CS50T

By Eng. Rasha Abdeen

Youtube: Coders Camp
https://youtube.com/playlist?list=PLnrlZUDQofUvLtIMvVxZRYYju7ni0Xsxq

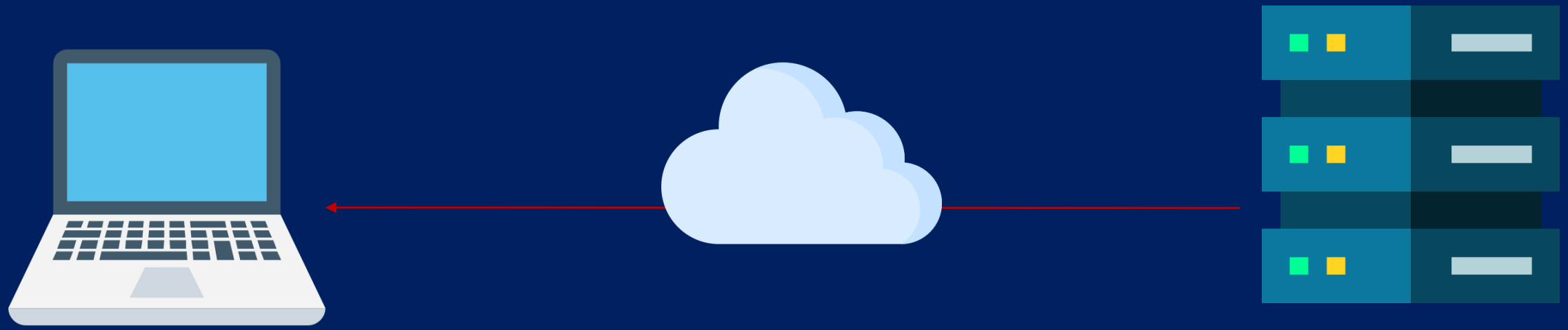
Security

- Computers are among the lease secure devices you own
  - Data or files are stored on them as 0s and 1s
    - Can be financial info, photos, etc.

Privacy:

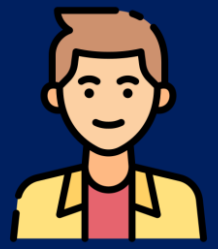
- Keeping people away from things you don’t want them to see

Security



Cyber Security

Is the practice of protecting critical systems and sensitive information from digital attacks.

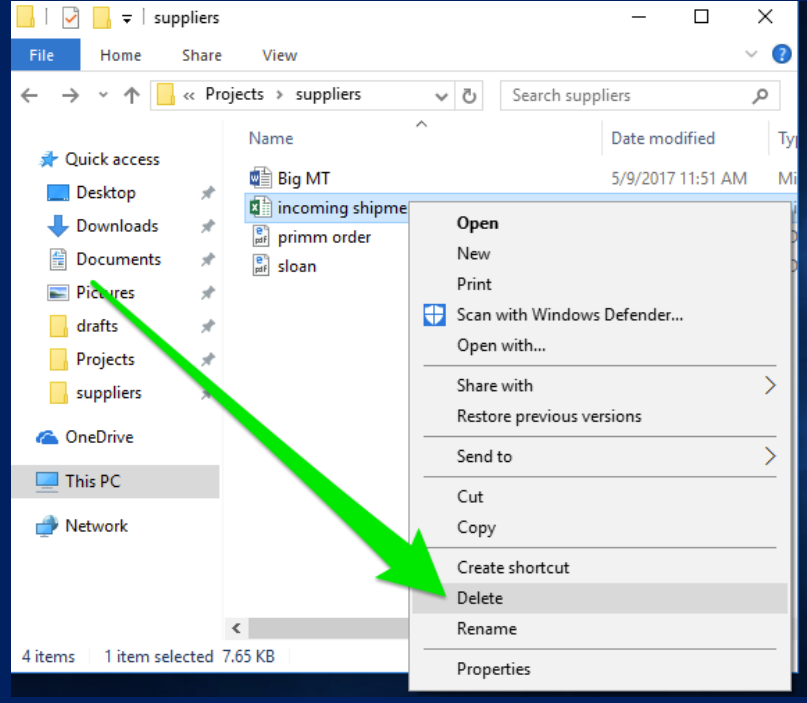


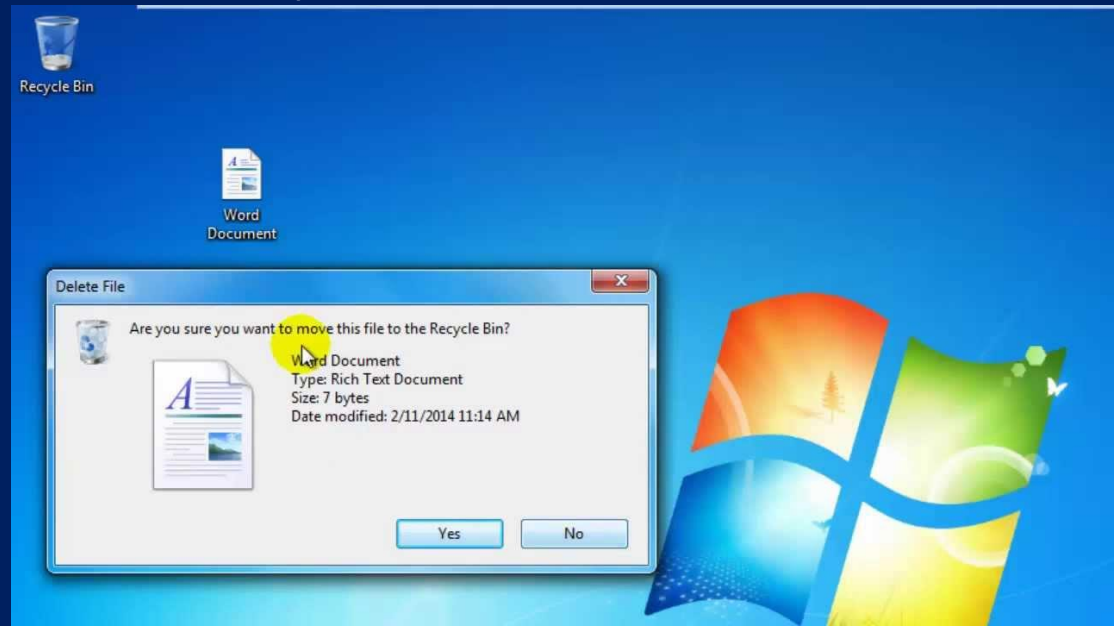
Security

Deleting Files:

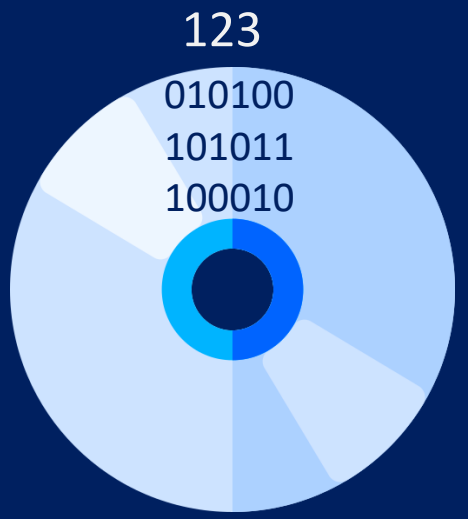
What does it mean to delete a file off of a hard drive?

- When you delete a file visually, it disappears from a desktop or folder
  - Graphically, when a file is deleted, it moves to the trash (or recycle bin)





Security



Deleting Files:

What does it mean to delete a file off of a hard drive?

Files are stored on a computer as 0s and 1s
The operating system has a file that keeps track of files an their location on disk

File	Location
~~CV~~	~~123~~
….	….

Operating system doesn't actually delete it from the hard drive
It simply forgets the location and existence of the file!

Security

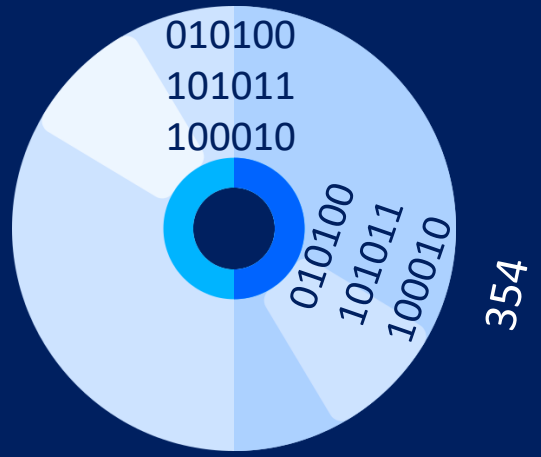
Deleting Files:

How do we delete more securely?!

Re-saving a file with overridden information.

Re-saving a file with overridden information actually could not override the old bits but rather create more 0s and 1s stored on a hard drive!

File	Location
CV	354
….	….



Security

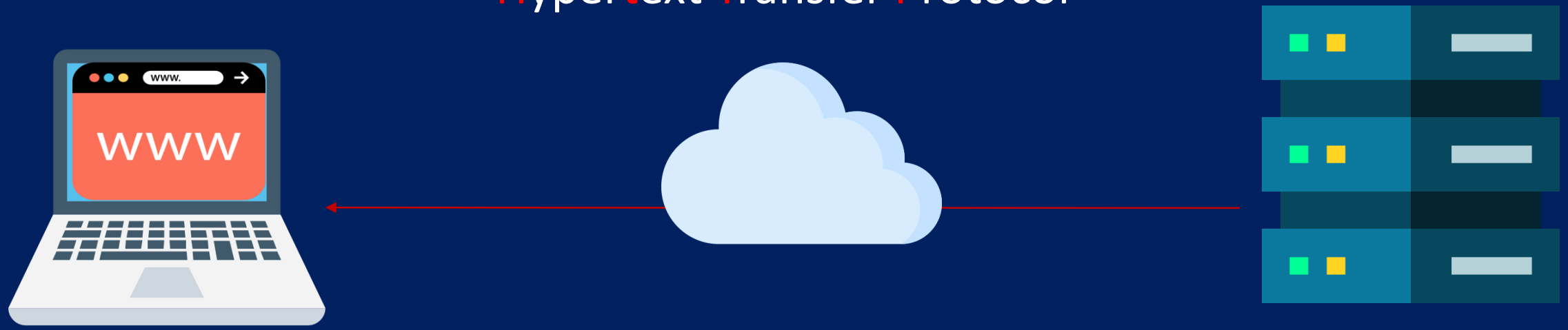
Deleting Files:

Why computers do this obvious flaw with deleting?

- What if we accidentally delete a file?
  - This structure allows for recovery
- Wiping data also takes a lot of time, so it’s much faster to just forget locations of data

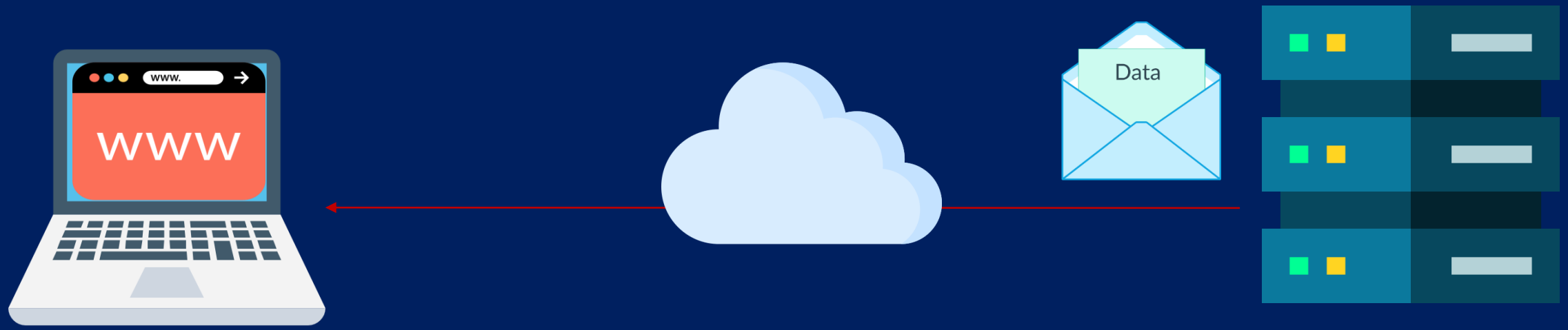
Security

HTTP
Hypertext Transfer Protocol



HTTP stands for **H**yper **T**ext **T**ransfer **P**rotocol
WWW is about communication between web **clients** and **servers**
Communication between client computers and web servers is done by sending **HTTP Requests** and receiving **HTTP Responses**

Security



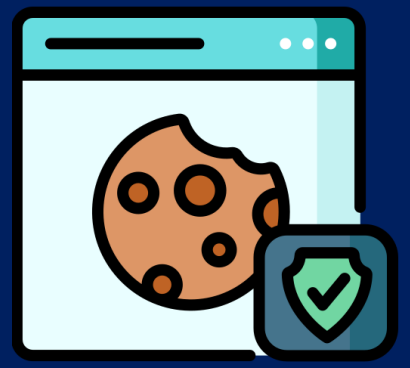

```
GET / HTTP/1.1
Host: example.com
```

```
HTTP/1.1 200 OK
Set-Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

The server gives us a cookie.

```
GET / HTTP/1.1
Host: example.com
Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

Security



Cookies:

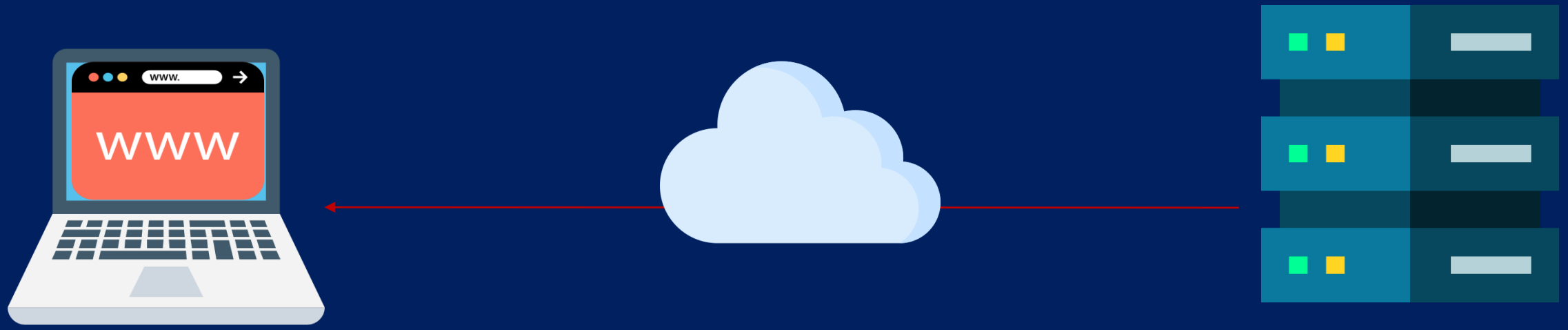
- A feature supported by HTTP
- Little values a web server puts on a user's browser
- Used to remember if a user has visited a website before
  - Allows you to not have to log in every time you visit or refresh a page
    - When you log into a web server, a cookie is planted on your browser
  - Stored in a database
  - Browser will send value to web server to remind of previous login

```
HTTP/1.1 200 OK
Set-Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

Security

Cookies:

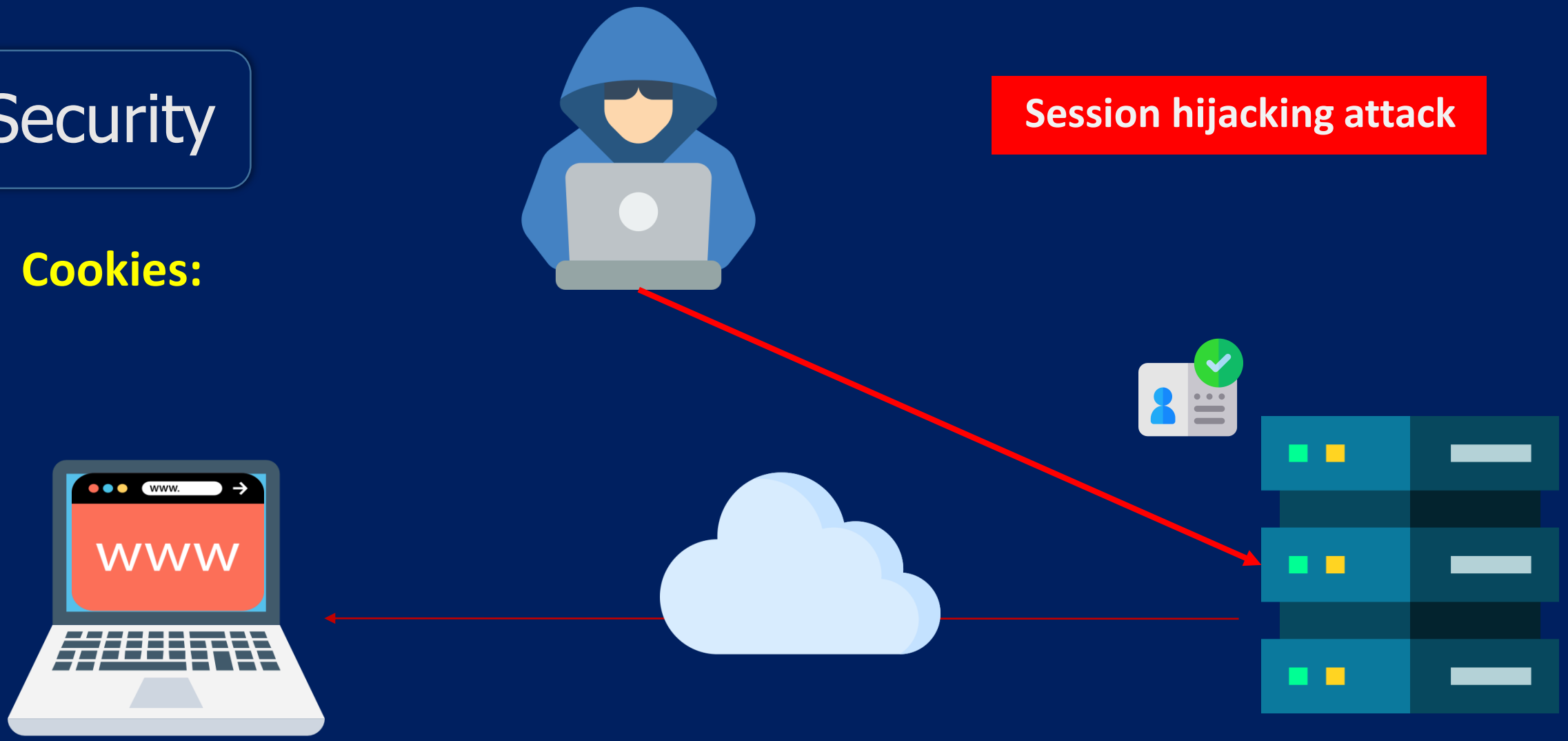
- A cookie is like an ink-based hand stamp for an amusement park or club



Security

Cookies:

Session hijacking attack



Security

Cookies:

Session hijacking attack:

- Wireless information can be intercepted
  - What if a hacker could obtain the cookie
    - Session hijacking attack
    - If you have already logged in, hacker can pretend to be you

How do we protect against that?

Security

Cookies:

How do we protect against that?

- Most websites that these days encrypt this information, scramble it so hackers cannot easily use it.

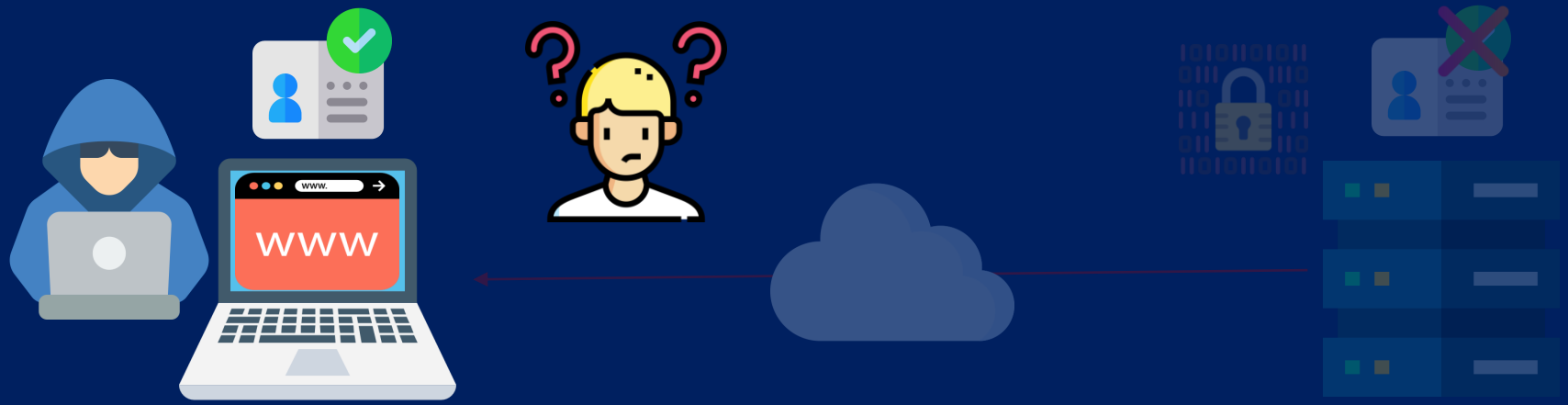
- Hypertext Transfer Protocol Secure (https)

Security

Cookies:

How do we protect against that?

- Browser history remembers everywhere you've been and everything you've done there
  - Convenient if you want to recall a website you've visited
  - **But**, so can anyone else with access to your browser



Security

Cookies:

How do we protect against that?

- Can clear browser history and cookies.
  - History likely not securely scrubbed
  - Will protect you from nosey friends
- Websites will forget you visited as the cookies will be deleted as well!

Security

Incognito Mode

Cookies:

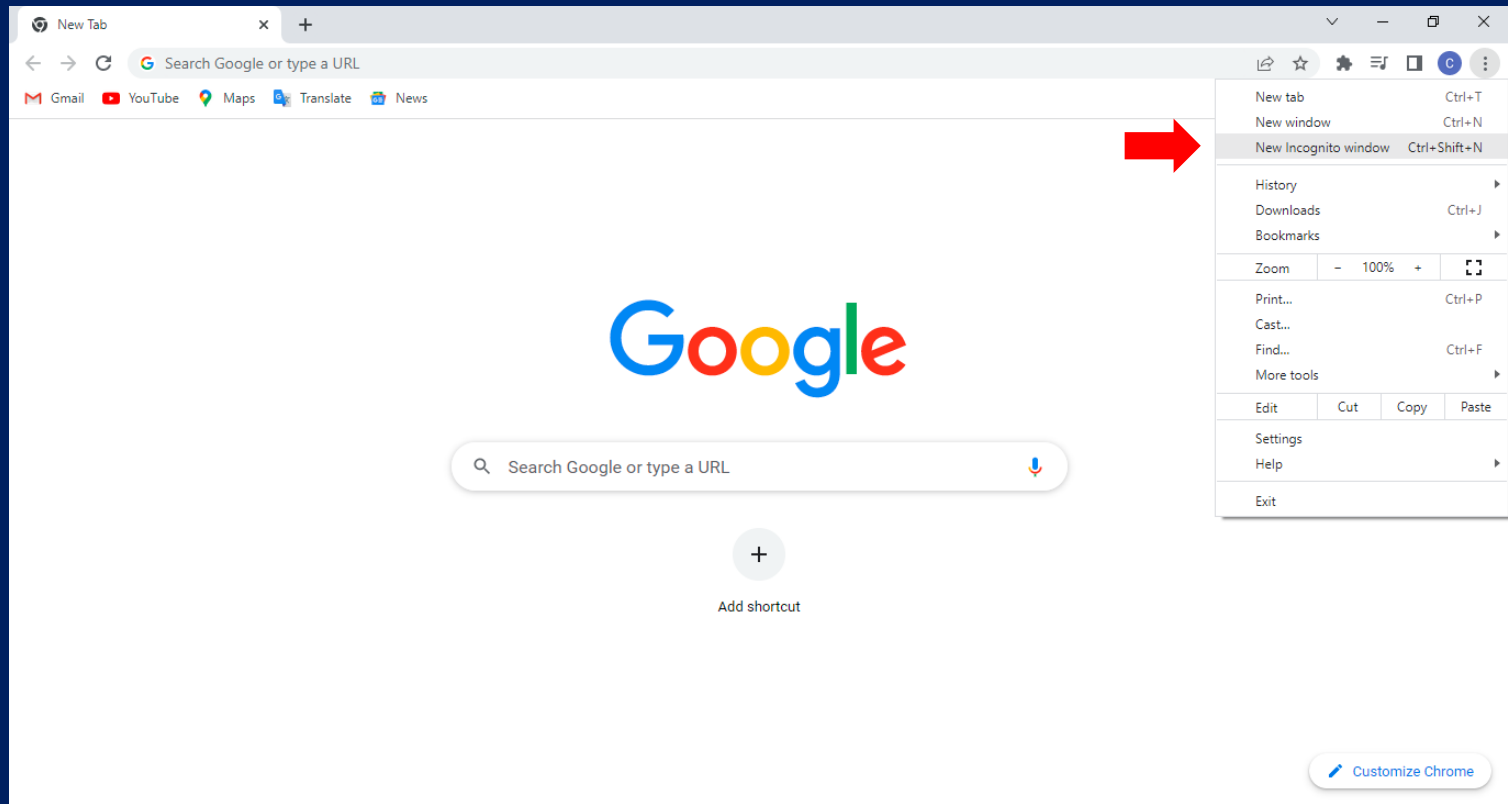
How do we protect against that?

- Can clear browser history and cookies.
  - History likely not securely scrubbed
  - Will protect you from nosey friends
- Websites will forget you visited as the cookies will be deleted as well!

Security

Cookies:

Incognito Mode (Private Mode):



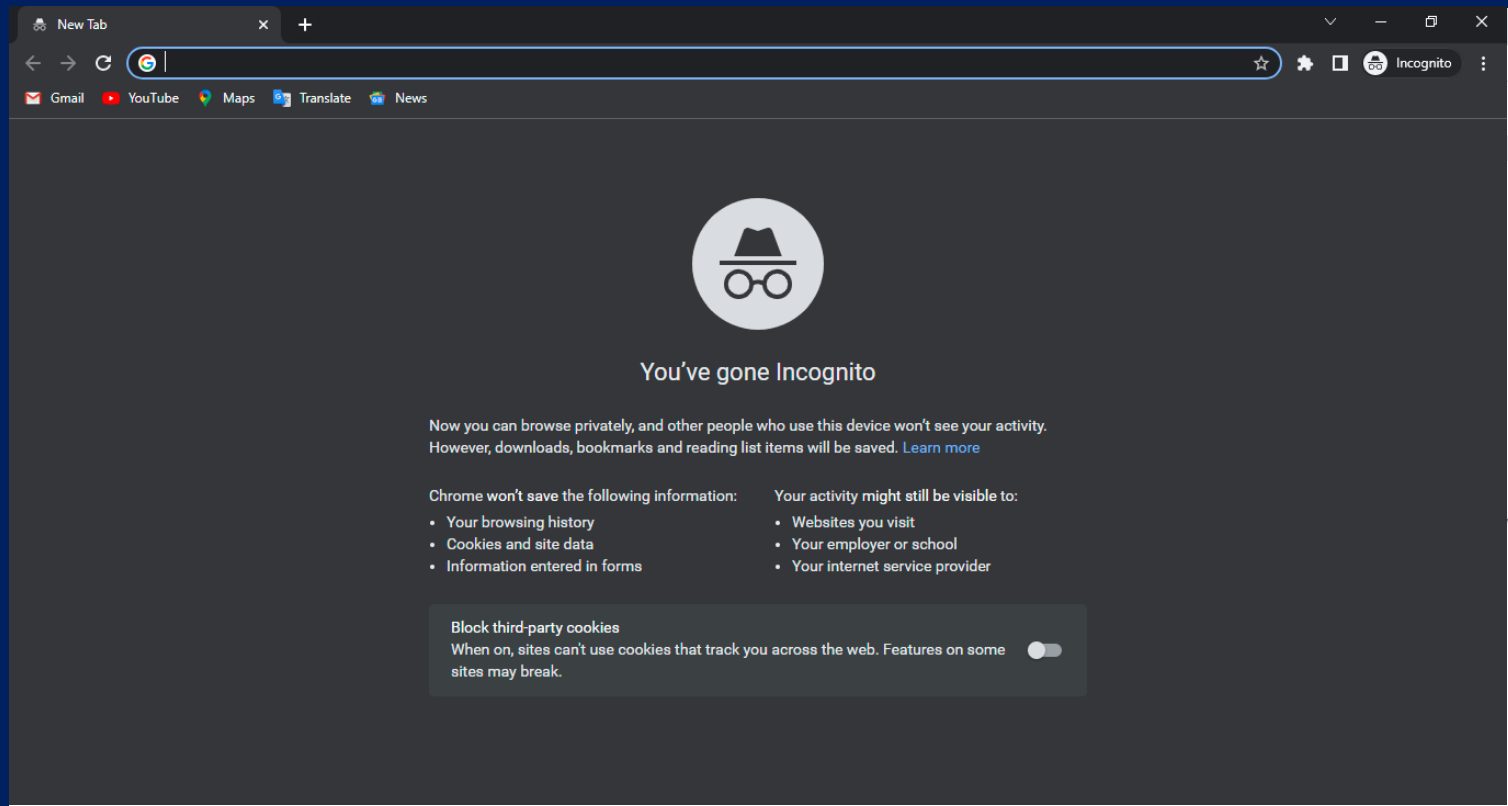
Security

Cookies:

Incognito Mode (Private Mode):

Use if you want history automatically removed.

Useful when building a website as sometimes you want a browser to forget old iterations of your website build.



Security

Authentication

Is the process of validating the identity of a registered user or process before enabling access to protected networks and systems.

1. Password
2. Multi-Factor Authentication
3. Biometric Authentication
    1. Fingerprint
    2. Retina & Iris
    3. Facial
    4. Voice Recognition

Security

Authentication

Password:

Phone

On a phone could only be a few digits (4 digits in iPhone)

Not super secure

_____ _____ _____ _____

10 10 10 10 options

10 X 10 x 10 x 10 = 10,000 possibilities

0000-9999

- On many smartphones, you will have to wait for an amount of time if you have entered a bad passcode
  - Slows down the process of someone guessing

Security

Authentication

Password:

Phone

- Add more digits or letters of the alphabet using a-z, A-Z, 0-9
- Each space now has 62 options (26 + 26 + 10)

62		62		62		62	options
62	X	62	x	62	x	62	= 14,776,336 possibilities

Maybe you're super secure and you have a 20-char password

- You could forget it
- Annoying to type in repetitively

Security

Authentication

Bad Passwords:

Don’t use popular words and phrases

- Hackers will look for words or common phrases

Security

Authentication

2017

Bad Passwords:

Most common Passwords

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

Hackers have dictionaries of bad passwords that they can search through and try

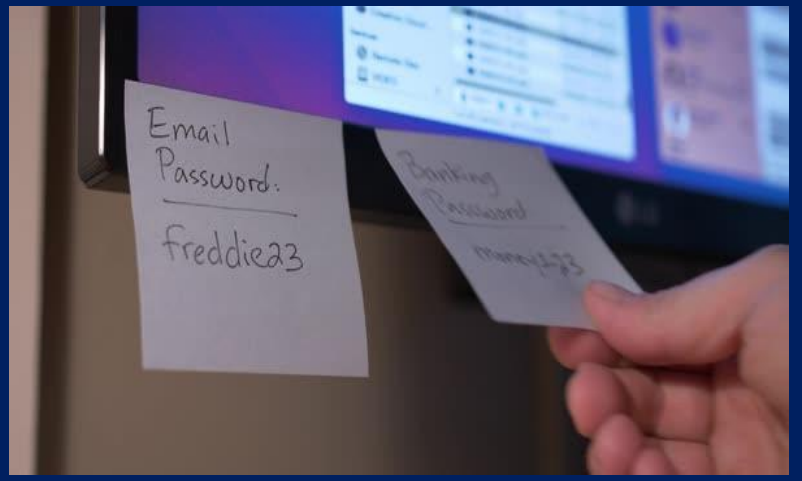
Security

Authentication

Bad Passwords:

1. Four Digit Years
   - Examples: 19XX, 20XX, other anniversaries or famous years like 1776 or 1066
2. "Password"
   - Examples: pass, password, p@$$word or any variant
3. Sports References
   - Examples: footballfan, hockey, gosox
4. Names
   - Examples: pets, spouses, children, grandchildren, celebrities
5. Personal Information
   - Examples: your name, email address, phone number, or social security number
6. Keyboard Patterns or Sequences
   - Examples: qwerty, asdf, 123456,abc123

Security



Authentication

Bad Password Habits:

1. Use random passwords
   - Usually have to confirm so it can be hard to replicate or remember.
2. Using numbers to represent letter is common
   - 1 for l
   - 4 for A

   The hacker can also be just as clever as you, and try those things first before he even bothers trying the completely random ones.
3. Don’t put your post-it with your password on your monitor!
4. Constant password changes can be a net negative
   - Can encourage easier passwords to help with memorization

Security

Authentication

Good Password:

1. An English uppercase character (A-Z)
2. An English lowercase character (a-z)
3. A number (0-9) and/or symbol (such as !, #, or %)
4. Ten or more characters total.

- It’s suggested you mix uppercase, lowercase, and throw in numbers
  - Good to use misspellengs

- One way to do this is to start with a word you will remember:
  - Bookworms
  - Then heavily modify it with special characters, numbers, and mixed capitalization.

    b0-OK&wurms

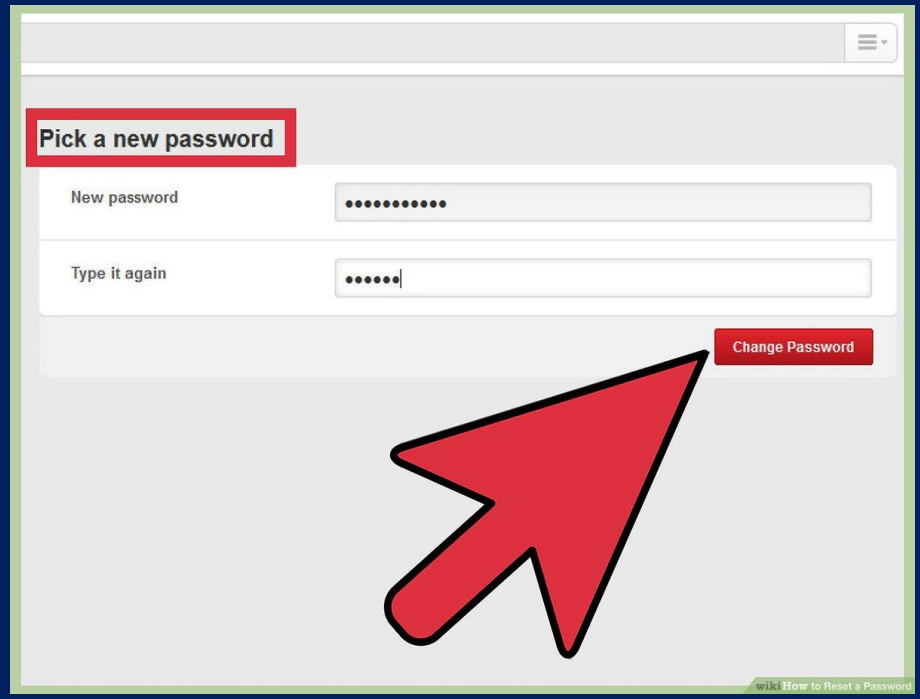
Security

Authentication

Password Resetting:

- Often can click on a link to reset your password
  - Asks you to type email address or username
- Typically, you get an email with a link
  - Hopefully this goes back to the same website!
  - It likely has a random value in the URL
- Once back at the website, you update your password

What if you've wanted to know what your password is !!

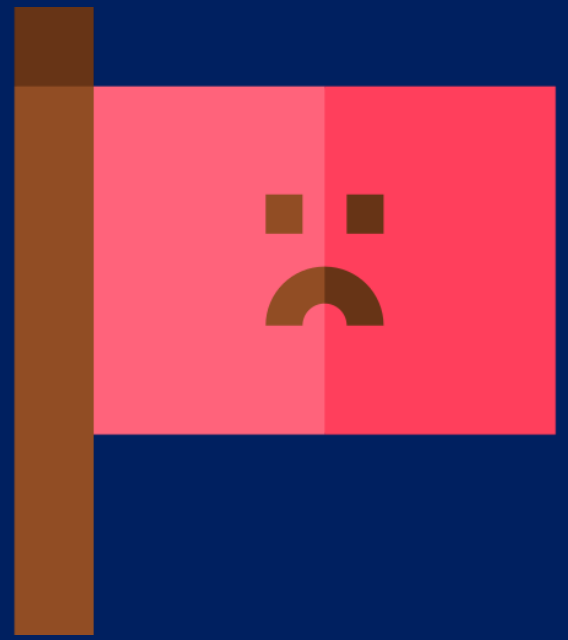


Security

Authentication

Password Resetting:

What if you've wanted to know what your password is !!



- Typically, tech staff can't tell you what your password is
  - Odds are your password is encrypted (scrambled) or, more technically, hashed in their database
- Getting a password in email means that the password are not hashed or encrypted!
  - Also, sending a password over email opens that email to interception
  - This is a red flag if a website does this

Security

Authentication

Bad Password Habits:

- **Using The Same Password**
  - You may have a favorite password that you reuse
  - However, what if one of the websites are hacked?
  - A hacker may try to use the password on other websites to see what she or he can get into!

But its difficult to remember all these passwords

Security

Authentication

Password Managers

- Software called password managers exist that store on your phone or hard drive all usernames and passwords in an encrypted way
  - You have a master password that logs you into everywhere!
    - Store it physically in somewhere like a safety deposit box
- Password managers create long random passwords and will log in for you
  - All websites have different passwords!

Security

Authentication

Two-Factor Authentication:

1. First factor is a password
   - Historically, something “only” the user knows
   - Can be guessed
2. Second factor should be fundamentally different
   - An RSA device displays a unique value that is synced with a server
   - This number needs to be typed in too!
   - As long as this device isn’t stolen by someone with your password, they can’t get in as easily

Security

Authentication

Two-Factor Authentication:

- Now you don’t need a physical device like a company you can actually use software.
- Some companies can use SMS (text messages)

You should think about what websites you care about the most and enable two factor authentication

Security

Authentication

Is the process of validating the identity of a registered user or process before enabling access to protected networks and systems.

1. Password
2. Multi-Factor Authentication
3. Biometric Authentication
    1. Fingerprint
    2. Retina & Iris
    3. Facial
    4. Voice Recognition

Security

Authentication

Is the process of validating the identity of a registered user or process before enabling access to protected networks and systems.

1. Password
2. Multi-Factor Authentication
3. Biometric Authentication
    1. Fingerprint
    2. Retina & Iris
    3. Facial
    4. Voice Recognition

Security

Authentication

Is the process of validating the identity of a registered user or process before enabling access to protected networks and systems.

1. Password
2. Multi-Factor Authentication
3. Biometric Authentication
    1. Fingerprint
    2. Retina & Iris
    3. Facial
    4. Voice Recognition

Security

Network security:

Wireless connection

If the wireless connection has not password to log in the connection is not secure

- You may still visit https or secure websites
- However, everything you do on http sites can be seen

What to do?

- Don’t use that network
- Use a VPN (Virtual Private Network)

Security

Network security:

Wireless connection

VPN (Virtual Private Network):

- Virtual because no physical cables are involved in the connection process.
- Private because through this connection, no one else can see your data or browsing activity.
- Networked because multiple devices—your computer and the VPN server—work together to maintain an established link.

Security

Network security:

Wireless connection

VPN (Virtual Private Network):

By using VPN your Connection to internet is **encrypted**

- First establish encrypted connection to a server and let this server communicate for you
  - The connection between the VPN server and website can still be insecure!
- Because we are encrypting data through an algorithm, using a VPN it can slow down speed.

- **Suppose that you're visiting a country in which some website is blocked. How, technically, might using a VPN allow you to visit that website nonetheless?**

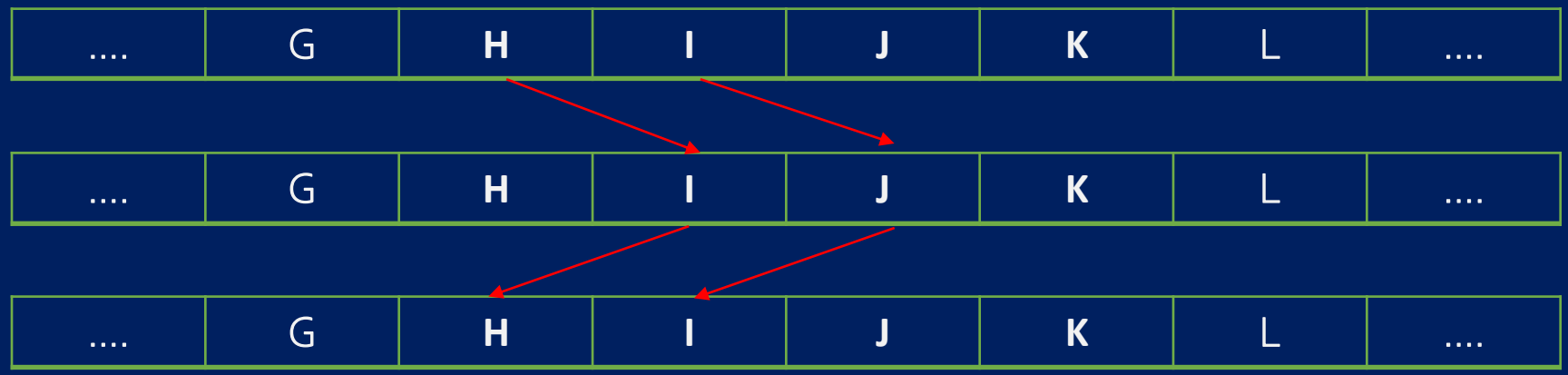
Security

Network security:

Encryption

Data sent via public networks can be “sniffed” by adversaries.

Security



Network security:

Encryption

Plaintext ⇢ Cyphertext ⇢ Plaintext

- HI ⇢ IJ ⇢ HI

This is called a **Caesar cypher**

- Rotational cyphers are not that secure
  - Can be guessed easily
  - Not used for internet encryption
- For this to work, recipient needs the key
  - To know the key, we need to agree in advance
    - Can't send it encrypted as well as they need the key!

A Caesar cypher is secret-key cryptography

- Only one key

Security

Bob

Private Key
Public Key

Alice

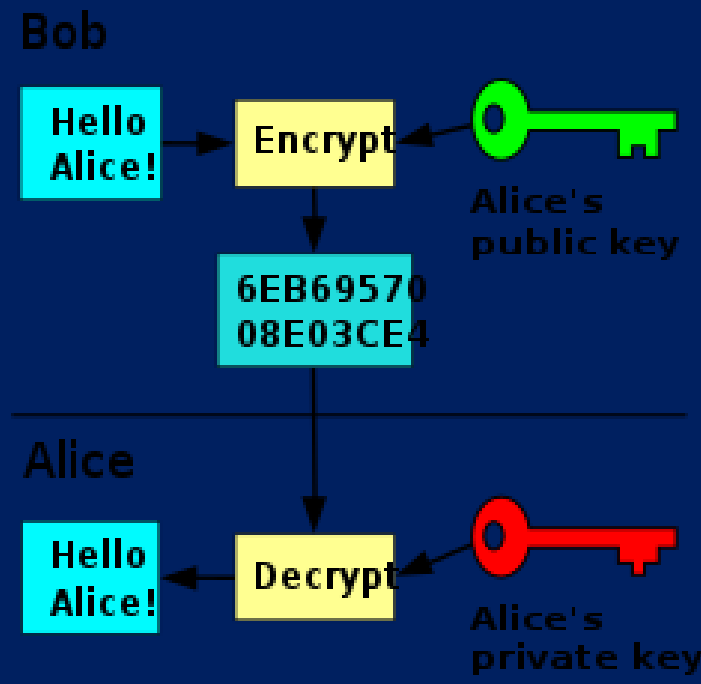
Private Key
Public Key

Network security:

Encryption:

Public Key Cryptography:

- Your browser has its own public and private keys
  - So does websites like Google and Amazon
    - This allows them to communicate securely with you
- Often this processes is used to exchange a secret key



Security

Network security:

Wireless connection

VPN (Virtual Private Network):

By using VPN your Connection to internet is encrypted

- First establish encrypted connection to a server and let this server communicate for you
  - The connection between the VPN server and website can still be insecure!
- Because we are encrypting data through an algorithm, using a VPN it can slow down speed.

Why you might use a VPN ?!

- A VPN protects its users by encrypting their data
- masking their IP address.
- leaving their browsing history and location untraceable
- Prevent ISP and third-party tracking

Security

Network security:

Firewalls

A physical firewall is a wall between connected buildings that prevents the spread of fire

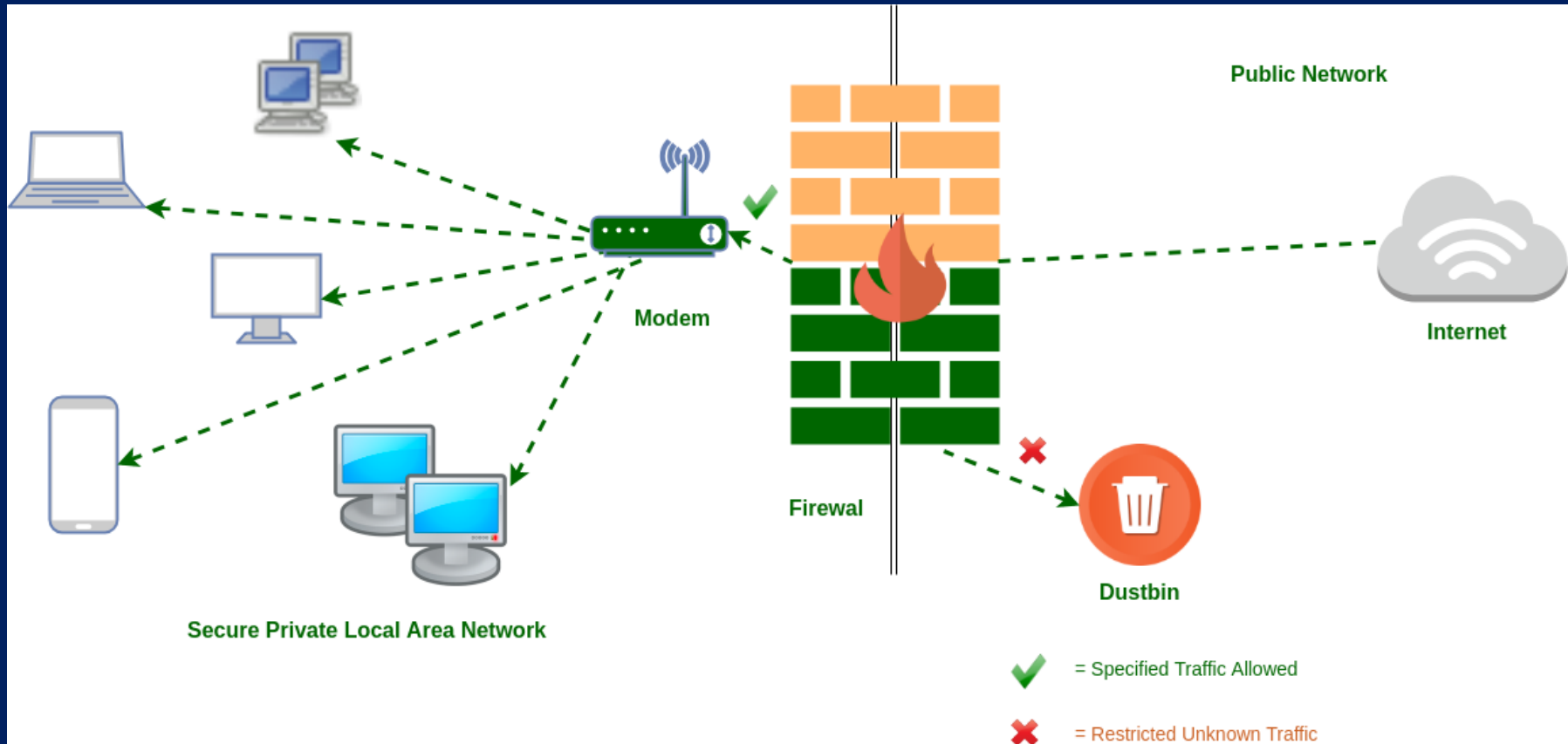
In the world of computer science, a firewall is software that looks at IP addresses and helps keep bad guys out and user data inside

Helps prevent people from accessing your computer

Security

Network security:

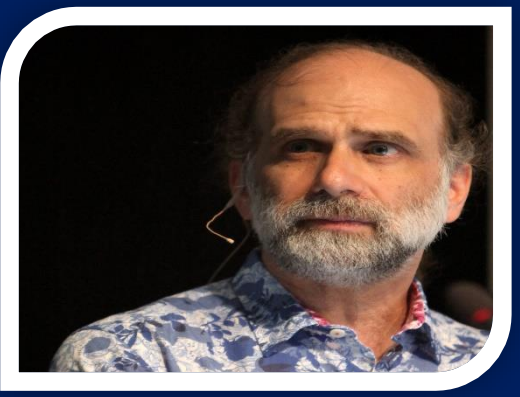
Firewalls



“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted; none of these measures address the weakest link in the security chain.”

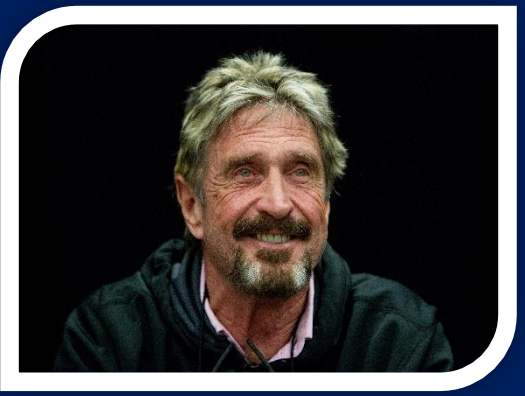
Kevin Mitnick

“People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.”



Bruce Schneier

“**Social engineering** has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more.”



John McAfee

Security

Social Engineering Attacks:

1. Phishing
2. Vishing and Smishing
3. Baiting
4. Pretexting
5. Tailgating

   ……..

Security

Network security:

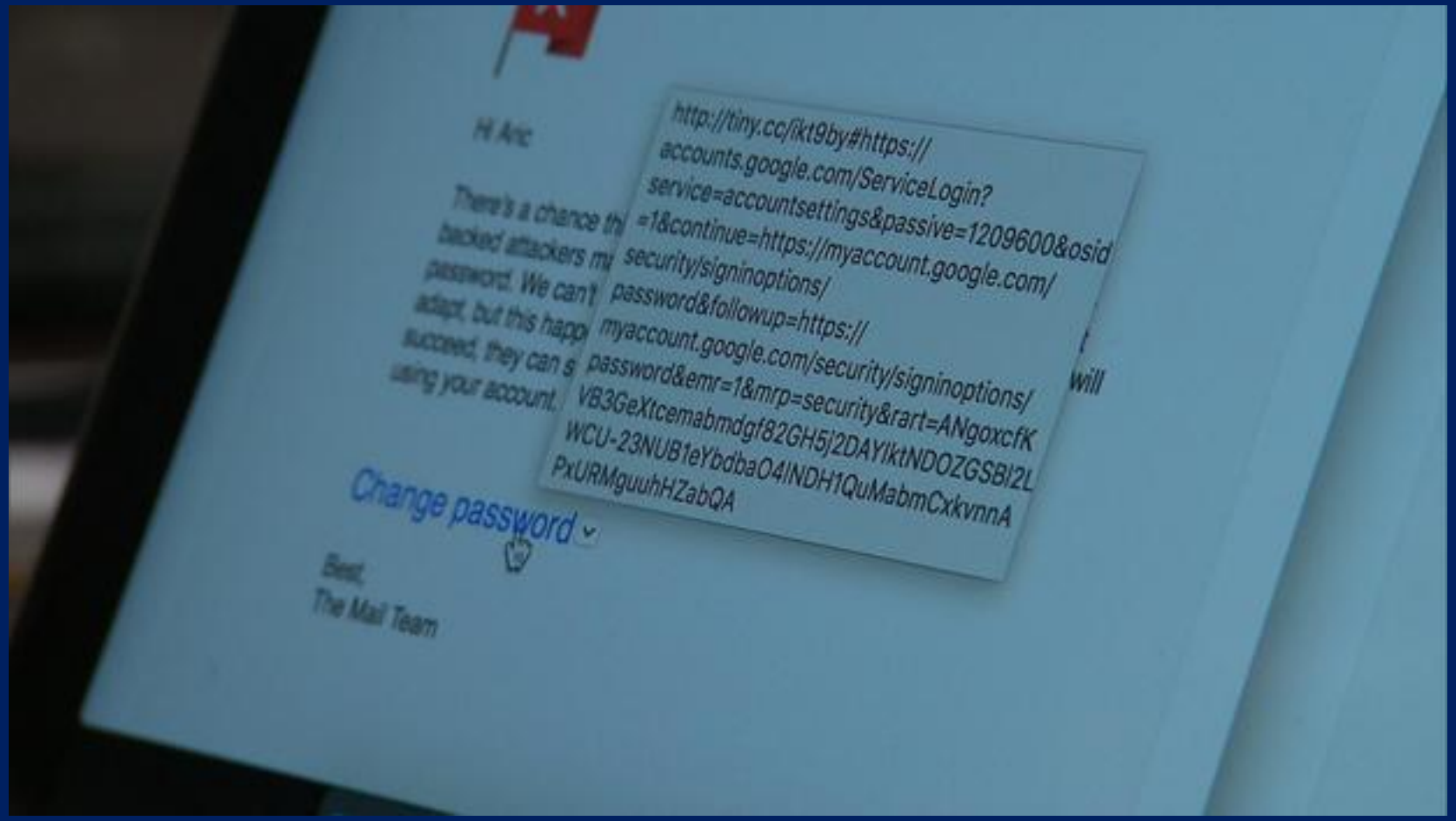
Phishing >> Fishing

- Phishing attacks are when an adversary sends a somewhat official-looking email
- May contain a link asking for a password or account info
- The email may contain an elaborate backstory “justifying” the request
- The malicious email is trying to obtain information from you

Security

Network security:

Phishing



Security

Social Engineering Attacks:

Trojan :

A trojan, sometimes called a trojan horse, is a program that either pretends to have, or is described as having, a set of useful or desirable features. But, it actually contains a damaging payload.

Security

Network security:

Malware

- Malware is short for malicious software, and is a general term used to describe software that is harmful or intrusive.
  - Viruses
  - Ransomware
  - Worms
  - Trojans

  Are all examples of malware.

Security

Network security:

Malware

- Malware is short for malicious software, and is a general term used to describe software that is harmful or intrusive.
  - Viruses:
    - A virus is a program that can replicate or make copies of itself
    - Viruses typically contain code that causes an unwanted, unexpected, and usually malicious event to occur after some time.
    - Viruses are often disguised as games or other types of legitimate software. They can also be disguised as images with clever marketing titles.

Security

Network security:

Malware

- Malware is short for malicious software, and is a general term used to describe software that is harmful or intrusive.
  - Viruses
  - Ransomware:
    - Ransomware is malware that locks your computer or mobile devices, and encrypts your documents, pictures, and other important files.
    - When the ransomware has encrypted your data, a demand is usually made for money. Sometimes, paying the ransom results in your files being decrypted. But this result isn't guaranteed.

Security

Network security:

Malware

- Malware is short for malicious software, and is a general term used to describe software that is harmful or intrusive.
  - Viruses
  - Ransomware
  - Worms:
    - A worm is a type of virus that spreads by creating copies of itself on other drives, computers, or networks.
    - Worms might send copies of themselves to other computers across network connections, through email, through an infected website, or through instant messaging systems.

Security

Network security:

Malware

- Malicious software can also be sent via email
- Software can be injected into your browser and your computer to erase your hard drive, make your computer send spam, or hold your data hostage
- Malware can ultimately do anything on your computer

THANK YOU
Rasha Abdeen