15 Security

Today we will discuss the following topics:

- Security basics
- Viruses and malware
- Account security
- Internet scams and spam
- Cryptography
- Denial of service (DoS) attacks

Security

Computer security

is the prevention of unauthorized computer access, including viewing, changing, or destroying a computer or data.

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security

Computer security

is the prevention of unauthorized computer access, including viewing, changing, or destroying a computer or data.

A security breach is a case of unauthorized computer access.

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security

Computer security

is the prevention of unauthorized computer access, including viewing, changing, or destroying a computer or data.

A security breach is a case of unauthorized computer access.

A malicious security breach done by unauthorized access is often called a hack. Hacks are the most common form of a breach.

Other breaches may be caused by *system glitches* or by *human error*.

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security

Computer security

is the prevention of unauthorized computer access, including viewing, changing, or destroying a computer or data.

A security breach is a case of unauthorized computer access.

A malicious security breach done by unauthorized access is often called a hack. Hacks are the most common form of a breach.

Other breaches may be caused by *system glitches* or by *human error*.

A computer that has been hacked is said to be compromised.

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security

Computer security

Some examples of security breaches:

- a person's private email and photos being viewed by someone without permission.
- a person's email or social media account being used by someone else to post inappropriate messages.
- a computer having a hidden program installed that sends "spam" emails without the computer owner's knowledge.
- an organization's confidential customer and financial data being accessed by a competitor.
- an organization's customer credit card data being copied and sold.

see more at zyBooks

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security

Security holes

A security hole, or vulnerability, is an aspect of a computer that can be used to breach security.

Security holes commonly exist in operating systems. Once discovered, OS makers update the OS to close such holes.

Thus, computer users are advised to keep their OS'es up-to-date, not only to gain new features, but to close security holes.

image is by blogtrepreneur.com/tech
https://www.flickr.com/photos/143601516@N03/albums

Security: viruses and malware

Computer viruses

A computer virus is a program that runs on a user's computer without permission, and spreads itself to other computers, often via email. A computer with a virus is said to be infected.

A computer virus can:

- use the computer for illicit tasks
- stealing information from the computer (e.g.: credit card numbers, passwords, etc.)
- delete data or encrypt data and ask for ransom

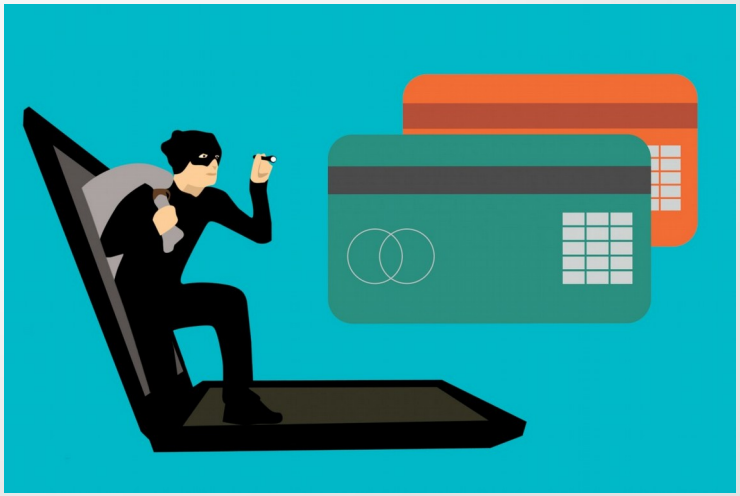

image by Mohamed Hassan
https://pxhere.com/es/photo/1449185

Security: viruses and malware

Computer viruses

Ways and places to get a virus:

- from an email, where a user is tricked into downloading and running an application that installs a virus
- At a website, either by downloading items from such a site, or sometimes merely by visiting the site. *Sites that host free games, that support illegal free music/video downloads, that provide gambling, or that provide free pornography, commonly exist for the purpose of spreading viruses.*
- some viruses also use peer-to-peer file transfers (commonly used for illegal video/music sharing) to spread

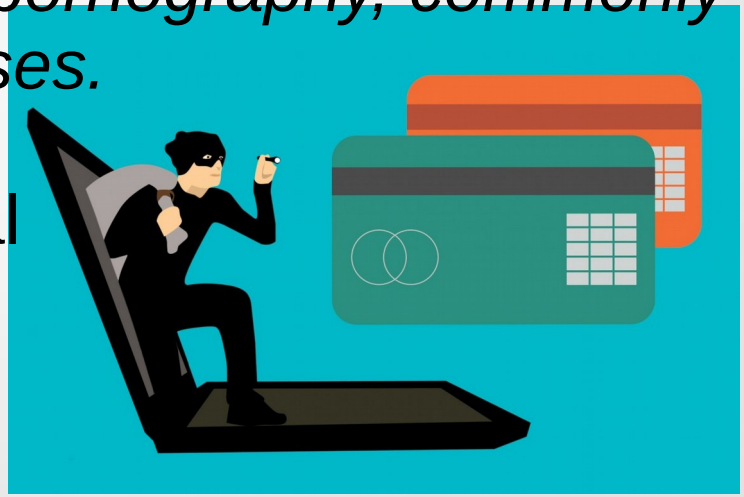

image by Mohamed Hassan
https://pxhere.com/es/photo/1449185

Security: viruses and malware

Computer viruses

A computer may show little or no sign of being infected.

A clue: the computer may be slower than usual,

A clue: the computer is active even when not in use.

Security: viruses and malware

Computer viruses

Antivirus software is a program that:

- looks for known viruses (by searching a hard drive, and/or by monitoring visited websites and downloaded files), and
- disables found viruses.

Some company websites, like drive.google.com, check for viruses on the server before providing a file for download.

Security: viruses and malware

Computer viruses

Antivirus software is a program that:

- looks for known viruses (by searching a hard drive, and/or by monitoring visited websites and downloaded files), and
- disables found viruses.

Some company websites, like drive.google.com, check for viruses on the server before providing a file for download.

Tens of thousands of known viruses exist, with hundreds discovered each month.

In the worst case: a user may have to wipe the computer's drive and reinstall the operating system and programs.

Security: viruses and malware

Computer viruses: smartphones and tablets

Smartphones and tablets tend to have fewer viruses due to having newer OS'es designed for security, and to having most applications being checked for viruses before being available.

Security: viruses and malware

Computer viruses' objectives

A virus commonly has the infected computer do illicit tasks:

- send spam emails (unsolicited mass email)
  e.g.: advertising prescription drugs for sale; further spreading the virus; etc.
  Spamming is illegal in many countries.
  If a spammer sent millions of emails from one computer, email companies might block that computer, and authorities might find the spammer. Instead, a spammer instructs thousands of infected computers to send the spam emails.

Security: viruses and malware

Computer viruses' objectives

A virus commonly has the infected computer do illicit tasks:

- attack an organization's website.
  A denial of service (DoS) attack is achieved by submitting huge numbers of access requests simultaneously to one website, which overloads that site's web server, thus preventing legitimate requests from being handled (those requests are denied service).

Security: viruses and malware

Malware

Malware (short for "malicious software") is undesired software that is typically installed without a user's knowledge and typically bad for the computer or user.

A virus is one type of malware.

The objective of malware includes doing damage, selling products, spying, and more.

Malware is less common in smartphones and tablets.

Security: viruses and malware

Malware

Malware type	Description
Virus	spreads itself via attachment to a host file, like a biological virus attaches to a human
Worm	spreads itself without using a host file
Trojan (trojan horse)	a user installs it believing the software to be legitimate, but the software actually has a malicious purpose
Adware	displays advertisements to the user, commonly in a web browser
Spyware	collects information from a computer without the user's knowledge

Security: account security

Securing online accounts

A common security breach involves unauthorized access to a person's online account, such as an email account or Amazon account.

Such breaches can occur if:

- a person leaves a computer unattended without signing out, especially a public computer(in a school lab or hotel lobby).
- a person saved a password on a public computer.
- a person's computer is stolen and email was left signed in or the password was saved.
- a hacker obtains or guesses a user's password.

Security: account security

Securing online accounts

A common security breach involves unauthorized access to a person's online account, such as an email account or Amazon account.

To prevent a security breach:

- sign out regularly,
- change passwords frequently,
- never write a password in a file, email, or paper,
- use different passwords for different sites,
- use hard-to-guess passwords.
  Good passwords typically are not words in the dictionary, and may mix letters, numbers, and special characters like !, @, $, and %.

Security: account security

Two-step account verification

Some accounts (like gmail) support two-step verification.

Two-step verification helps secure a user's account by requiring the user during sign in to enter a temporary code appearing on the user's mobile phone, which the user usually carries.

Some accounts allow a user to provide a backup access means, such as another email address or a mobile phone number. Thus, if a password is forgotten, or illegitimately changed, the user might still be able to regain access to the account.

Security: Internet scams and spam

Internet scams and spam

An Internet scam is a dishonest scheme or fraud using the Internet.

refer to the zyBooks to see examples of different “types” of scam

Spam is unwanted mass-sent email.

Most spam advertises products or sites (often porn sites).
Some (about 5%) is used for phishing (scam) or spreading malware (like viruses).
Spam costs the sender almost nothing, hence it has grown tremendously, making up 50%-80% of all Internet email traffic in 2014.

Security: Cryptography

Cryptography

We discussed in one of our previous meetings that many of Internet message transmissions between a sender and receiver should be kept secure, meaning others cannot read the message.

Let’s consider three types of message encryptions:

- symmetric-key cryptography
- public-key cryptography
- hybrid public-key/symmetric-key cryptography

Security: Cryptography

Symmetric-key cryptography

A key is a number (or a text string) used to encrypt or decrypt messages.

The sender and receiver use the same key for encryption and decryption (thus symmetric-key cryptography)

Security: Cryptography

Public-key cryptography

Public-key cryptography uses two keys:

- a public key (to encrypt messages), and
- a mathematically-related private key to decrypt messages encrypted by that public key.

Receiver creates two keys that are mathematically related: public and private. The public key is send to the ‘sender’.

Anybody can encrypt with the public key, but only a person with the private key can decrypt.

Security: Cryptography

Public-key cryptography

pros: used when a sender and receiver don't already share a secret key, and the single shared key of course can't just be sent over the Internet unencrypted since an eavesdropper could then know the key.

cons: requires more computation during encryption/decryption due to being mathematically more complex

Security: Cryptography

Hybrid public-key/symmetric-key cryptography

A common hybrid approach used in https (and other scenarios) is:

- public-key cryptography only once: just to share a random secret key.

The web server provides a public key to the web browser, which randomly generates a new secret key and sends that key encrypted to the web server.

The server decrypts using a matching private key, so now the web browser and web server share that randomly-generated single secret key.

Security: Cryptography

Hybrid public-key/symmetric-key cryptography

A common hybrid approach used in https (and other scenarios) is:

- symmetric-key cryptography for everything else: that single shared secret key is used for subsequent message transmissions (in either direction) between the browser and server, using symmetric-key cryptography.

When the session is done, the secret key is discarded; future communications will require a new secret key.