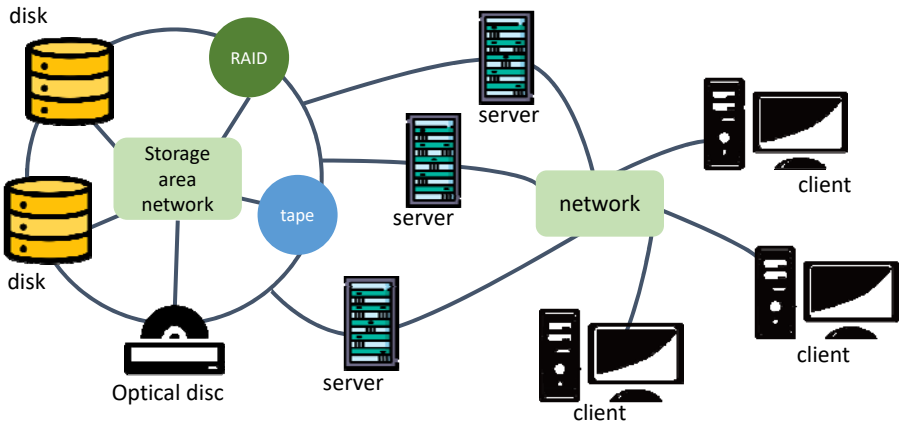
- **Network attached storage** (**NAS**) is a server placed on the network, its sole purpose is to provide storage for users, computers and devices connected to the network



An example of how network attached storage connects on a network

Enterprise Storage - SAN

- A storage area network (**SAN**) is a high-speed network with the sole purpose of providing storage to other attached servers



Clip: https://www.youtube.com/watch?v=3yZDDr0JKVc

DAS vs. NAS vs. SAN

- DAS (direct attached storage)
  - Simple, efficient, low cost
- NAS (network attached storage)
  - Remote access, file sharing, affordable, scalability
  - small and medium enterprises
- SAN (storage area network)
  - Top security and huge capacity, higher speed and performance
  - Large company

https://www.youtube.com/watch?v=bpUzGZLO948

Digital Security and Privacy

Shih-Yi (James) Chien
Assistant Professor
Dept. of Management Information Systems
National Chengchi University, Taiwan
sychien@nccu.edu.tw

Photo credit: https://en.wikipedia.org/wiki/The_Interview
Clip: https://www.youtube.com/watch?v=...RHM&t=...

Cybercrime

- Cybercrime: crime that involves a computer and a network
  - Unauthorized access and use of computers devices or networks
- Digital security risks are the events that may cause loss or damage of computer hardware, software, data, or information
- Identity theft: someone uses another person's personal identifying information
  - Name, ID card or credit card number, password, fingerprints
  - Without their permission, to access a person's (financial) resources

Perpetrator of Cybercrime

- Script kiddie
  - Same intent as a cracker, but without technical skills
  - Use a pre-written cracking program to break into the computer/network
- Corporate spies (excellent tech skills)
  - Good intentions: hired to break into specific computers to identify potential security risks in their organization
  - Bad intentions: Hired to steal information and gain a competitive advantage
- Cyberextortionist
  - Demand payment to stop attacks on the organization
  - Threatening to disclose confidential information or exploit security flaws
- Cyberterrorist (cyberwar)
  - Destroy computers/networks for political reasons

Types of Malware

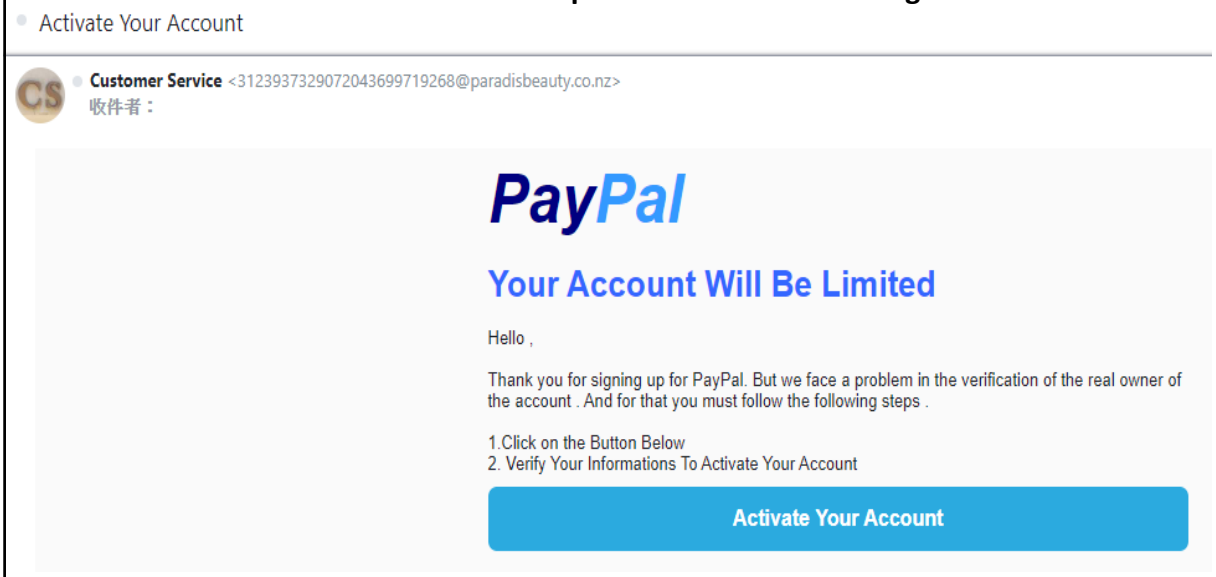
Malware (malicious software) is run by programs that run without the user's knowledge and deliberately change the operation of computers and mobile devices

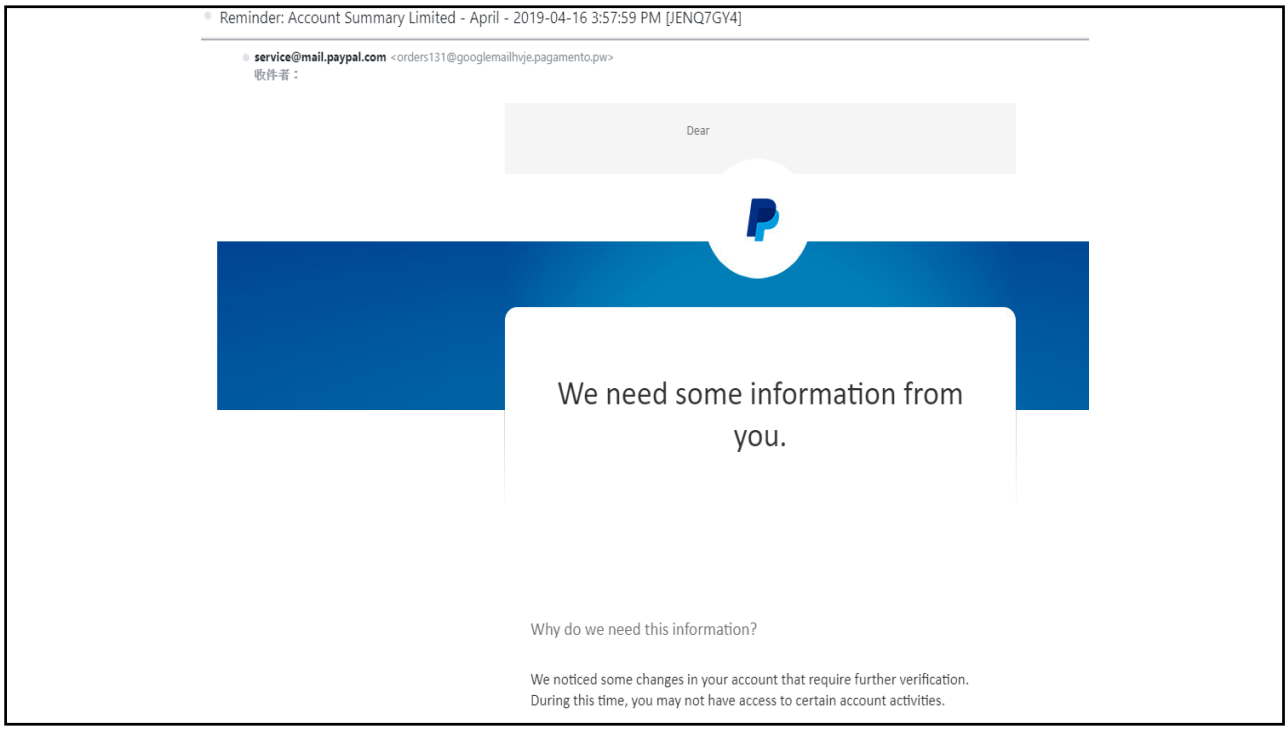
- Social media websites
- e-commerce websites
  - Email
  - ID & Password

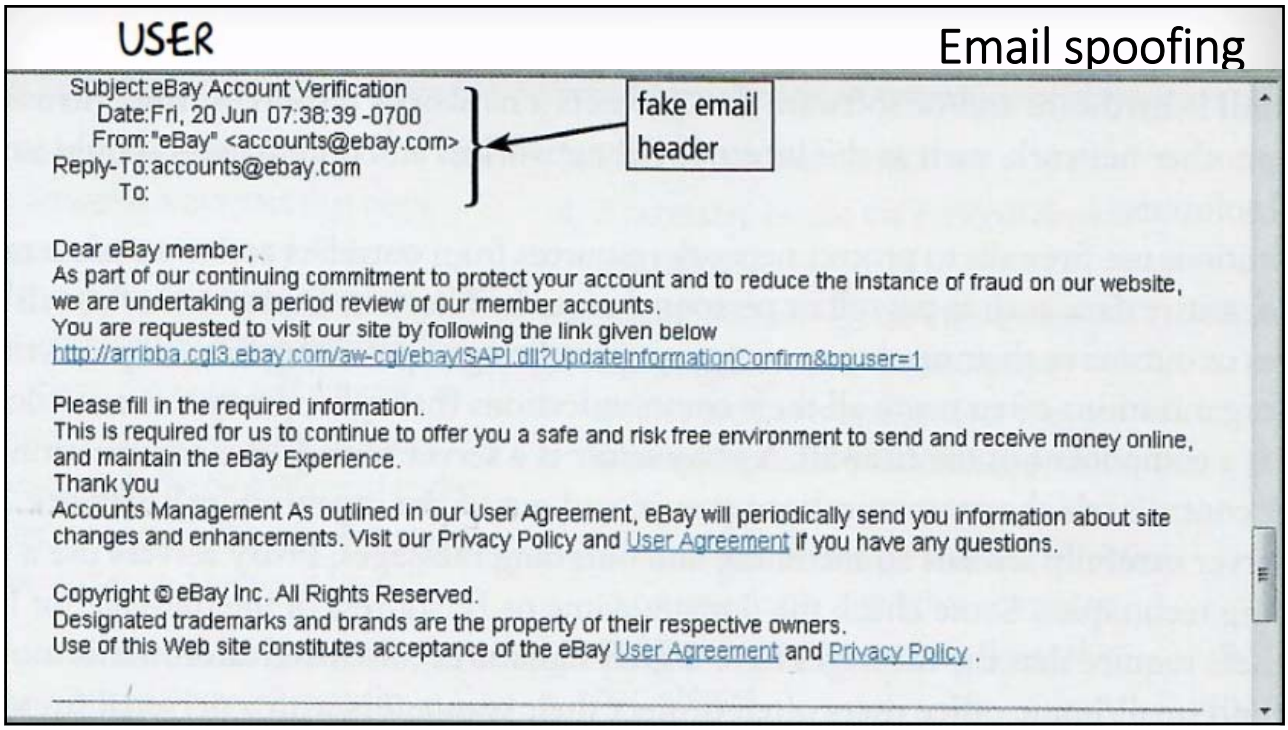
Source: https://en.wikipedia.org/wiki/Malware
Clip: https://www.youtube.com/watch?v=cZ543_0bjbw&ab_channel=CNN

Type	Description
Adware	Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.
Ransomware	Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Rootkit	Rootkits can prevent a harmful process from being visible in the system's list of processes, or keep its files from being read.
Spyware	Spyware describes software with malicious behavior that aims to gather information about a person or organization and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security.
Trojan horse	Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
Virus	Virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.
Worm	A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behavior will continue.

How a Virus can spread via an Email message



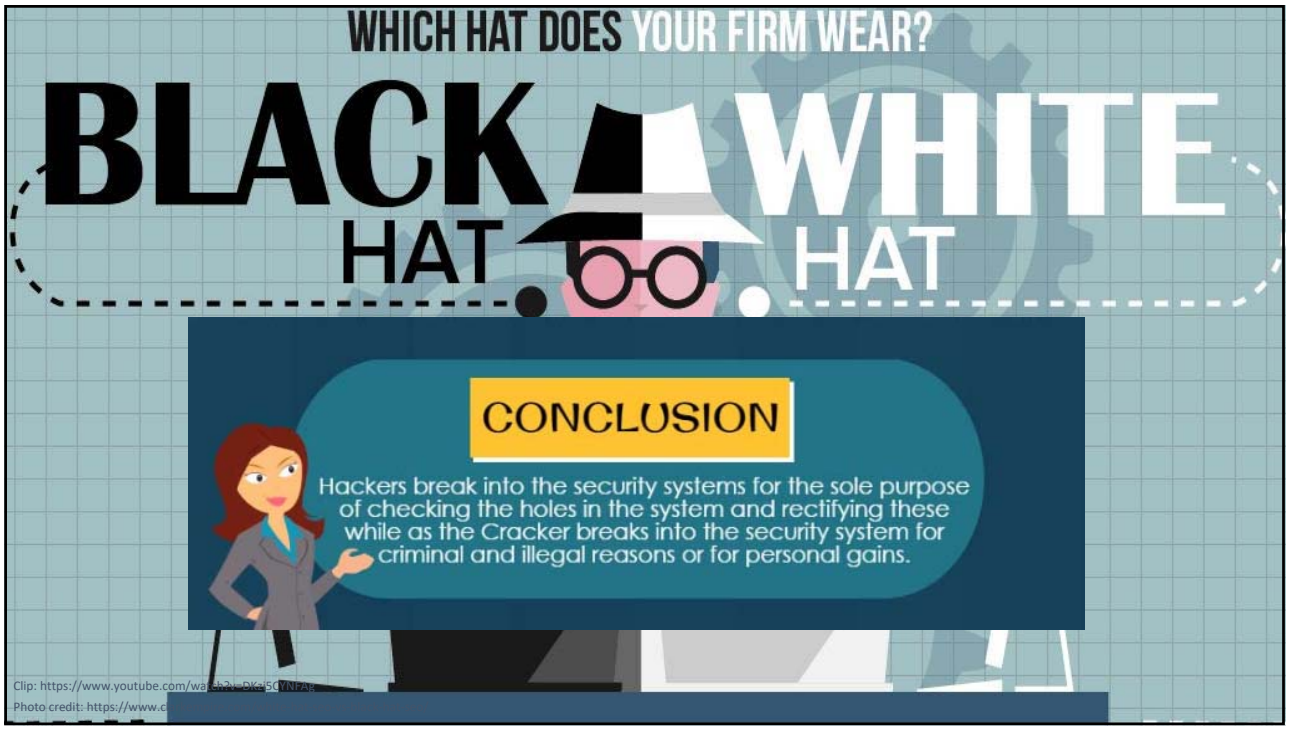

Reminder: Account Summary Limited - April - 2019-04-16 3:57:59 PM [JENQ7GY4]
service@mail.paypal.com <orders131@googlemailhvje.pagamento.pw>
收件者：
Dear
We need some information from you.
Why do we need this information?
We noticed some changes in your account that require further verification.
During this time, you may not have access to certain account activities.


USER
Email spoofing
Subject:eBay Account Verification
Date:Fri, 20 Jun 07:38:39 -0700
From:"eBay" <accounts@ebay.com>
Reply-To:accounts@ebay.com
To:
fake email header
Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1
Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.
Copyright © eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy .

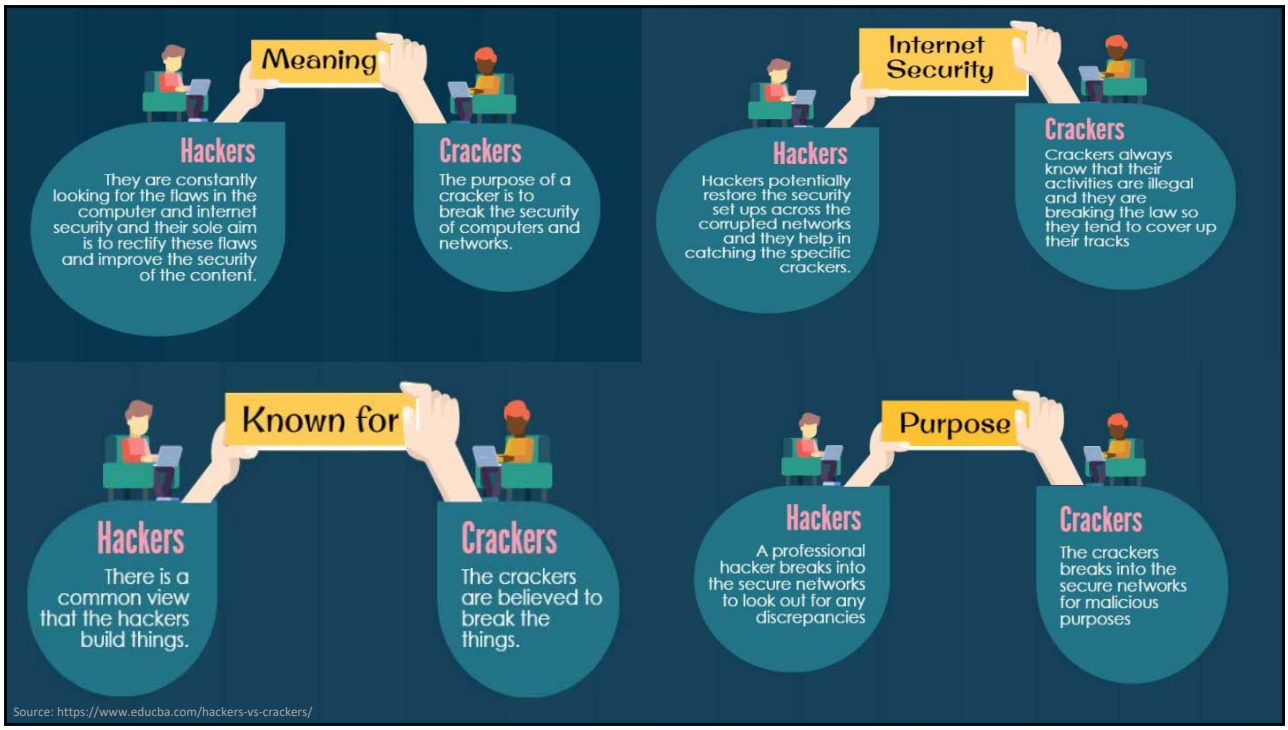
Internet and Network Attacks

- **Botnet** is a group of compromised (mobile) computers connected to the network
  - A compromised computer or device is called as a **zombie**
  - The owner does not know that the computer is remotely controlled by an outsider
- **Denial of service attack** (**DoS attack**) disrupts computer access to Internet
  - Distributed DoS attack (DDoS attack): utilize **many** computers and networks (zombie army)
- **Back door** is a program that allows users to bypass the security control program and remotely access the computer without the user's knowledge
  - Programmers often install back doors to test programs
- **Spoofing** is a technique used by intruders to make network or Internet transmissions appear legitimate
  - IP, email, caller ID spoofing

Clip: https://www.youtube.com/watch?v=c9EjuOQRUdg

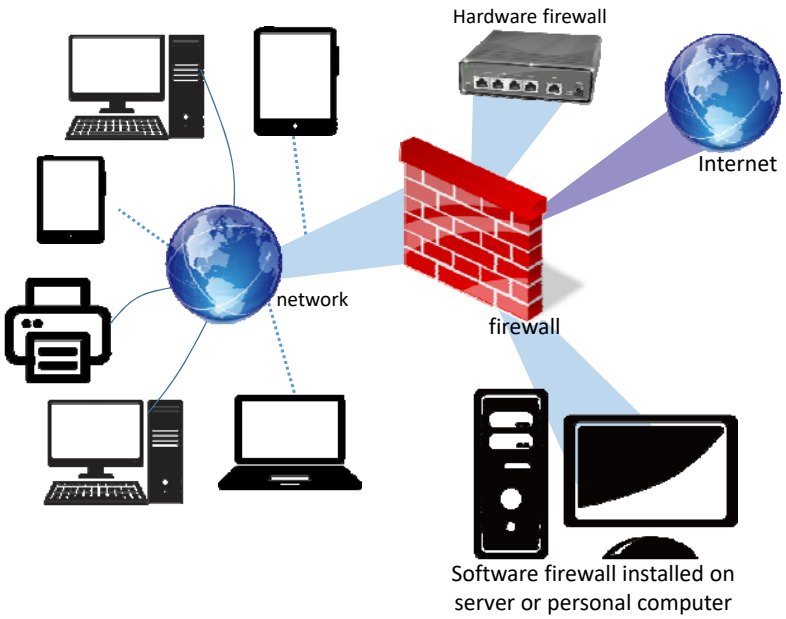


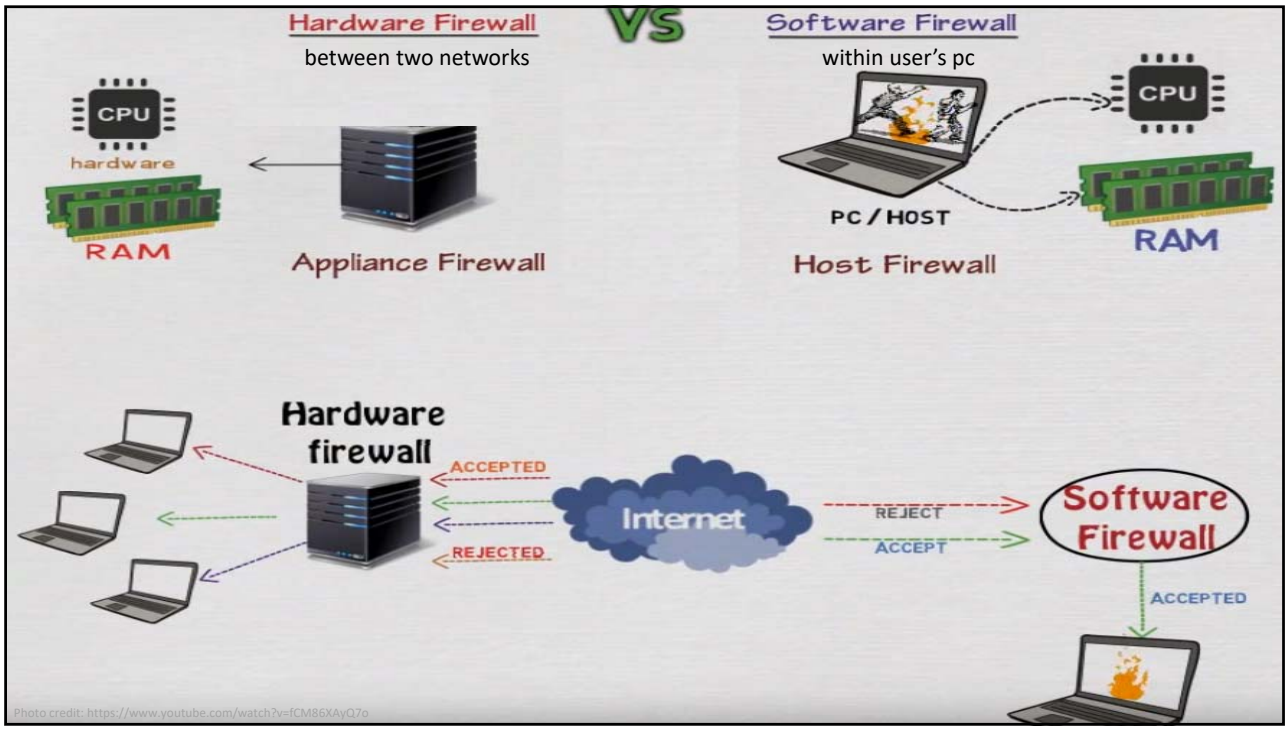
Clip: https://www.youtube.com/watch?v=DKaj5CYNrAs
Photo credit: https://www.c



Firewall

Firewall is hardware and/or software that protects a network's resources from intrusion





Creating Strong passwords

- https://www.betterbuys.com/estimating-password-cracking-times/

SECURE IT 1-3

Creating Strong Passwords

A good password is easy for you to remember but difficult for criminals and password-breaking software to guess. Use these guidelines to create effective, strong passwords:

- **Personal information:** Avoid using any part of your first or last name, your family members' or pets' names, phone number, street address, license plate number, Social Security number, or birth date.
- **Length and Difficulty:** Use at least eight characters, including a variety of uppercase and lowercase letters, numbers, punctuation marks, and symbols. Select characters located on different parts of the keyboard, not the ones you commonly use or that are adjacent to each other. Criminals often use software that converts common words to symbols, so their program might generate the passwords GoToSleep and Go2Sleep as possibilities to guess.
- **Modify:** Change your password frequently, at least every three months.
- **Variation:** Do not use the same password for all websites you access. Once criminals have stolen a password, they attempt to use that password for other accounts they find on your computer or mobile device, especially banking websites.
- **Passphrase:** A passphrase, which is similar to a password, consists of several words separated by spaces. Security experts recommend misspelling a few of the words and adding several numerals. For example, the phrase, "Create a strong password," could become the passphrase, "Creaet a strang pasword42."
- **Common sequences:** Avoid numbers or letters in easily recognized patterns, such as "asdfjkl;," "12345678," "09870987," or "abcdefg." Also, do not spell words backward, use common abbreviations, or repeat strings of letters or numbers.
- **Manage:** Do not keep your passwords in your wallet, on a sheet of paper near your computer, or in a text file on your computer or mobile device. Memorize all of your passwords, or store them securely using a password management app on your computer or mobile device. Additional information about password management software is provided in Module 5.
- **Test:** Use online tools to evaluate password strength.

Consider This: How strong are your passwords? How will you modify your passwords using some of these guidelines?

Worst Passwords of 2020

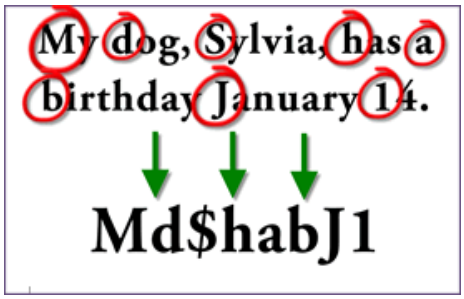
1	123456
2	123456789
3	password
4	qwerty
5	12345678
6	12345
7	123123
8	111111
9	1234
10	1234567890
11	1234567
12	abc123
13	1q2w3e4r5t
14	q1w2e3r4t5y6
15	iloveyou

Passphrases

- A passphrase is a private combination of words, usually containing mixed case and punctuation
- At least 8 characters in length
- Contain characters from 3 of the 4 character classes
  - Numeral
  - Upper case letter
  - Lower case letter
  - Special character (e.g., !, @, #, *, ?)
- Passphrases shall be changed at a minimum of once every 90 days

This Is My Nccu Account Password In Oct 2019

TIMNAPIO2



Source: https://itcs.ecu.edu/passphrase-resources/

Biometric Device

- **Biometric device** verifies the identity of a person by converting personal characteristics into a digital code
  - Fingerprint reader
  - Face, voice, and signature recognition system
  - Hand geometry system: shape and size
  - Iris recognition system: patterns in the iris of the eye

Two-step Verification

- **Two-step verification** uses two different methods (one after another) to verify the user's identity
  - ATM card, then enter a PIN
  - ID and password, then enter security code (text message)

Signing in to your account will work a little differently

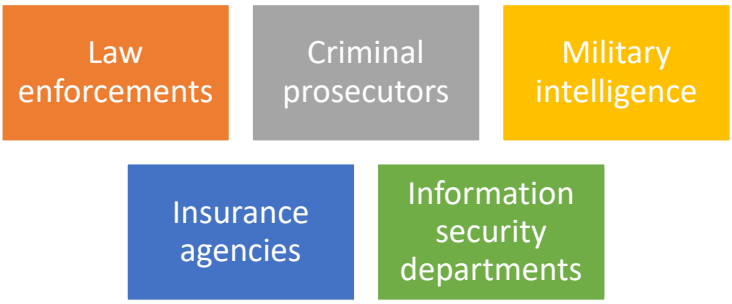
1 **You'll enter your password**
Whenever you sign in to Google, you'll enter your password as usual.

2 **You'll be asked for something else**
Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.

Image credit: https://www.google.com/landing/2step/#tab=how-it-works

Unauthorized Access and Use

- **Digital forensics** is the discovery, collection, and analysis of evidence found for cyber crime
  - https://www.youtube.com/watch?v=ZUqzcQc_syE
- Many areas use digital forensics



Information Theft

- **Information theft** occurs when someone steals personal or confidential information
- To prevent information theft, **Encryption** is the process of converting human-readable data into encoded characters to prevent unauthorized access.
  - To read the data, the recipient must **Decrypt**
    - Imitation Game message decoded
      - http://www.youtube.com/watch?v=_C25CwNlVjA&t=3m5s

An Example of Public Key Encryption

Step1
The sender creates a document to be sent via email to the receiver.

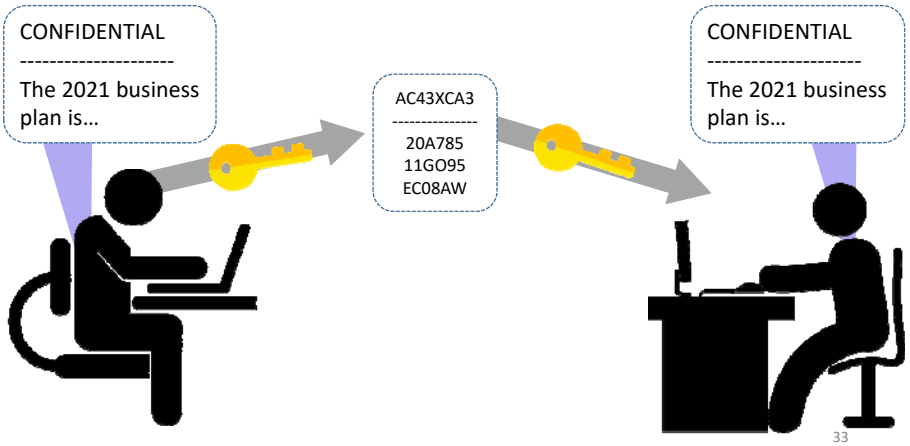
Step2
The sender uses the receiver's public key to encrypt a message.

Step 3
The receiver uses his or her private key to decrypt the message.

Step 4
The receiver can read or print the decrypted message.

Symmetric key encryption: Originator and recipient use **the same secret key** to encrypt and decrypt data

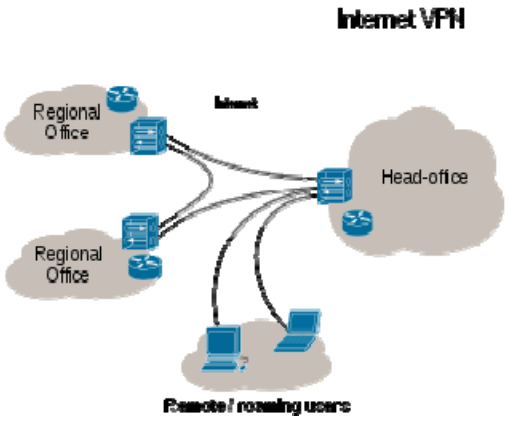
Asymmetric key encryption Originator (**public** key) Recipient (**private** key, must be confidential)



33

Virtual Private Networks (VPN)

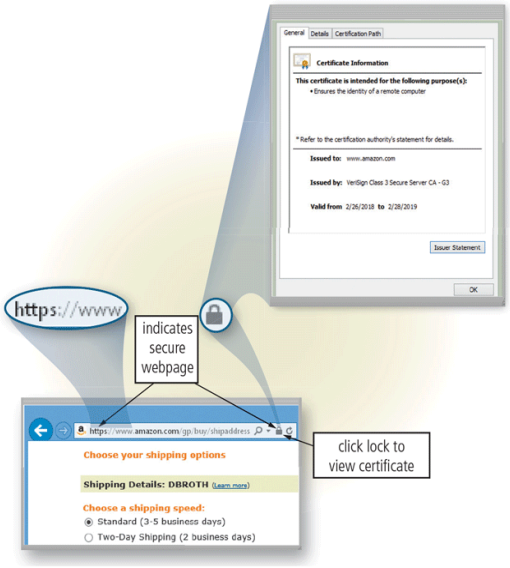
- VPN extends a private network to public network
  - Enable users to send and receive data via shared or public networks
  - As if their device is directly connected to the private network
  - Allow remote users to access corporate applications and resources
  - Allow user who experiences internet censorship to create a secure connection to access the prohibited information
    - https://www.youtube.com/watch?v=_wQTRMBAvzg



Source: https://en.wikipedia.org/wiki/Virtual_private_network

Digital Signature & Certificate

- **Digital signature** is an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity o the sender
  - Internet transaction
- **Digital certificate** is a notice that **guarantees** a user or a website is legitimate
- **Secure site** which uses **encryption technique** to secure its data
  - HTTPS: Hypertext Transfer Protocol Secure



Backup

- **Backup** is a copy of a file, program, or media. If the original file is lost, damaged or destroyed, you can use the backup
  - To **back up** a file means to make a copy of it
- Off-site backups are stored in a different location from the computer or mobile device site

Types of Backups

Type	Description
Full backup	A full backup is the process of making at least one additional copy of all data files that an organization wishes to protect in a single backup operation. The files that are duplicated during the full backup process are designated beforehand by a backup administrator or other data protection specialist.
Differential backup	A differential backup is a cumulative backup of all changes made since the last full backup, i.e., the differences since the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the last differential backup to restore the entire data repository.
Incremental backup	An incremental backup is a backup type that only copies data that has been changed or created since the previous backup activity was conducted. An incremental backup approach is used when the amount of data that has to be protected is too voluminous to do a full backup of that data every day.
Selective backup	Selective backup is a type of data backup process in which only user-specified data, files and folders are backed up. It enables short listing only selected files in a backup process rather than backing up the whole folder, disk or system. Selective backup is also known as partial backup.
Continuous data protection (CDP)	Continuous data protection (CDP), also called continuous backup or real-time backup, refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves. In its true form it allows the user or administrator to restore data to any point in time.[1] The technique was patented by British entrepreneur Pete Malcolm in 1989 as "a backup system in which a copy of every change made to a storage medium is recorded as the change occurs.
Cloud backup	Cloud backup, also known as online backup or remote backup, is a strategy for sending a copy of a physical or virtual file or database to a secondary, off-site location for preservation in case of equipment failure or catastrophe. The secondary server and data storage systems are usually hosted by a third-party service provider, who charges the backup customer a fee based on storage space or capacity used, data transmission bandwidth, number of users, number of servers or number of times data is accessed.

- Differential: backup the files changed since last full backup (sun<->mon, sun<->tues)
- Incremental backup: backup the files changed since last incremental backup (sun<->mon, mon<->tues)

Wireless Security

- Wireless access brings additional security risks
- Risks
  - Reading wireless transmissions
  - Viewing or stealing computer data
  - Injecting malware
  - Downloading harmful content
- Precautions
  - Only connect to an approved wireless network in public
  - Limit the type of activity you conduct on public networks to simple web surfing or watching online videos.
  - Configure the router to improve security

Clip: https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

Wireless Protocol

- WEP (wired equivalent privacy)
  - Earliest wireless security protocol
  - 40 bit encryption key
  - Easily hackable
- WPA (wifi protected access)
  - Use TKIP (temporal key integrity protocol): dynamic change its key
- WPA2
  - Use AES (advanced encryption standard): symmetric encryption algorithm
- WPA3
  - Certification began in June, 2018, enable more robust authentication

Protect Yourself While Online

Configure Browser Security

- **Cookies**
- Scripting
- Plug-ins
- Pop-ups
- Clear browsing data
- Plug-in validation

Intellectual Property

- Intellectual property (IP) refers to **unique and original works**
  - Ideas, inventions, art, writings, processes, company and product names, logos, etc.
- Intellectual property rights are the rights of creators to entitle to their work
- Copyrights protects any tangible form of expression
- Digital rights management (DRM) is a strategy designed to prevent illegal distribution of movies, music, and other digital content

Information Privacy

- **Information privacy** refers to the right of individuals and companies to refuse or restrict the collection, use, and dissemination of information about them
  - Websites often collect data about you, so that they can customize ads and send you personalized emails
  - Some employers monitor your computer usage and emails
  - Try https://activity.google.com

Cyberbullying & Cyberstalking

Cyberbullying

- Bullying on technical devices using online social media platforms, public online forums, gaming websites, text messages or emails
- Considered more harmful than general bullying

- **Cyberstalking**
  - Involves the use of technology to stalk others through email, text messages, phone calls, and other forms of communication

Week	Topic	Lab	Assignment
1 (9/18)	Impact of digital technology	Brief Intro	
2 (9/25)	Computer Hardware and Digital Media	Hardware	
3 (10/2)	**Holiday**		
4 (10/9)	**Holiday**		
5 (10/16)	Operating Systems and Internet *Online Session: Data Visualization by Prof. Hsiao	MS Excel Advanced Functions	
6 (10/23)	Software Development *Online Session: Introduction to AI by Prof. Ku	MS Excel Advanced Functions	HW-1 (5%) Excel
7 (10/30)	Networking Standard *Online Session: Algorithmic Governance by Prof. Chen	MS PPT Advanced Functions	HW-2 (5%) PPT
8 (11/6)	Digital Security and Privacy *Online Session: Intro to Social Technology by Prof. Hsiao	MS Word GitHub Setup	Bring your laptop to the class
9 (11/13)	Midterm Review & Programming Language: HTML I *Online Session: Fake News in Social Media by Prof. Su	Personal Website	HW-3 (10%) Personal Website @ GitHub
10 (11/20)	**Midterm (30%)**		Final Project Topic & Team Members

9 (11/13)	Midterm Review & Programming Language: HTML I *Online Session: Fake News in Social Media by Prof. Su	Personal Website	HW-3 (10%) Personal Website @ GitHub
10 (11/20)	**Midterm (30%)**		Final Project Topic & Team Members
11 (11/27)	Programming Language: HTML II & CSS I	HTML	HW-4 (5%) HTML Exercise
12 (12/4)	Programming Language: CSS I & JavaScript I	CSS	HW-5 (5%) CSS Exercise
13 (12/11)	Programming Language: JavaScript II	JavaScript	HW-6 (5%) JS Exercise
14 (12/18)	Final Project Discussion to polish your ideas (online discussion with the U.S. Profs.)		Prepare slides to discuss your ideas
15 (12/25)	Final Project Discussion to polish your ideas		Prepare slides to discuss your ideas
16 (1/1)	**Holiday**		
17 (1/8)	**Demo Day- Final Project Presentation (35%)**		**Up to 4 students**
18 (1/15)	**Winter Break**		

online or offline discussion with the U.S. Profs and teams

Grading

Homework 35% (7 homework)

- Personal website: 10 pts
- Excel, PPT, HTML, CSS, and JavaScript: 5 pts each

Midterm 30% (Nov. 20)

- Multiple choice questions, true/false questions
- Open questions

Final Group Project 35% (Jan. 8)

- Details shown on next page (submit your poster file by 12/30)

Course participation: 5%

- In case you are in the borderline (#urwelcome)

47

Final Group Project- Presentation

1. Watch all five online videos
2. Find your teammates and form the team wisely
   - Up to 4 students
3. Discuss with teammates and pick up the potential topics
   - The proposed topics must be related to the videos
4. Submit your team info and the proposed topics by Nov. 20
   - First come first serve; prioritize and submit at least three topics
5. Demo day: final group presentation on Jan. 8
   - Provide your own opinions; cite your references- **DO NOT** copy and paste
   - Grade by the instructor, TAs and other groups
   - In-group evaluation: no free rider policy (#howdareyou)

48

CH

科目代號(Course #)：306005001
科目名稱：計算機概論
Course Name：Introduction to Computer Science
授課教師：簡士鎰
Instructor：CHIEN SHIH-YI
系所：資管一甲、資管一乙
上課時間 (Session)：五23 (fri09-11)

EN

科目代號(Course #)：306005011
科目名稱：計算機概論
Course Name：Introduction to Computer Science
授課教師：簡士鎰
Instructor：CHIEN SHIH-YI
系所：資管一甲、資管一乙
上課時間 (Session)：五D5 (fri13-15)