Applications of Information and Communication Technologies (AICT)

(CSC – 107)

Dr. Rizwan A Khan

*C*yber*S*ecurity

*S*ecurity & *P*rivacy

1. Privacy

- **Privacy** : Keeping your data secure or not allowing to be seen by un wanted person.

- Some of the devices that we use daily are vulnerable (unsecure) and have our private **data**:
  - Laptops
  - Desktops
  - Phones
  - .

- Data is a collection of files and are of course just 0s and 1s

SALIM HABIB UNIVERSITY
(FORMERLY BARRETT HODGSON UNIVERSITY)

1. Privacy : Data

- What kind of files do we have on our devices:
  - Images (vacations, home, office, friends ….)
  - Videos (home function, entertainment …)
  - Financial documents
  - Academic documents
  - Audio files
  - .

1. Privacy : Deleting files (vulnerabilities in files)

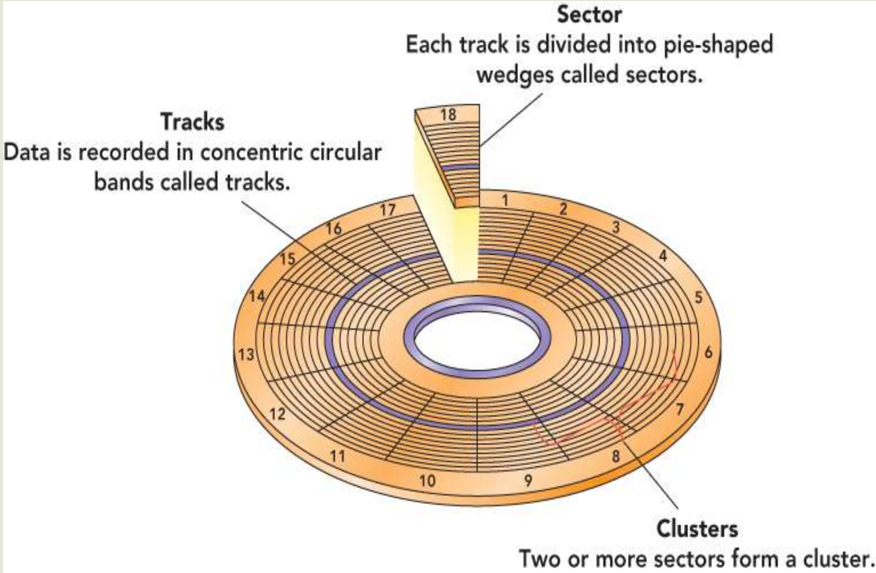
- You are cautious about data and anything that is not required you delete it.

- What happens when data is deleted?
  - Files are stored on HDD or SSD
  - They disappear once file is deleted
  - Where those 1s and 0s are gone?
  - Is there any mechanism to wipe them out from physical device?

1. Privacy : Deleting files (vulnerabilities in files)

- **Operating system** keeps track of data being stored on physical media.
- It records file address (location / lookup table)

File name	Physical Location (byte number)
myImage.jpg	123
myDocument.doc	890
…	…
…	…



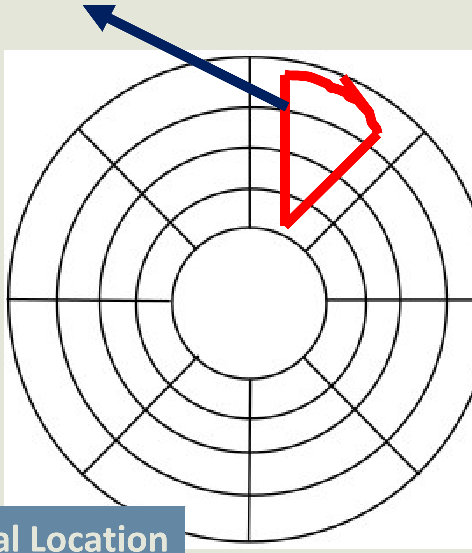
Sector
Each track is divided into pie-shaped wedges called sectors.

Tracks
Data is recorded in concentric circular bands called tracks.

Clusters
Two or more sectors form a cluster.

1. Privacy : Deleting files (vulnerabilities in files)

- What is it mean to delete file?
- Graphically file disappears.
- It may goes to trash can / bin. But file can be retrieved from bin.
- Ok you clear bin as well. What happens to those 1s and 0s?
- It turns out OS does nothing to file on physical media, it just deletes entry in location table
  - Data is not destroyed on physical disk


File to be deleted

File name	Physical Location (byte number)
~~myImage.jpg~~	~~123~~
myDocument.doc	890
…	…
…	…

1. Privacy : Deleting files (vulnerabilities in files)

- 1s and 0s are still on physical media, till it gets over written by some other data pattern.

- If there is some adversary with right software, data (theoretically) can still be recovered from HDD / SSD.

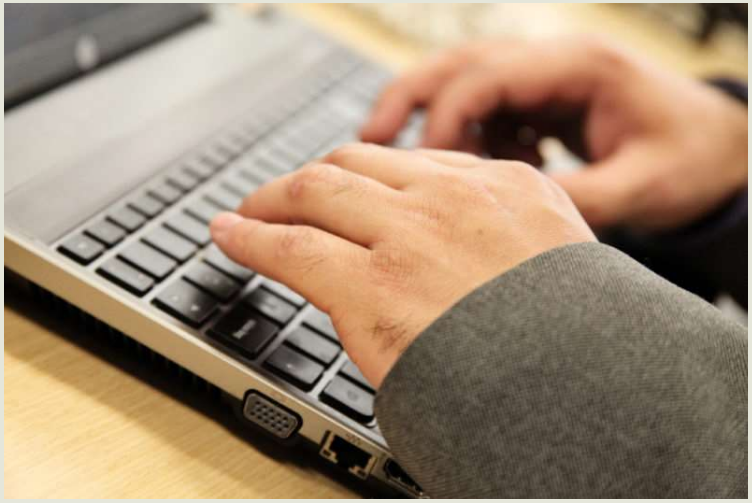
- What are **benefits and draw backs** of just forgetting entry in location table:
  - Can recover accidently deleted files. **(benefit)**
  - Its speed efficient to just delete entry from location / lookup table rather than wiping out data from each location of physical media. **(benefit)**
  - Adversary can recover private data. **(drawback)**

Internet Security

2. Vulnerabilities in browsing internet

- Internet users spend an average of **2 hours and 22 minutes** per day only on social networking in 2019[1]. And now?

- Time spent on internet surfing: **6 hours 49 minutes**[2]



- We use browsers for surfing:
  - Chrome
  - Edge
  - Firefox
  - Safari
  - .

[1] Review42

[2] Thenextweb.com

2. Vulnerabilities in browsing internet

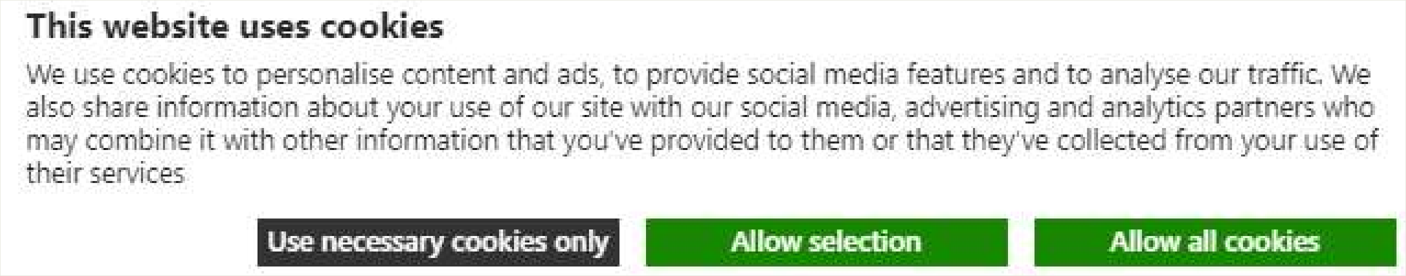
- All recent web browser uses **COOKIES**

- **Cookies** are text files with small pieces of data like
  - username
  - Password

- **HTTP cookies** are used to identify specific users and improve web browsing experience. No need to enter same information again and again.
  - **Example:** logging in Gmail account, social media accounts etc.

2.1 Cookies

- Web server puts these cookies on computers after user **authenticates** (more on this later) him/her self on that server.



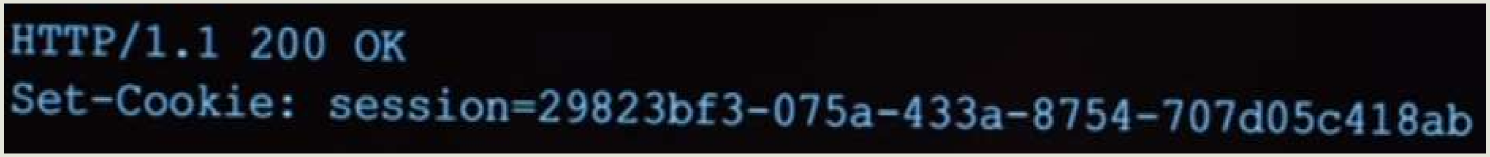
This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services

- That cookie usually doesn't contain username or password, instead it just contains big random number.
- When returned to that server again, the browser presents that cookie to remind specific user(<u>no need to enter my name, email ID, password, etc</u>.).

2.1 Cookies : HTTP header

- Data stored in a cookie is created by the server upon connection. This data is labeled with an ID unique for specific user.



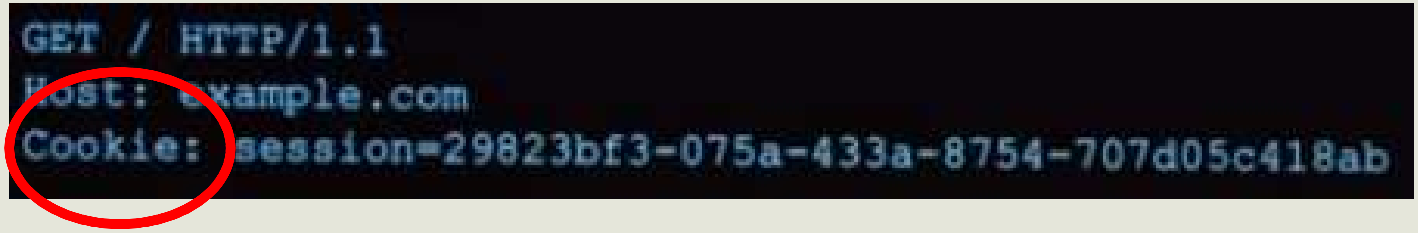
```
HTTP/1.1 200 OK
Set-Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

  - HTTP 200 OK → all is ok
  - Cookie → key : value (pair)

- Big random number **uniquely identifies specific user.** The same **number will never be sent** to another user.

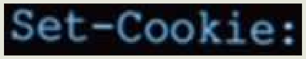
2.1 Cookies : HTTP header

- Browser on every subsequent webpage visit on “example.com” will sent something like this (HTTP header):



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

- **Is Cookie statement same as shown previously?**
- **Previously, it was**

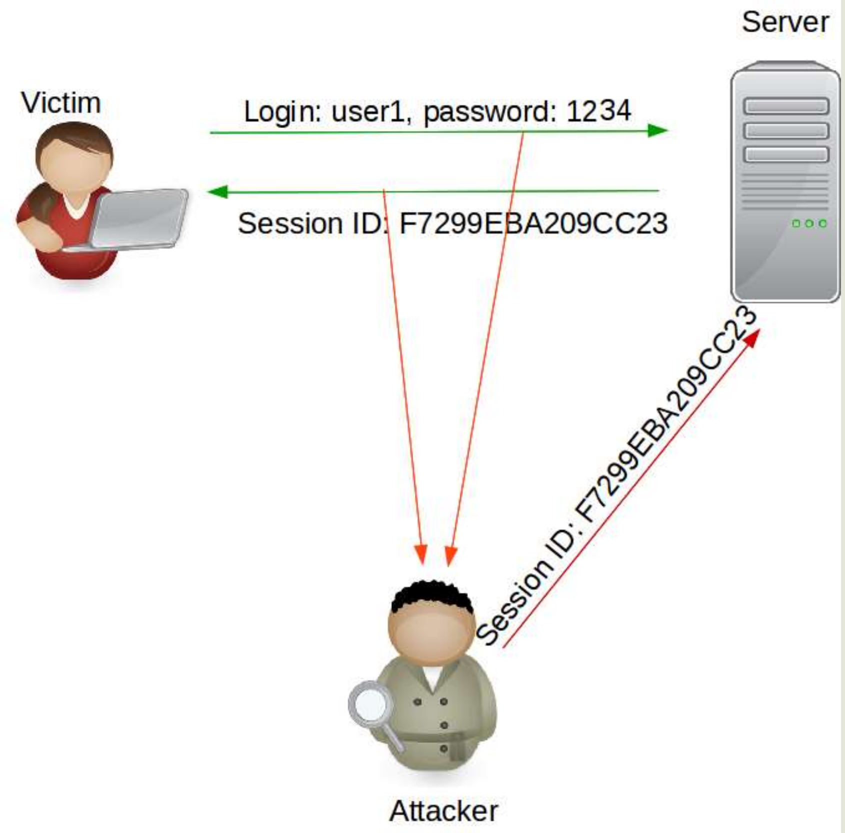


```
Set-Cookie:
```

- **Set-Cookie → sent by server to browser**

2.1 Cookies : session hijacking

- **Are cookies presenting threat to privacy?**
- **Consider:** Data is being communicated via wired or wireless medium and an adversary / hacker can sniff packets. What if an adversary sees this information?
  - In this situation, hacker can impersonate specific user by duplicating cookie value and can get access to private data (Gmail, Facebook, Outlook, etc.)
  - This is called **session hijacking attack**
  - **How to protect against such attack?**

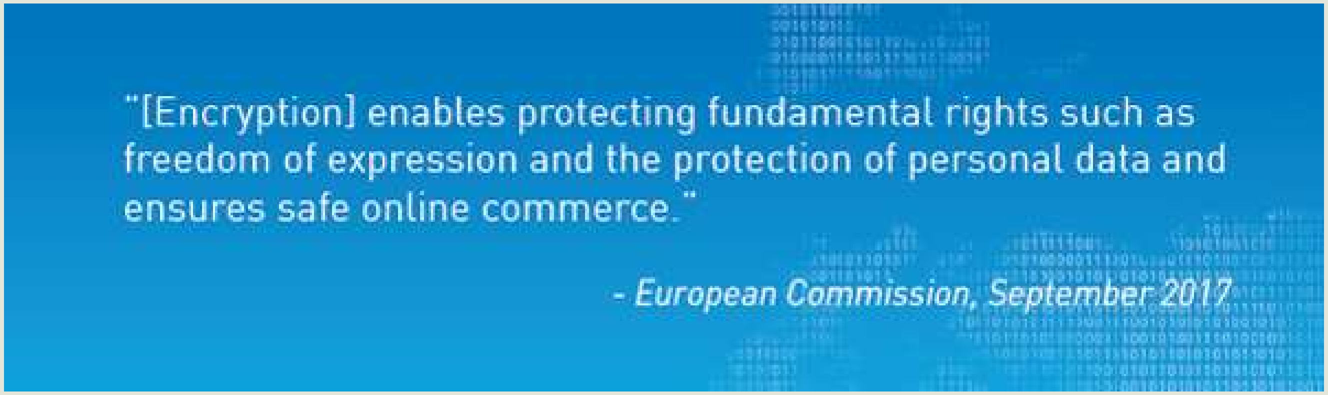

Server
Victim
Login: user1, password: 1234
Session ID: F7299EBA209CC23
Session ID: F7299EBA209CC23
Attacker

2.1 Cookies : Session hijacking attack

- **How to protect against session hijacking attack?**

1. **Delete cookies** (implications – browsing experience? Delete cookies from physical media?)
2. Usually most websites these days **encrypt** this information.

"**Encryption** is the method by which information is converted into secret code that hides the information's true meaning"

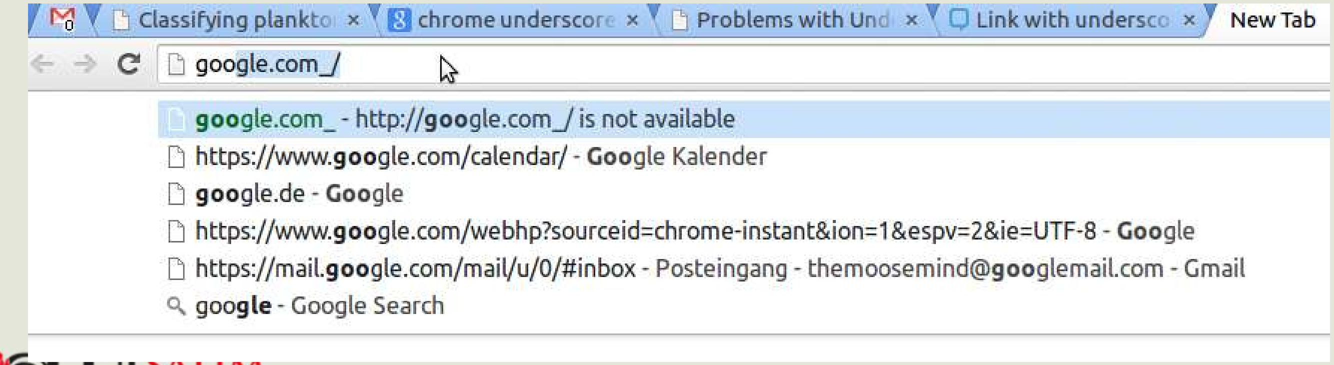


"[Encryption] enables protecting fundamental rights such as freedom of expression and the protection of personal data and ensures safe online commerce."

- European Commission, September 2017

2.2 Browsing history

- Another threat to privacy while browsing internet is stored **browsing history**
- Browsers are powerful, they do keep track of online activities. <u>They are beneficial</u> as:
    - User doesn’t need to keep typing same address
    - Type first few letters to search website that has the useful content (don’t need to search again)
    - Search browsing history to find webpage that has required information

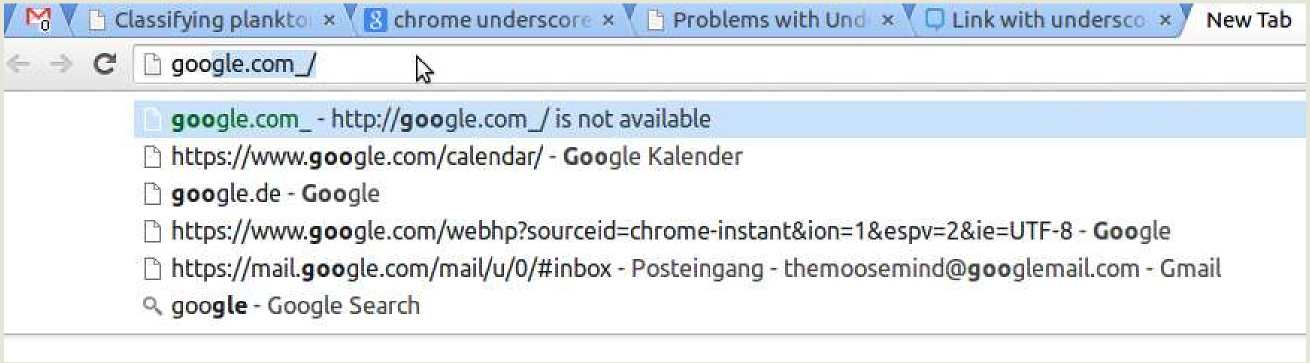


google.com_/

google.com_ - http://google.com_/ is not available
https://www.google.com/calendar/ - Google Kalender
google.de - Google
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8 - Google
https://mail.google.com/mail/u/0/#inbox - Posteingang - themoosemind@googlemail.com - Gmail
google - Google Search

2.2 Browsing history

- Another threat to privacy while browsing internet is stored **browsing history**
- Apart from benefits, they present privacy threat as well, as:
  - Some individual, if get a chance, can see online activities
  - Visible search history with date and time information



google.com_/

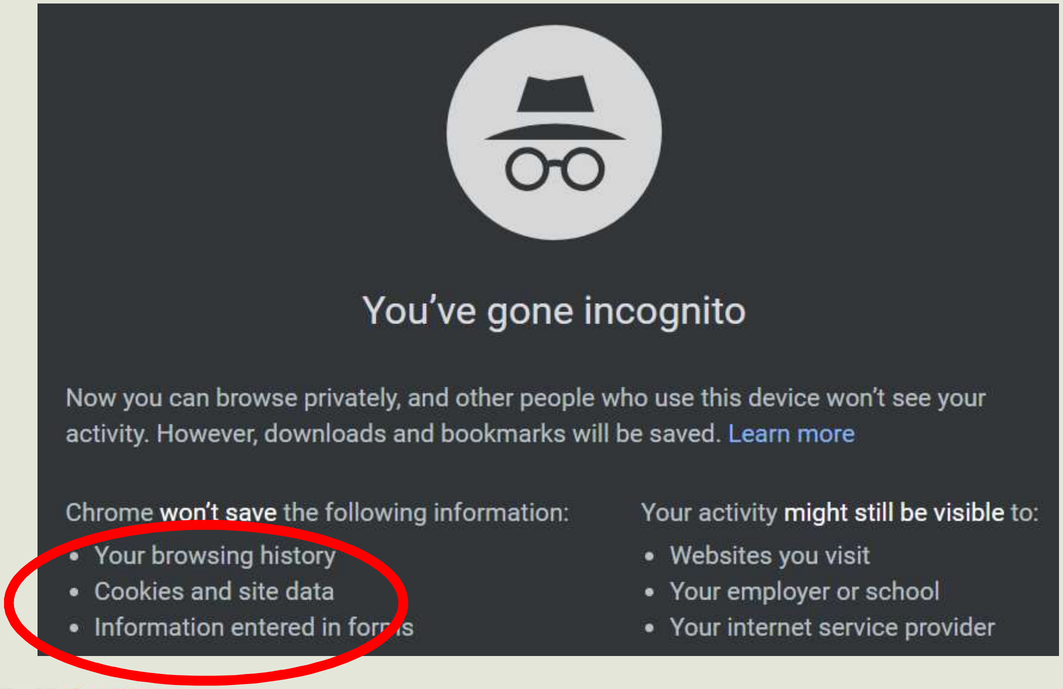
google.com_ - http://google.com_/ is not available
https://www.google.com/calendar/ - Google Kalender
google.de - Google
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8 - Google
https://mail.google.com/mail/u/0/#inbox - Posteingang - themoosemind@googlemail.com - Gmail
google - Google Search

2.2 Clearing browsing history

- Usually with **clearing browsing history, cookies are also deleted**.
- **Upside:**
  - Some individual, if get a chance, can't see online activities of other user.
  - Search history deleted.
  - Adversary can't get hold of session of authenticated user.
- **Downside:**
  - User need to login again to any website that was ever logged in (annoying browsing experience).
  - Need to type complete webpage addresses (annoying browsing experience).
  - Can't search information within browsed pages.

2.3 Private browsing

- Any alternative for not deleting cookies?
- Most of the web browser have private mode or incognito mode



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

2.3 Private browsing

- Incognito mode automatically deletes history and cookies without effecting what previously has been stored in browser i.e. cookies, browsing history etc.

- This mode is also used by tech people when they need to see current webpage as it ensures not to take information from browsing history (forgets history) and displays information from current process.

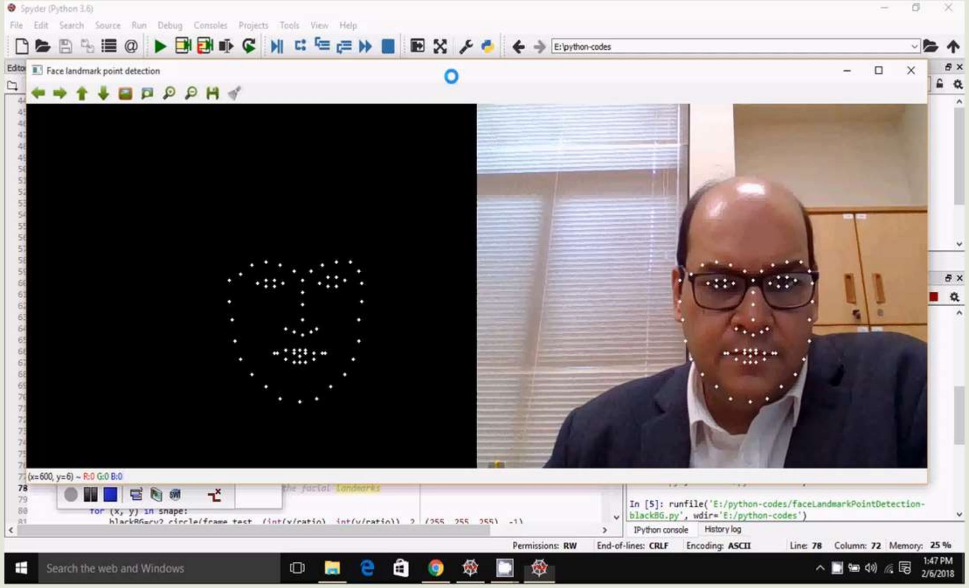
Authentication

*According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by **compromised, weak, and reused passwords**.*

3 Authentication

- All of the scenarios discussed in Section-2 **assumed that user is logged into system**.

- What type of security features **(essential to have)** are embed in our laptops, desktops, phones etc.?
  - Password
  - Passcode
  - Finger print
  - Face scan

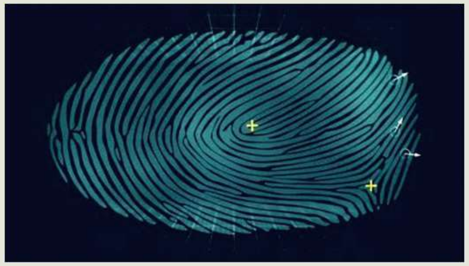

Spyder (Python 3.6)
File Edit Search Source Run Debug Consoles Projects Tools View Help
E:\python-codes
Face landmark point detection
IPython console
History log
Search the web and Windows

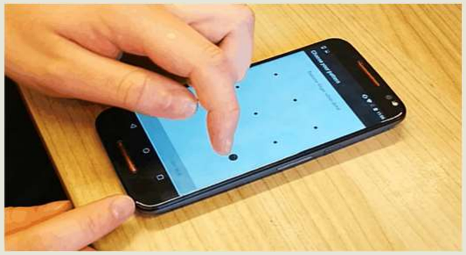
```
(x=600, y=6) ~ R:0 G:0 B:0
the facial landmarks
for (x, y) in shape:
    blackBG=cv2.circle(frame_test, (int(x/ratio), int(y/ratio)), 2, (255, 255, 255), -1)
```

```
In [5]: runfile('E:/python-codes/faceLandmarkPointDetection-blackBG.py', wdir='E:/python-codes')
```

Permissions: RW End-of-lines: CRLF Encoding: ASCII Line: 78 Column: 72 Memory: 25 %

1:47 PM 2/6/2018





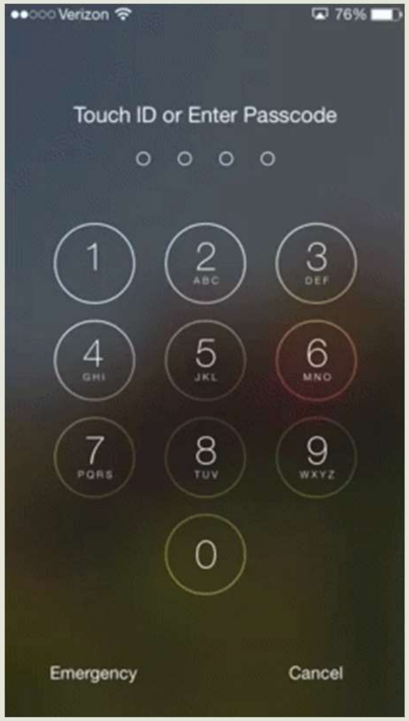
SALIM HABIB UNIVERSITY (FORMERLY BARRETT HODGSON UNIVERSITY)

3.1 Passwords

- Is password secure enough ?
- Usually how many digits are there in phone password?
  - Four possible position (each with 10 possible values, 0 – 9)

    ____ ____ ____ ____

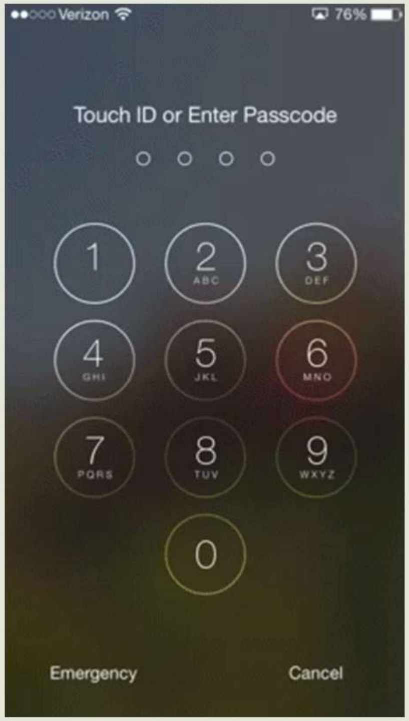
  - How many total combinations possible?
  - 10^4 (10,000) Possible values
    - **Value from 0000 – 9999**



- With **brute force search algorithm** it will be tedious to guess password, specially now devices put delays after “***X***” wrong entered passwords.

3.1 Passwords

- Putting delays after wrong entry is a good mechanism as **search space is small**, just 10,000 numbers to verify.
- Computers can verify these choices (10,000 passwords) pretty fast.
- Putting delays increases cost (**time complexity**) of searching. Thus, allowing legitimate user to take action (if required).
- Or are there more effective strategies to make password mechanisms more strong?


Touch ID or Enter Passcode

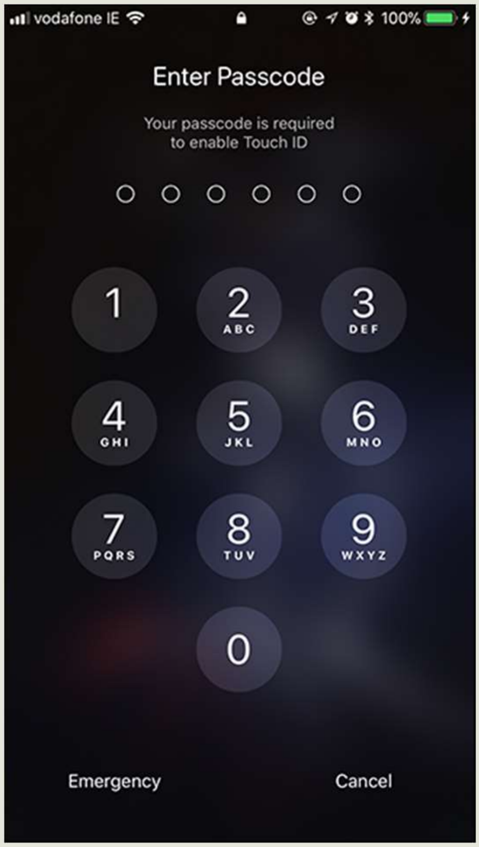
3.2 “Strong” Passwords

1. Or are there more effective strategies to make password mechanisms more strong?

- How about adding more digits in password. May be six (06)

  ____ ____ ____ ____ ____ ____

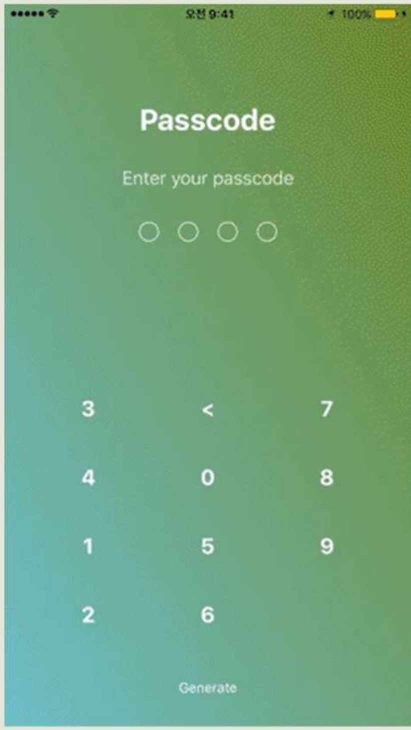
  - How many total combinations possible?
  - 10^6 (1 Million) Possible values


Enter Passcode

Your passcode is required to enable Touch ID

3.2 “Strong” Passwords

2. Or are there more effective strategies to make password mechanisms more strong?



- How about having Alpha-Numeric combination?
- Even with just four digit password, its complexity is large!

  ____ ____ ____ ____

  - How many total combinations possible?
- Now:
  - Each place can have **10** possible numeric choices + **26** capital alphabets + **26** small letter alphabets = **62** possible choice for one place.
  - **62^4 (more than 14 Million) Possible values**

3.2 “Strong” Passwords

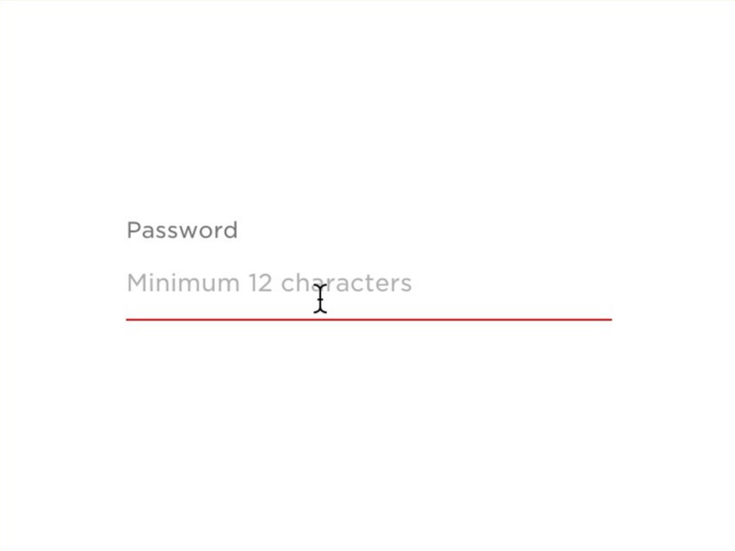
3. Or are there more effective strategies to make password mechanisms more strong?

- Why not have 6 or 12 or 20 or 100 character password (**no one can guess it**) ? It will be more secure?
  - Is it a good strategy?

- It’s **not a good strategy** for common user as:
  - Difficult to remember
  - Annoying to type long string again and again

3.2 “Strong” Passwords

- What is the best heuristic or rule of thumb?
- There is not necessarily **one fits all solution**. Depending on needs it may vary.
- Long passwords are generally better from security perspective, **but how long**?
  - As far as user can remember it!
  - And it should NOT be a popular word or phrase. Why?



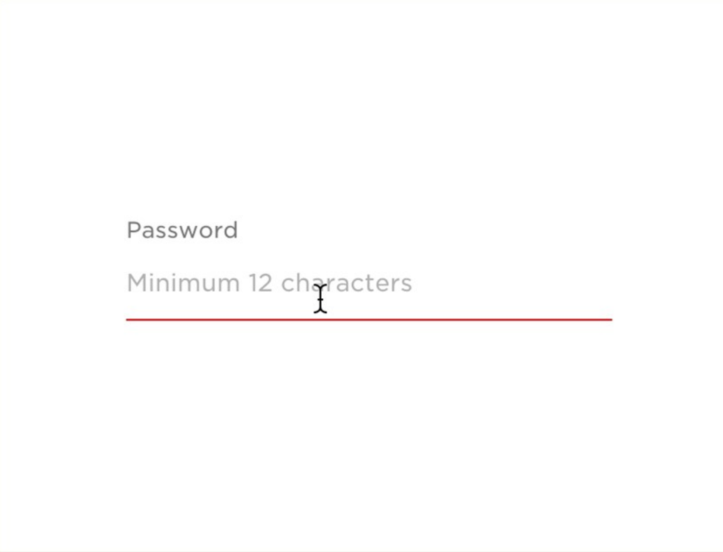
Password

Minimum 12 characters

3.2 “Strong” Passwords

- And it should NOT be a popular word or phrase. **Why**?

- Usually **hackers don’t apply brute force search, rather they try popular words and phrases** to try out.
  - They will not start by searching AAAA, AAAB, or 0000, 0001…. rather odds are they will **try something familiar words.**
  - For example:
    - If a password is “**password**” then it may break easily
    - Or password is “**123456**” then its vulnerable

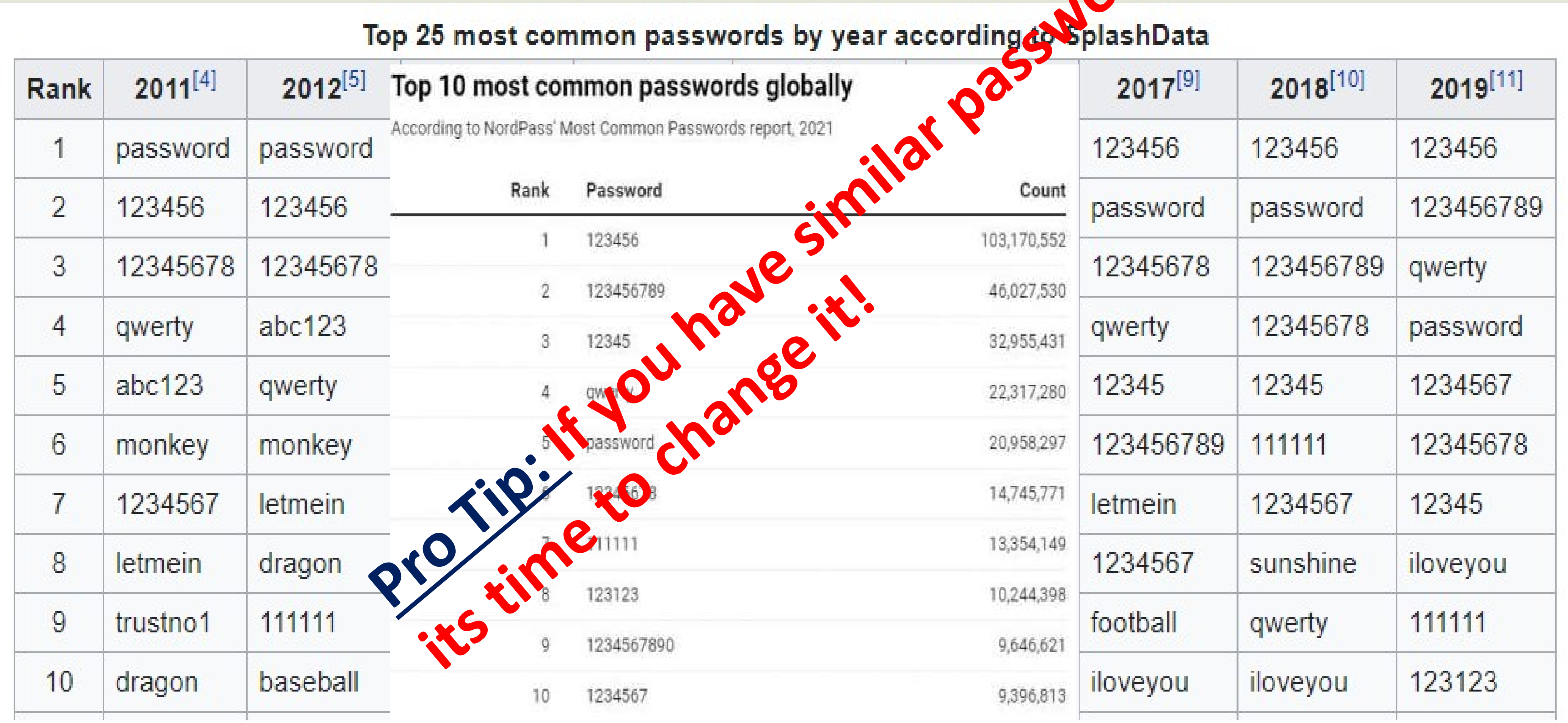


Password

Minimum 12 characters

3.2 “Strong” Passwords

- **Weak passwords are more common than we think:**



Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2017[9]	2018[10]	2019[11]
1	password	password	123456	123456	123456
2	123456	123456	password	password	123456789
3	12345678	12345678	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	password
5	abc123	qwerty	12345	12345	1234567
6	monkey	monkey	123456789	111111	12345678
7	1234567	letmein	letmein	1234567	12345
8	letmein	dragon	1234567	sunshine	iloveyou
9	trustno1	111111	football	qwerty	111111
10	dragon	baseball	iloveyou	iloveyou	123123

Top 10 most common passwords globally

According to NordPass' Most Common Passwords report, 2021

Rank	Password	Count
1	123456	103,170,552
2	123456789	46,027,530
3	12345	32,955,431
4	qwerty	22,317,280
5	password	20,958,297
6	12345678	14,745,771
7	111111	13,354,149
8	123123	10,244,398
9	1234567890	9,646,621
10	1234567	9,396,813

Pro Tip: If you have similar password, its time to change it!

3.2 “Strong” Passwords

- Weak passwords are more common than we think.
- Adversaries / hackers not only try these common words but rather they try words in dictionary i.e. Oxford or Merriam Webster dictionary.
  - **So don’t use English word as a password either**
- **Take away**
  - Use **completely random combination** (upper case, lower case letters) **of alpha-numeric** values as your passwords to secure different online accounts and computers.
  - Never use this (☺) to remember password----------------------→

SALIM HABIB UNIVERSITY
(FORMERLY BARRETT HODGSON UNIVERSITY)

Passwords

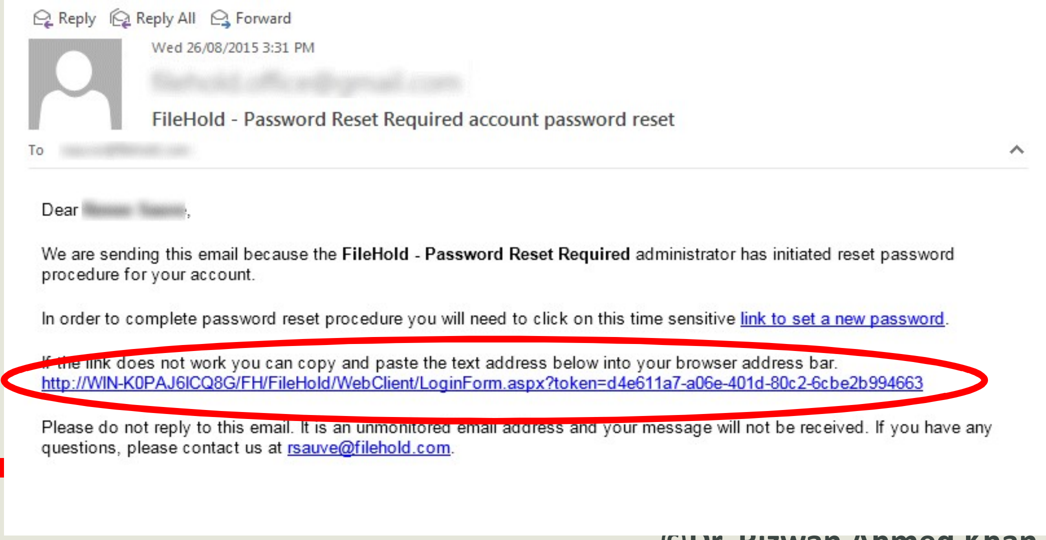
- Reading Assignment

Frequency of changing passwords. DOs and DON’Ts

3.3 Password Reset

- If you have **forgotten password**, webservers allows to reset password by sending email to email account that is used for registration.
- Thus, email account is used to authenticate user.
- Sometimes in such links **passwords are also sent**. If you are using such service, stop using it as good security practices are not implemented.
- Usually webservers **encrypt / hash** passwords, thus even there employ can't find password of any user.
  - **Facebook, Google, and Twitter,**

    all three tech giants have admitted to accidentally storing user passwords in plain, readable text



Wed 26/08/2015 3:31 PM

[redacted]

FileHold - Password Reset Required account password reset

To [redacted]

Dear [redacted],

We are sending this email because the **FileHold - Password Reset Required** administrator has initiated reset password procedure for your account.

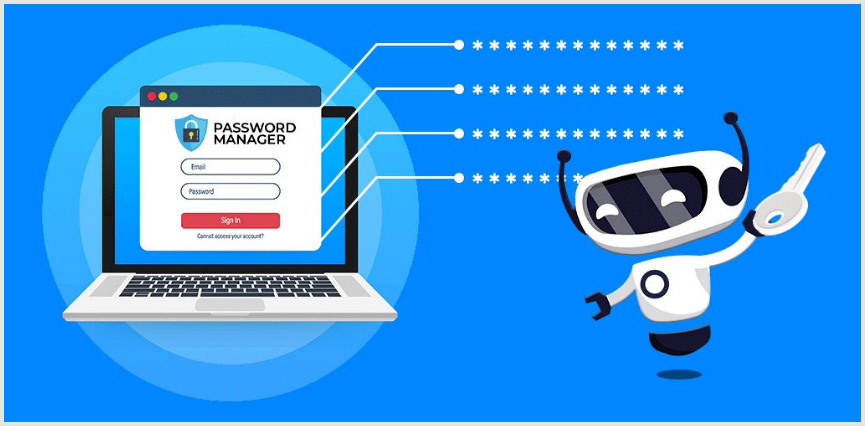
In order to complete password reset procedure you will need to click on this time sensitive link to set a new password.

If the link does not work you can copy and paste the text address below into your browser address bar.
http://WIN-K0PAJ6ICQ8G/FH/FileHold/WebClient/LoginForm.aspx?token=d4e611a7-a06e-401d-80c2-6cbe2b994663

Please do not reply to this email. It is an unmonitored email address and your message will not be received. If you have any questions, please contact us at rsauve@filehold.com.

3.4 Password Manager

- A **password manager** is “a software application designed to:
  - store and manage online credentials.
  - It also generates passwords.
  - Usually, these passwords are stored in an encrypted database and locked behind a master password.”



3.4 Password Manager

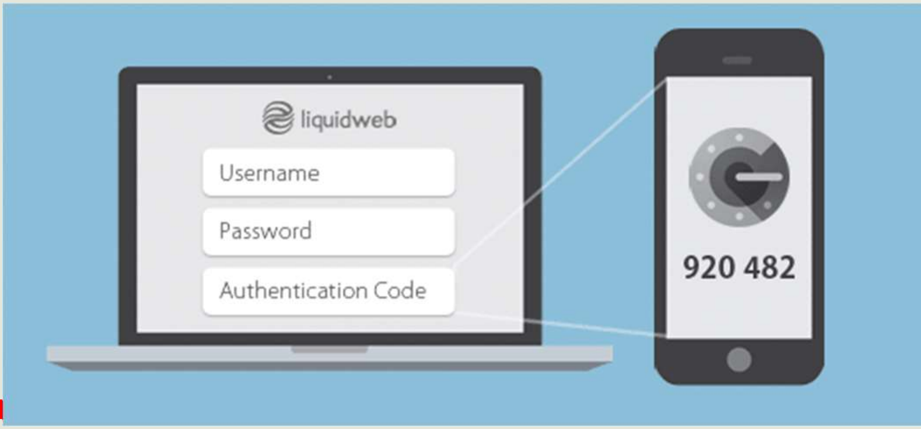
- Benefits of using password manager:
  - Don't have to **memorize** all your passwords anymore
  - Can **auto-generate** highly secure passwords
  - Can alert you to a **phishing (discussion in few slides)** site
  - Many password managers **sync across different operating systems** (Windows at home and Mac at office)

- Downside of using password manager:
  - If you forget password of password manager ….
  - If password manager database got hacked (happened but all passwords were encrypted)

SALIM HABIB UNIVERSITY
(FORMERLY BARRETT HODGSON UNIVERSITY)

3.5 Two-Factor Authentication

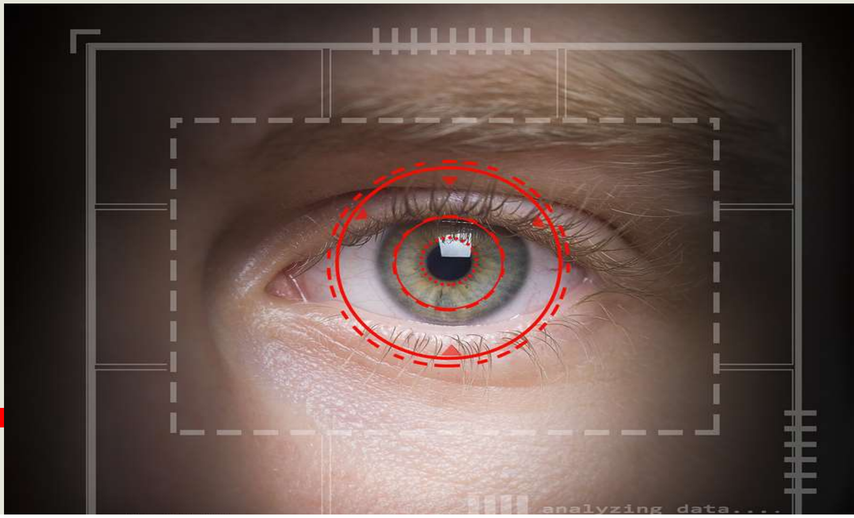
- When you login to Facebook or Outlook, their server just asks password.
- As we know passwords can be stolen, hacked etc.
- To make authentication process more secure, **another factor is added** to password-only authentication system, it is known as **two-factor authentication (2FA).**
- Usually banks are supporting 2FA or Multi-Factor Authentication



SALIM HABIB UNIVERSITY (FORMERLY BARRETT HODGSON UNIVERSITY)

3.5 Two-Factor Authentication

- To make authentication process more secure, **another factor is added** to password-only authentication system, it is known as **two-factor authentication (2FA).**
- There are three basic factors that can be used for authentication:
  - **Something you know** (Maybe a password, secret, **one time password (OTP)** or PIN)
  - **Something you have** (Your mobile phone or another device such as a key)
  - **Something you are** (Biometrics such as a retina or fingerprint)



3.5 Two-Factor Authentication

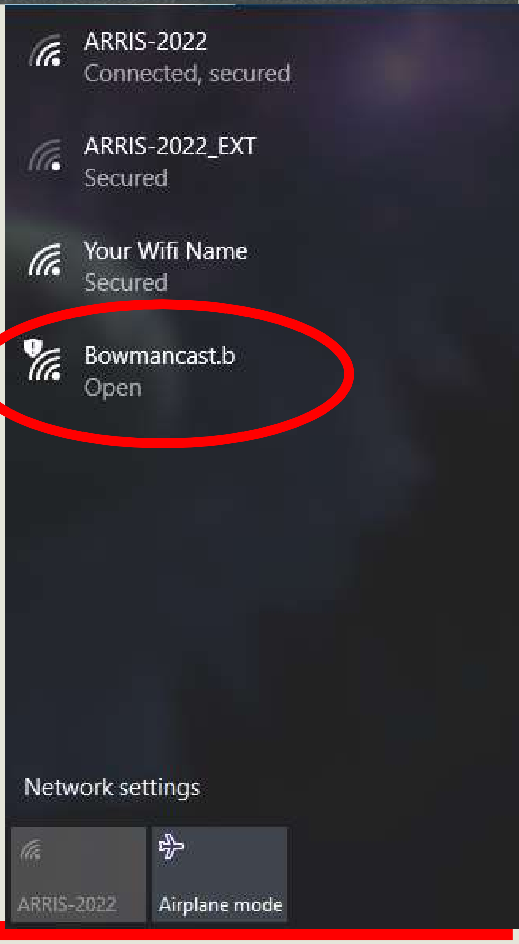
- Today, most services focused on improving the security of the users and their data have adopted 2FA as a standard method for authentication.
- This is mainly because **2FA ensures that even if one of the factors have been compromised or leaked, the other factor keeps hackers/criminals from breaking into your account**, thereby minimizing the risk of data theft.
- Here are the **other benefits** of using 2FA:
    - Provides **additional layer of security**
    - **Minimizes risk** of data and identity theft
    - Reduces operational and security cost

Network Security

https://cryptii.com/pipes/caesar-cipher

4 Network Security

- Up till now we have discussed issues with browsing internet and authentication, what about network it self?
- Usually networks we use these days are **wireless.**
- This is how list of available wireless networks looks on Windows.
- **Anything that seems to be not so secure?**
- Usually these free Wi-Fi networks are available in hotel, restaurant, parks etc.
  - Or sometimes once connected they (open Wi-Fi networks) ask to pay charges.
  - **By definition, such open Wi-Fi networks are not secure.**



ARRIS-2022
Connected, secured

ARRIS-2022_EXT
Secured

Your Wifi Name
Secured

Bowmancast.b
Open

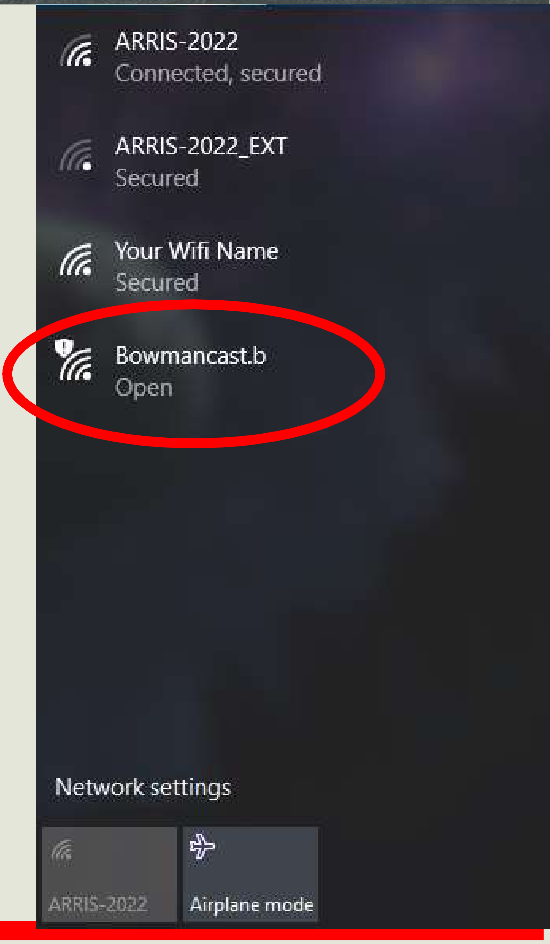
Network settings

ARRIS-2022

Airplane mode

4 Network Security

- Usually these free Wi-Fi networks are available in hotel, restaurant, parks etc.
    - Or sometimes once connected they (open Wi-Fi networks) ask to pay charges.
    - **By definition, such open Wi-Fi networks are not secure.**
    - Its not encrypted
    - If you are visiting a website (http://), that is not using **secure connection** (**httpS://**) then its vulnerable.
- Theoretically, if you are using unsecure network that is not using encryption by default, data transmitted can be sniffed / seen by an adversary.



ARRIS-2022
Connected, secured

ARRIS-2022_EXT
Secured

Your Wifi Name
Secured

Bowmancast.b
Open

4.1 Virtual Private Network (VPN)

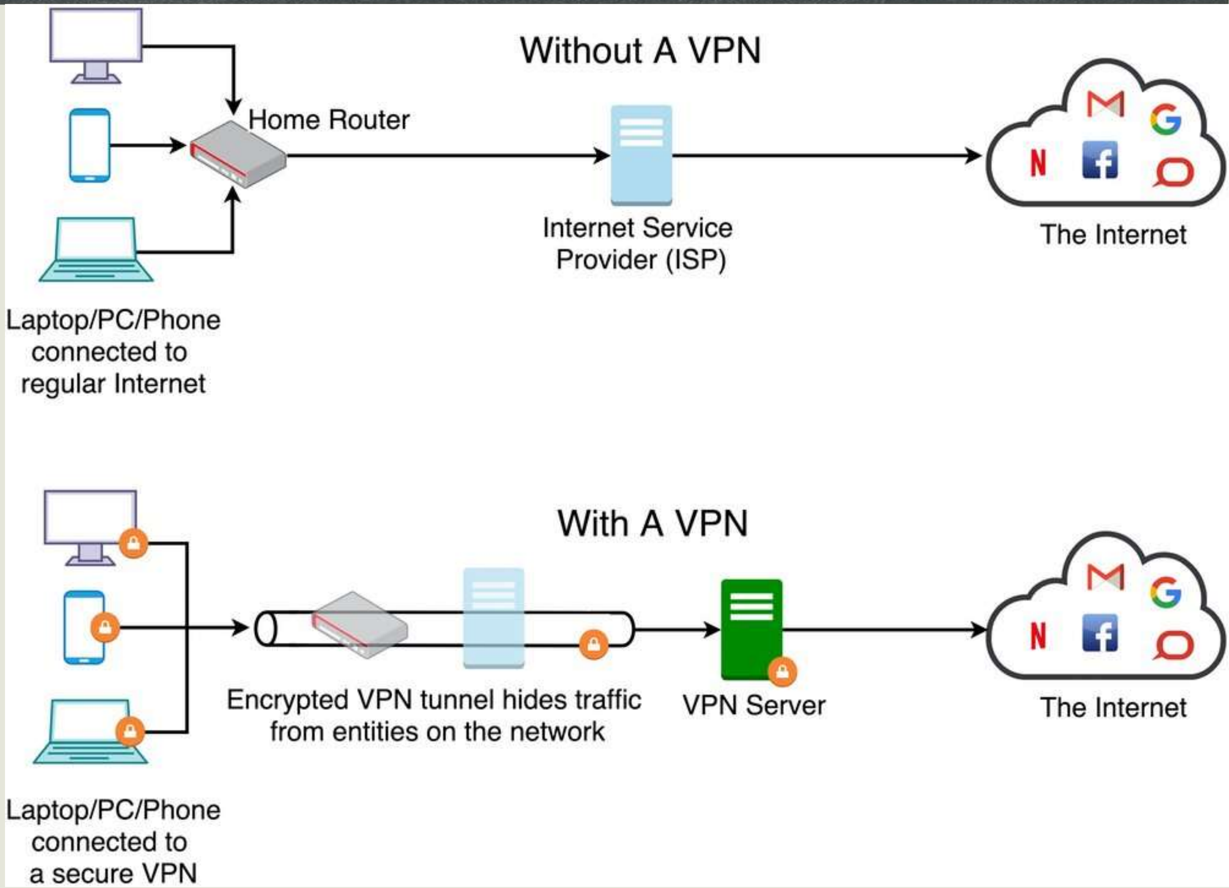
- How to mitigate issue of using unsecure network?
  1. Don’t use that network, if possible
  2. Use VPN.

- A **VPN gives you online privacy and anonymity** by creating a private network from a public internet connection.
- **VPN services establish secure and encrypted connections** to provide greater privacy than even a secured Wi-Fi hotspot

4.1 Virtual Private Network (VPN)

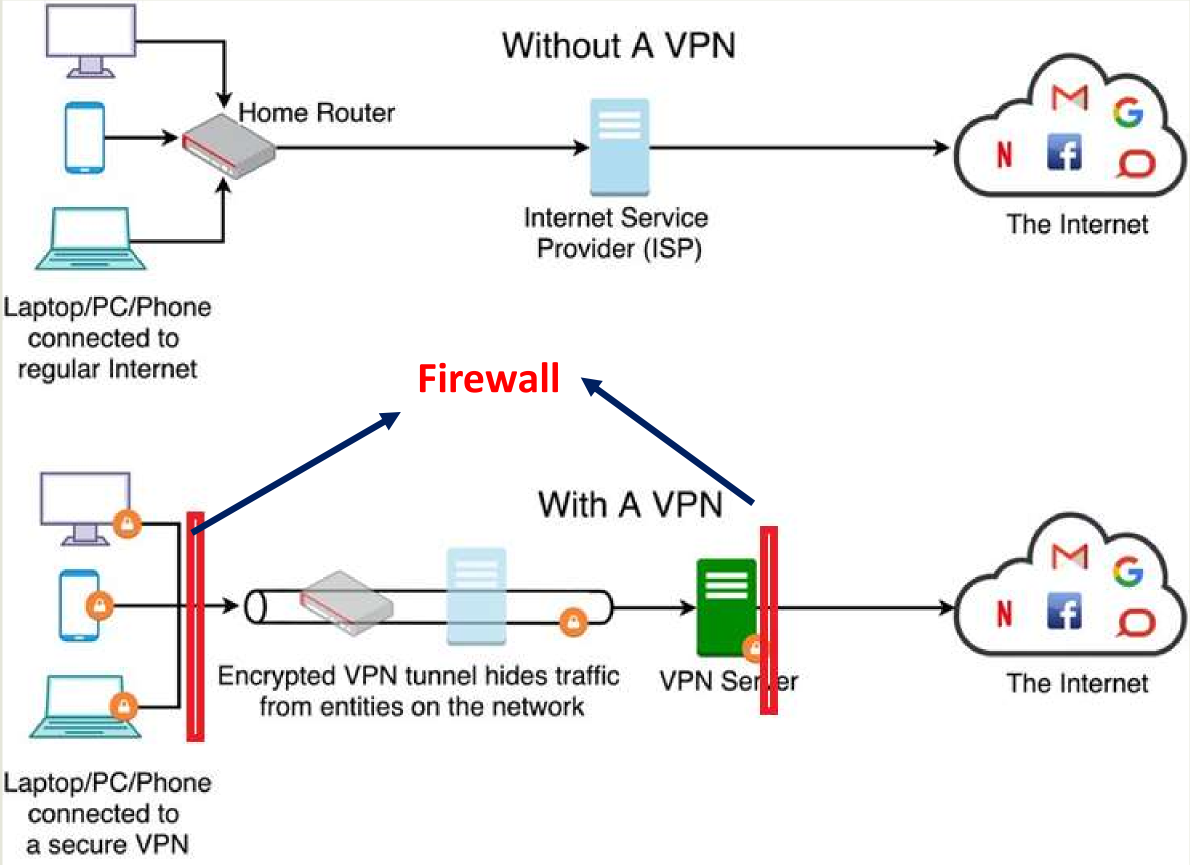
- VPNs can be provided by companies you work for or Universities or you can get third party VPN by paying subscription charges.

- Downside:
  - Data encryption would take some time, so you might encounter some delays


Without A VPN
Home Router
Internet Service Provider (ISP)
The Internet
Laptop/PC/Phone connected to regular Internet
With A VPN
Encrypted VPN tunnel hides traffic from entities on the network
VPN Server
The Internet
Laptop/PC/Phone connected to a secure VPN

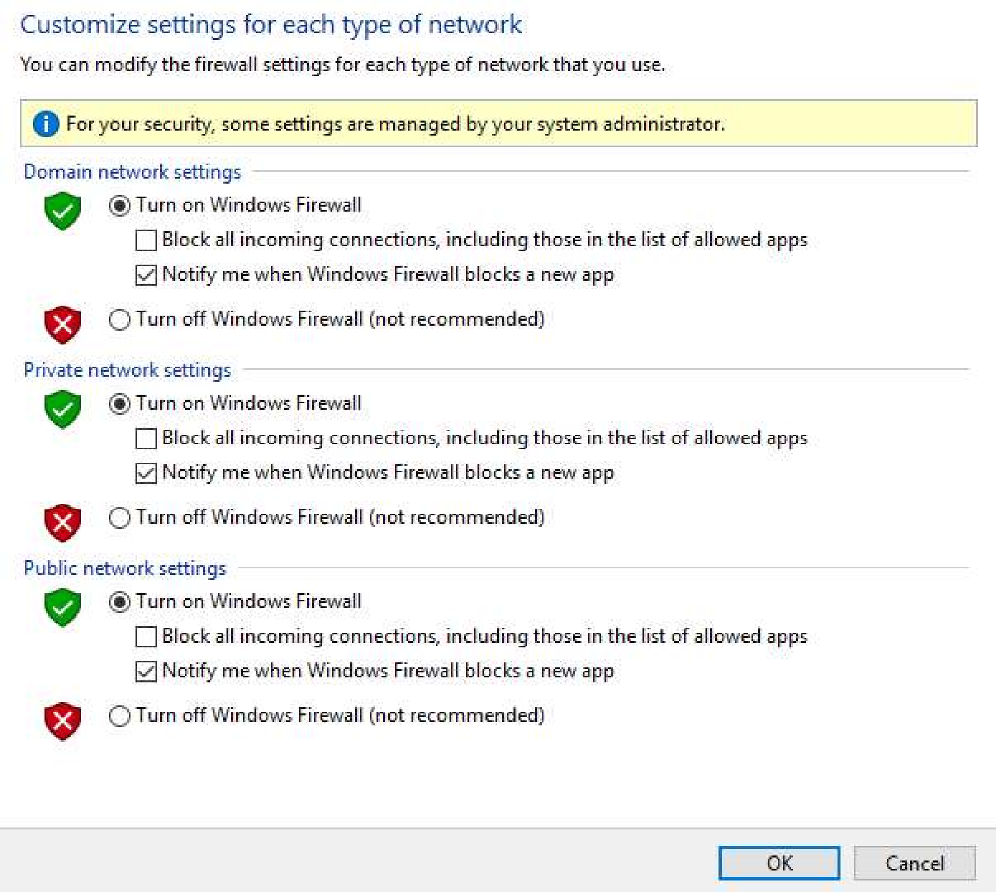
4.2 Firewalls

- Servers and even PC have special device or software that is called **firewalls.**
- A firewall is a **network security system** that:
  - monitors and controls incoming and outgoing network traffic based on predetermined security rules
  - Prevent unauthorized internet users from accessing private networks connected to the internet


Without A VPN
Home Router
Internet Service Provider (ISP)
The Internet
Laptop/PC/Phone connected to regular Internet
Firewall
With A VPN
Encrypted VPN tunnel hides traffic from entities on the network
VPN Server
The Internet
Laptop/PC/Phone connected to a secure VPN

4.2 Firewalls

- A firewall is a **network security system** that:
  - monitors and controls incoming and outgoing network traffic based on predetermined security rules
  - Prevent unauthorized internet users from accessing private networks connected to the internet
  - In Windows and mac OS, firewalls are built into the operating system.
  - Make sure you have **enabled it your system** if you are using unencrypted public network



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

For your security, some settings are managed by your system administrator.

Domain network settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Private network settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

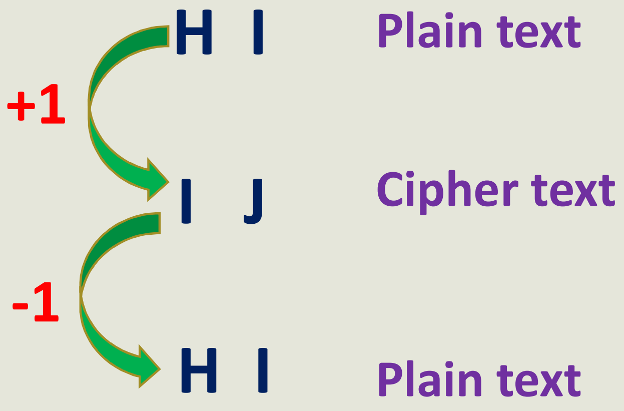
4.3 Encryption

- We used word “Encryption” in this lecture, but **what Encryption is**?
- Encryption is the “process of converting Information or data into a code“, so that even if it gets landed in wrong hand it doesn’t convey the message.
- **Example:**
  - Suppose I want to send message “**H I**”, but I don’t want any one to know what I am sending. Instead I send “**I J**”.
  - Now, even someone reads it would not understand it
  - Why I send “I J”? **Pretty trivial (adding +1 in alphabets)**, but it attempts to make it secure
  - **But, what receiver needs to know to de-crypt it?**
    - **Number of places alphabets are moved**

SALIM HABIB UNIVERSITY
(FORMERLY BARRETT HODGSON UNIVERSITY)

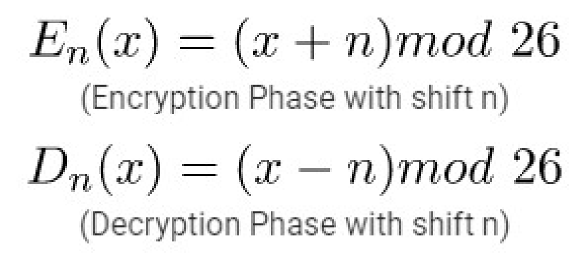
4.3 Encryption

- This is an example **of Caesar Cipher, or rotation Cipher** Encryption.
- We can make it interesting by rotating two places or fifteen places.
- Is it hard to guess?
  - No, just by brute force search it can be decrypted. There are only 26 choices to verify!
  - Secondly, receiver needs to know key in advance. How to securely transfer that in unsecured environment? (**Drawback**)



4.3 Encryption : Cesar Cipher

- Cesar Cipher is given mathematically by:

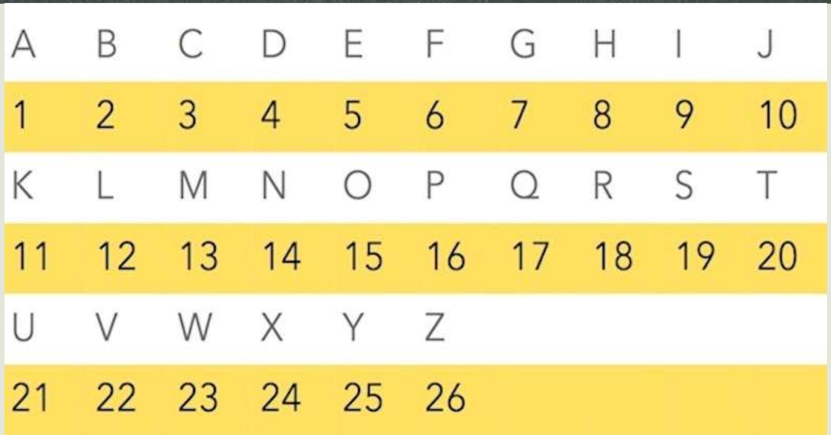


$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)



A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26				

- Cesar Cipher is **Symmetric Encryption**, meaning sender and receiver use same key.
- Cesar Cipher is not used these days as there is no mechanism to establish secure communication to transfer key.
- **Decode**, by brute force search algorithm:
  - TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB

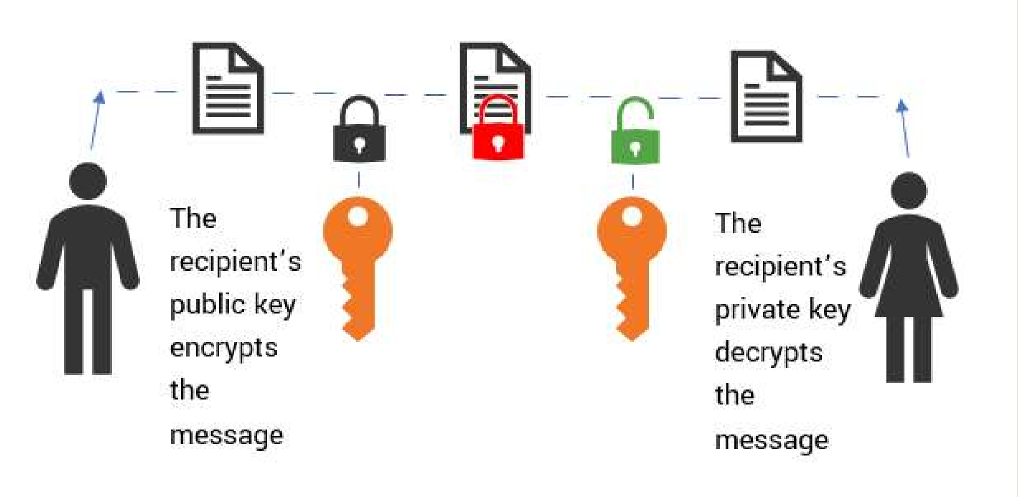
https://www.dcode.fr/caesar-cipher

4.3 Encryption : Public Key Encryption

- To address the issues of single key encryption, public key encryption is introduced and is widely used.

- **Public-key cryptography**, or **Asymmetric Cryptography**, is a encryption system that uses pairs of keys:
  - public keys, which may be disseminated widely, and
  - private keys, which are known only to the owner

- There is mathematical relationship b/w these two keys


The recipient's public key encrypts the message
The recipient's private key decrypts the message

4.3 Encryption : Video

- Look out for these concepts in the video presented in next slide:
  1. What is Key?
  2. Problem with Cesar Cipher
  3. How to make more secure messaging (moving ahead of Cesar Cipher)
  4. x digit encryption, with x=10, search space will increase to 10 Billion choices
  5. How to make encryption more harder (too many possibilities / choices)
  6. Symmetric and Asymmetric Keys
  7. Mores law implication
  8. Public Key Encryption

4.3 Encryption : Video

Social Engineering

*Even if **all the data is encrypted and connection is secure**, an adversary may try to manipulate **user online behavior** and get user trapped.*

Social Engineering

- **The act of manipulating people into divulging confidential information or performing actions for malicious purposes.**
- **Humans are the weakest link in security system**

- Exploits human psychology (trust, fear, urgency).
- Circumvents technical security systems.
- Relies on a lack of awareness among individuals.

Statistics:

- Over 90% of cyberattacks begin with a phishing email.

Social Engineering

- Attacker usually play with human trait of
  - Greed
  - Fear
  - Or both

- In order to get
  - Use Credentials
  - Control of the system, or
  - Intellectual property

Social Engineering

- The act of manipulating people into divulging confidential information or performing actions for malicious purposes.

Common Methods:

- **Phishing** (trick people into sharing sensitive information)
- **Pretexting** (fabricates a scenario or pretends to be someone else to manipulate a target into revealing confidential information.)
- **Baiting** (attackers use the promise of something enticing i.e. a reward or free item to trick victims)
- **Tailgating** (sneaks into a secure area by following someone else, by polite social gestures)
- **Quid Pro Quo** (offers something in exchange for sensitive information or access)

Social Engineering

Real-world Examples

- Phishing: Fake bank email asking for login details.
- Pretexting: Caller impersonating IT support to gain credentials.
- Baiting: USB drive left in a public space with malicious software.

5.1 Phishing

- **Phishing** is a method (cyber attack) of trying to gather personal information using deceptive e-mails and websites.

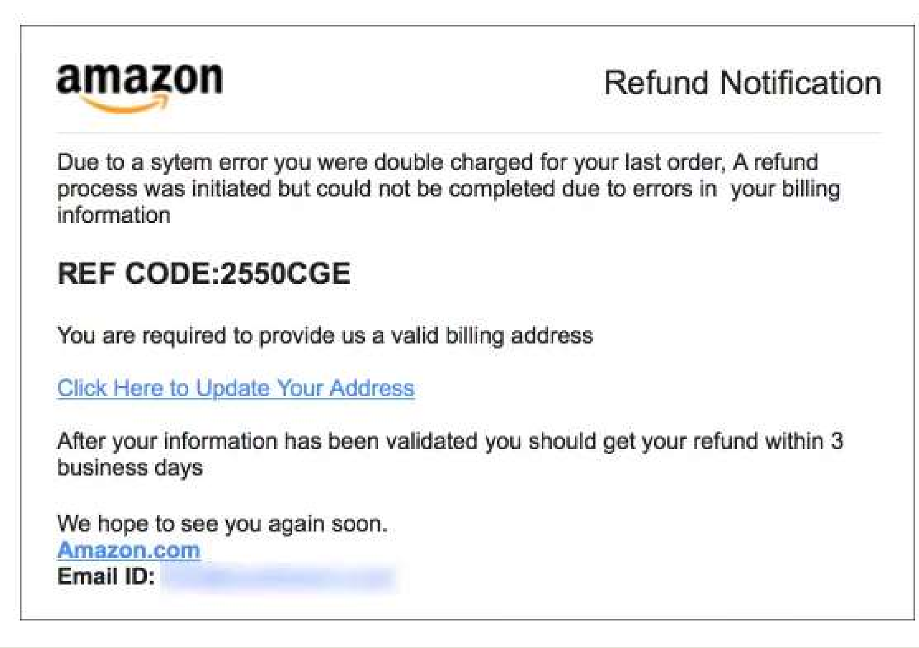
- It's one of the oldest types of cyberattacks, dating back to the 1990s, **but still widely employed by the adversaries.**

- The goal is to trick the email recipient into **believing that the message is legitimate and something they want or need**
  - a request from their bank,
  - an email from website account that is used,
  - or a note from someone in their company,
  - and to click a link or download an attachment.

5.1 Phishing

- Usually such “malicious” email asks user to click on certain link
  - To click to reset password
  - To click to claim your reward
  - To click to update personal information
  - .

- Such **email text** explains that it’s a standard security procedure or after update in security terms you need to update personal information etc.



amazon Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

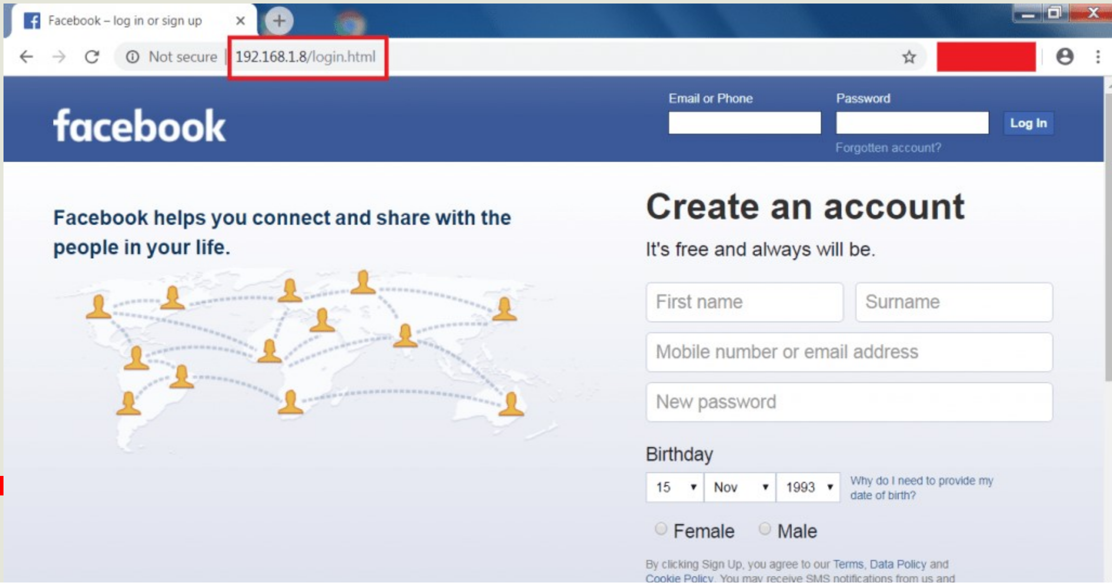
Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID: [redacted]

5.1 Phishing

- Phishing emails trick user to click on a link for “whatever” reason but usually websites that are linked in the email text are **fictitious or fake or completely random website** pops up.
- Sometimes websites are copies (just copy HTML code) of some famous website and trick user to enter user ID and password.



Facebook – log in or sign up ×

Not secure | 192.168.1.8/login.html [redacted]

facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

New password

Birthday

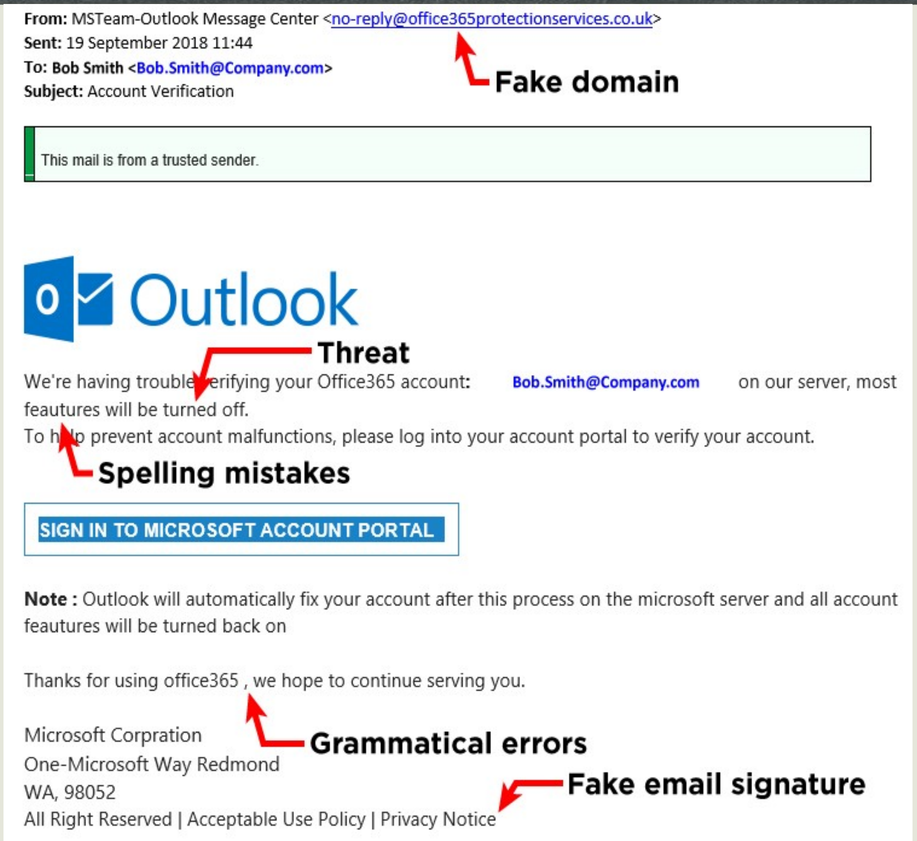
15 ▾ | Nov ▾ | 1993 ▾ Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and

5.1 Phishing

- Save yourself by such attacks by:
  - **Distrust:** Don't trust email that asks to click on a link. Even it seems legitimate, its better to go to that server / website yourself that links points to but don't click on the link.
  - **Verify sender email Address**: Sketchy looking email ID are big clue too



From: MSTeam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

This mail is from a trusted sender.

Outlook

We're having trouble verifying your Office365 account: **Bob.Smith@Company.com** on our server, most feautures will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

SIGN IN TO MICROSOFT ACCOUNT PORTAL

Note : Outlook will automatically fix your account after this process on the microsoft server and all account feautures will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corpration
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

Fake domain

Threat

Spelling mistakes

Grammatical errors

Fake email signature

5.2 Malware (Malicious Software)

- With phishing attack , user's following attributes may be compromised
  - ID
  - Passwords
  - Personal information
  - Bank account details
  - .
- But sometimes **phishing link may lead to server that will infect computer with malware**.
- **Malware** is any software intentionally designed to cause damage to a computer.

5.2 Malware

- A wide variety of malware types exist, including
  - Computer viruses
  - Worms
  - Trojan horses
  - Ransomware
  - Spyware
  - Adware
  - Rogue software
  - Scareware

5.2 Malware

- **Ransomware** is a type of malware from crypto-virology that threatens to publish the victim's data or perpetually block access to it unless a **ransom** is paid.
- **Ransomware attacks** are typically carried out using a **Trojan** that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.
  - There were **181.5 million ransomware attacks** in the first six months of 2018.

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

NEXT

Precautions

Verify the identity of the requester through independent channels.

- **Avoid clicking on suspicious links** or downloading unknown attachments.
- **Educate and train** employees on recognizing social engineering tactics.
- **Implement multi-factor authentication (MFA)** for sensitive accounts.