Malicious
Software Analysis

Computer Security

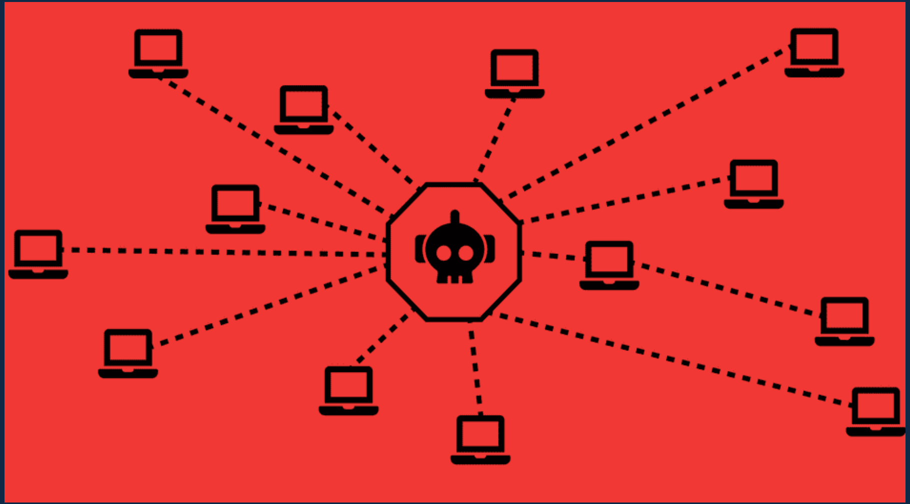
How the computer become more secure?

The weakest chain in cybersecurity is the human.

Be Careful

Be careful when performing operations on the computer.

E-mails (phishing attack)
unknown addresses, unknown software (trojen horse, spyware, backdoor, botnet, …)



Install updates and use the latest software

Operating system updates

Anti-virus program updates (signature based working)

Latest sofware and open the updates

The defensive side has to cover all the holes on the wall.
It is enough if the attacker finds only one hole on the wall.

Passwords

Passwords at the appropriate level for the service used should be determined.

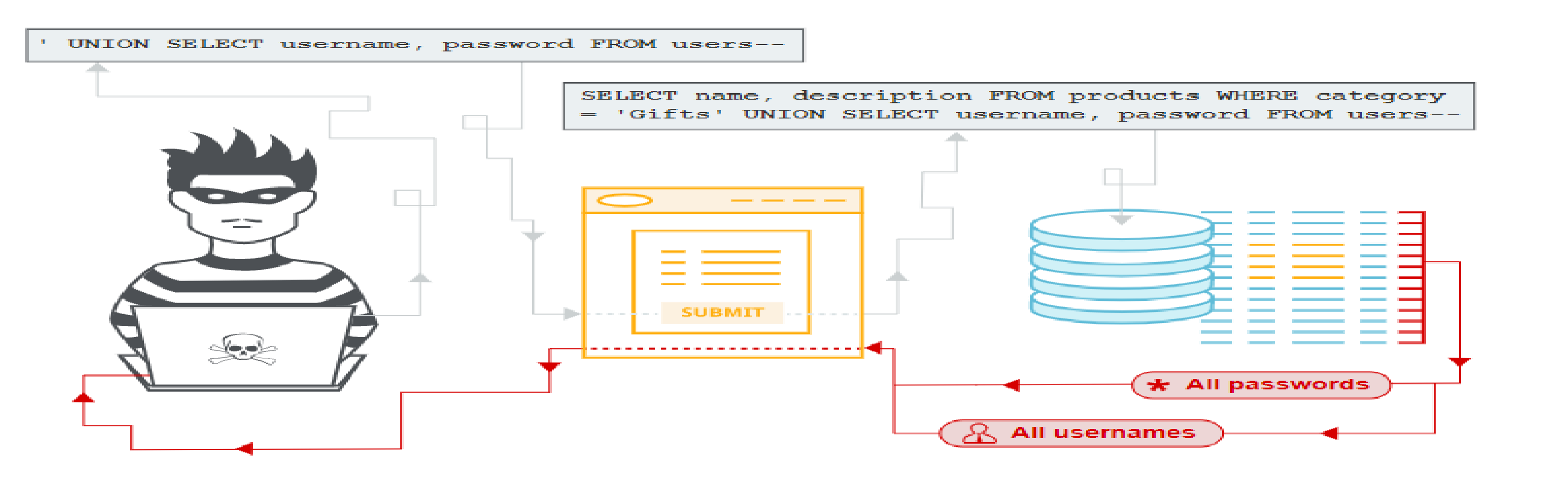
simple password
do not use the same password on different platforms
do not share passwords with others
1Password, Keepass, Lastpass etc. Tools

Password recovery questions
don't provide rational responses

Two Step Verification/Two Factor Authentication

A second authentication must be used when logging into any account

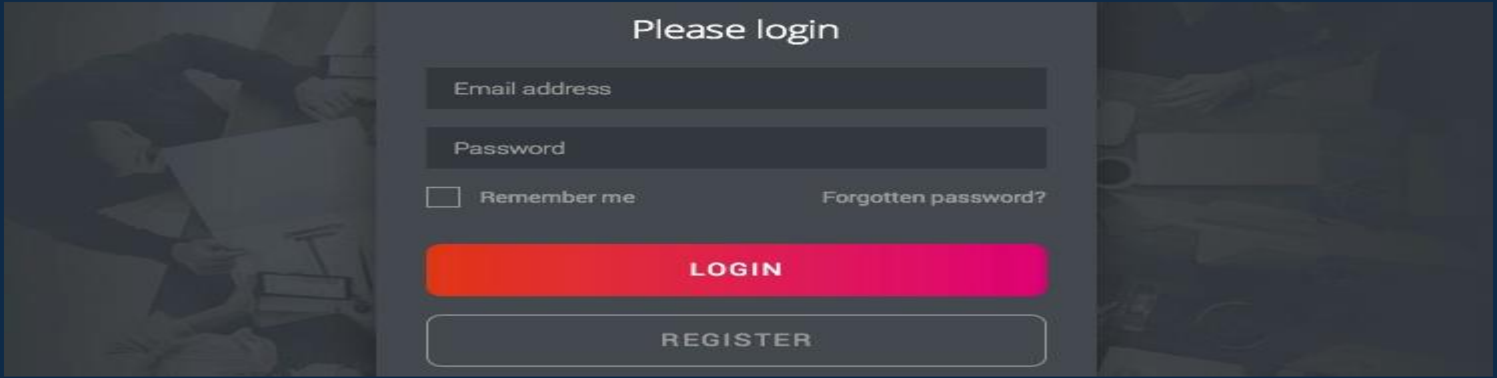
1. User name – Password 2. Phone code
1. User name – Password 2. E-mail
…



```
' UNION SELECT username, password FROM users--
```

```
SELECT name, description FROM products WHERE category
= 'Gifts' UNION SELECT username, password FROM users--
```

SQL Injection



```
txtUserId = getRequestedString(“UserId”);
sqlrequest = “SELECT * FROM Users WHERE UserId = ” + txtUserId

 “SELECT * FROM Users WHERE UserId = 105 OR 1 = 1”
 “SELECT * FROM information_schema.tables”
```

Encryption

Internet Encryption: Use secure protocols and channels when using the internet.

* http → https

System Encryption: Systems of authorized users should be protected with a password

Operating System Security: OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.

File Encryption: local disks and files with important content should be encrypted

Backup

*System backups: C*reate a backup of your computer periodically (System restore point, restore disk)

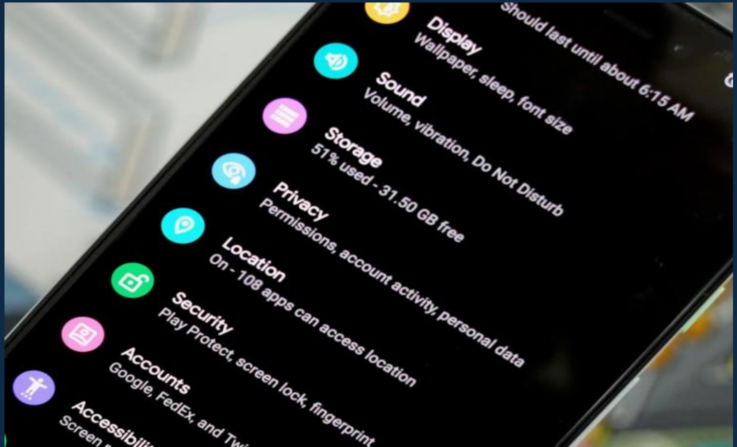
File backups: Backing up important files that are in development is a good idea.

Disk
USB disk
E-mail
Cloud → Google drive, one drive, dropbox … (synchronously).

Security on Mobile Devices

* Before installing an app, pay attention to the permissions it asks for. Consider whether it's reasonable for the app to be asking for these permissions.

Ex: phonebook app. → network permission
game app. → phonebook, location, SMS, file (foto, video) permisions etc.


Should last until about 6:15 AM
Display
Wallpaper, sleep, font size
Sound
Volume, vibration, Do Not Disturb
Storage
51% used - 31.50 GB free
Privacy
Permissions, account activity, personal data
Location
On - 108 apps can access location
Security
Play Protect, screen lock, fingerprint
Accounts
Google, FedEx, and Tw
Accessibili
Screen r

Less Common Softwares

* less common software should be preferred.

* Software that is in high demand and used is more targeted by attackers.

Ex: Windows, Internet Explorer, Chrome (Opera)

Antivirus Programs

An up-to-date antivirus program should be installed and all the features it provides should be turned on. (Antivirus, Firewalls, IDS etc.)

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop

KASPERSKY
ANTI-VIRUS
N
AVG
McAfee
ca
INTERNET SECURITY SUITE 2010
Microsoft Security Essentials
bitdefender
secure your every bit
F-Secure
avast!
be free
AVIRA
eset
NOD32
antivirus

Administrator Rights/Permissions

* Do not run programs as administrator.

* When a program is run as administrator, it can perform malware activities more easily because the program will have administrator permissions.

Ex: user files, critical system files, OS shell, etc.

Virtual Machine

* Use a virtual machine when performing operations that will compromise the computer.

* You can isolate infections by installing a virtual machine and delete or reset the virtual machine when you're done.

Ex: Vmware, Fusion, Workstation etc.

Browse The Web Safely

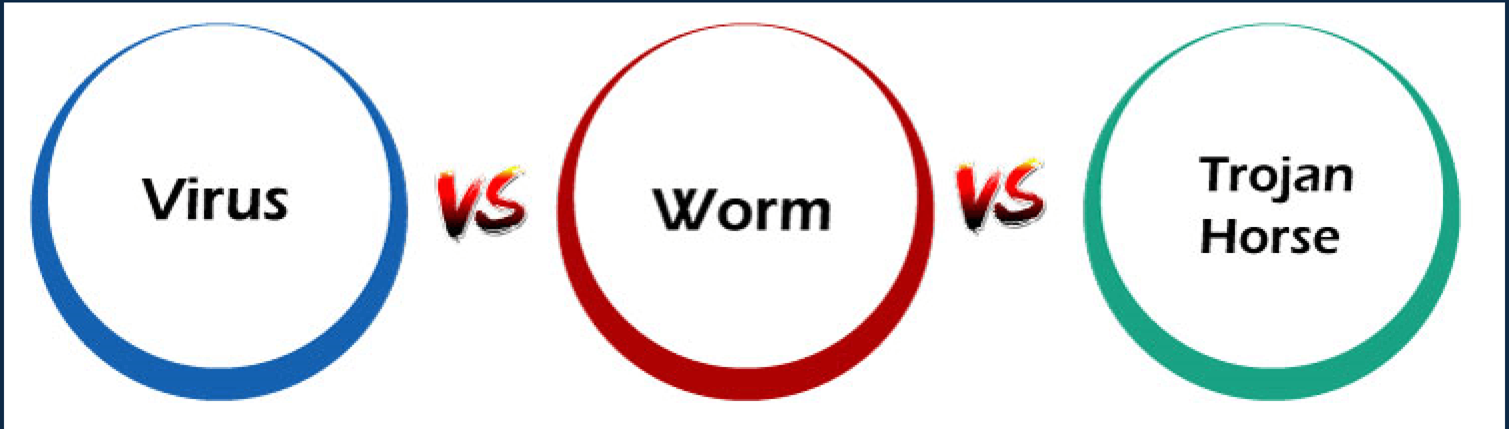
Avoid visiting sites that offer potantially illicit content. Many of these sites install malware on the fly or offer downloads that contain malware.

* Use modern browsers
* Up to date browsers
* Open the safety properties of browsers (blocking pop-ups, blocking automatic downloads)
…

Stay away from priated materials

Avoid streaming or downloading movies, music, books, or applications do not come from trusted sources. They may contain malware.

Viruses, Worms, Trojans, …



USB

* Don’t use USB or external devices unless you own them.

* To avoid infection by malware and viruses, ensure that all external devices either belong to you or come from a reliable source.