Cyber Security

Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as **Information Technology Security** or **Electronic Information Security**. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Types of Attacks

Cyber-attacks come in two main forms: passive attacks and active attacks.

1. Passive Attack
2. Active Attack

Passive Attack

- In a **Passive Attack**, an intruder monitors a system and network communications and scans for open ports and other vulnerabilities (for example, an unpatched system).
- The intruder will try to collect as much information as he or she can to use it later to attack the system or network; this type of attack is also known as **footprinting** and is used to gather intelligence about the target system to attack it in a later step.
- An example is when an intruder records network traffic using a packet analyzer tool (such as Wireshark) for later analysis.
- Installing a keylogger is also a kind of passive attack where an intruder waits for the user to enter his or her username and password and records them for later use.

Active Attack

- An Active attack involves using information gathered during a passive attack to attack a user or network.
- There are many types of active attacks. In a masquerade attack, an intruder will pretend to be another user to gain access to the restricted area in the system.
- In a reply attack, the intruder steals a packet from the network and forwards that packet to a service or application as if the intruder were the user who originally sent the packet.

- Other kinds of active attacks are denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, which work by preventing authorized users from accessing a specific resource on a network or the Internet (for example, flooding a web server with more traffic than it can handle).
- To counter these Internet attacks, individuals and companies deploy a set of defenses to protect their digital assets; however, despite your precautions, it is always possible that your system will get breached.

Digital Privacy

- Digital privacy is the protection of personal data when using the Internet.
- For example, when you conduct a search using Google, your search keyword, date/time of search, and your Internet Protocol (IP) address can be tracked back to you.
- The majority of Internet users do not know that their browsing activities and online habits are logged to formulate a complete profile about their online activities.
- Such precious information can be later sold to third parties for different purposes.
- To better understand the term digital privacy, you need to know the types of information that distinguish each person online.

Classification of Personal Information:

- When working online, there are two types of information can be collected from your activities
  1. Personally Identifiable Information (PII) or Sensitive Personal Information (SPI)
  2. Anonymous Information

1. **Personally Identifiable Information (PII) or Sensitive Personal Information (SPI)** is any information that can be used on its own or with other information to identify or locate a single person.
   - It includes name, Social Security number, passport number, date/time, place of birth, gender, father and mother names, biometric records, or any other detail that uniquely belongs to you and is personally identifiable.

- We think Anonymous information is trivial and not worth protecting.
- For example your browser type and version, operating system types and version, connected device type, area code, city, country, school or university name, current location, and anything else shared among more than one person cannot be considered personally identifiable.

Things You Want to Keep Private:

1. Contact Information
2. Private and Family Information
3. Location Information
4. Healthcare Records Information
5. Criminal Records
6. Financial Information, Purchase Information
7. Web Surfing History
8. Communication Logs

1. **Contact Information:**
    - This includes your full name, phone number, e mail address, work and home addresses.
2. **Private Information and Family Information:**
    - This includes your marital status, your wife's name, your parents' names, your age, children's names, children's age, children's school/university, and anything that is privately related to you and your close family.
        1. Unfortunately, the majority of Internet users already have such information published online (for example, on Facebook).
        2. This kind of information is dangerous to reveal as it may help outside observers hack into your online accounts, kidnap your children, and even impersonate you (identity theft).
3. **Location Information:**

- As computing technology advances, the majority of smart phones (and many IoT devices) have location sensors connected to different satellite services such as GPS.
- Others devices can determine location based on the cell tower network(Giant companies such as Google and Apple) already have large databases of cell towers and Wi Fi access points that can identify and track a user's current location.
- When enabled in smartphones and computers, location services can record your current location and all the places you were in, and Google has a facility (named Google Maps) that can draw a complete map of the places you've been and the routes you've traveled.
- Although this feature is private by default, we cannot guarantee that it really is Not all users prefer to reveal their location to the public (although many already do in Facebook).
- However, when using some apps (for example, using an app to find the nearest restaurant or gas station nearest your current location) that need location services to be turned on to work, they can record your physical location and use it later for different purposes without your explicit consent.

4. **Healthcare Records Information:**
   - This includes your physical characteristics such as your height and weight, eye and skin color, past illness history, medicine taken now and in the past, previous surgery, blood group, and anything that is recorded when you visit your doctor or hospital.
   - Such information is important, and it must be stored on computer records somewhere. Imagine if a security breach occurred and this information gets revealed and viewed by your insurance company or employer.
5. **Criminal records:**
   - If you have a past criminal record, what will be the consequence if it gets revealed to the public?
6. **Financial information:**
   - This includes your bank account details, bank transactions, financial partners, how much money you earn, tax statements, and anything else related to your financial condition.
7. **Purchase Information:**

- When you make an online purchase, you are using your credit card to pay for it Both credit card companies and banks will see your previous purchase history.
- This is something you cannot hide, and it is attached to your identity (you cannot open a bank account without showing them a valid government ID) If a security breach occurs and your purchase history is revealed.

8. **Web surfing history and communications log:**
   - When you visit a web site, the pages you visit, the amount of time you view each page, the links you click, the searches you make, every video you watch, every file you download, and the things that you interact with will be collected and recorded by this web site to create a "profile" that links to your web browser.
   - This data is stored somewhere on your computer or mobile phone (using cookies or caches) or somewhere on outside servers like the visited web site server or other third party server.
9. **Communication logs:**
   - Communication logs are also important they include all your e mail messages, Facebook and Twitter private messages, and any other activity conducted on a similar social networking web site Even after you delete your previous messages, you cannot guarantee that they have been completely deleted from all locations.
   - The main principle here is that what goes online never dies. Although this may be an overstatement in some cases, you should avoid posting or sending anything online that may lead to personal or legal problems if discovered someday.

Who Needs Your Personal Information?

1. Online Advertising Companies.
2. Intelligence Agencies.
3. Big Data.
4. Black Hat Hackers
5. People Who Know You
6. Other Parties

1. **Online Advertising Companies:**
    - Almost all free online services contain ads.
    - You cannot read the news, watch YouTube movies, use Facebook, or conduct Google searches without seeing advertisements.
    - Online advertising is a broad term used to describe the paid advertising that publishers put on their web sites or apps to enable them to provide you with content and services for free.
    - The advertiser is the one who pays the money to get advertisements shown, while the publisher is the one who gets the money for showing the ads.
    - The publisher could be a web site or application owner or anyone who has a digital channel to put ads on.
    - Advertisers are interested in profiling and tracking online users to target them with customized ads.
2. **Intelligence Agencies**
    - Security services are interested to know anything about you and your habits, previous purchases, political opinion, location, and even health status.
    - One of the major works of any intelligence agency is together as much information about its citizens, but the problem arises when an on authorized person or entity views this information or when it get shacked by an outside party.
3. **Big Data**
    - Big data can be analyzed for different purposes. For example, advertisers can use such data to profile and target users with customized ads, and security services can use it to extract a wealth of economic, security, and political information about any nation to make future predictions.
4. **Black Hat Hackers**
    - Some intruders may want to target you for fun; others may want to steal your data and money (stealing credit card and bank information). These latter intruders are called black hat hackers.
    - There are many methods that can be employed to steal your confidential data.
5. **People Who Know You**

- Your relatives, work colleagues, ex-wife or ex-husband, and any individual you have problems or a legal dispute with can use your personal information against you in some context.

6. **Other Parties**
    - There are additional groups of people who might become interested to know your private information.
    - For example, your future employer may seek to know information about you before signing a contract with you.
    - Insurance companies also have great interesting in gaining private information about their clients.
    - If you post your picture to your Facebook account while you are in the hospital, this can give a negative sign to your insurance company about your current health condition and may raise your health insurance rate.
    - Banks also need private information about their clients If you need a loan, your bank will need to know as much information about you as it can.

Online Tracking

- Online tracking is defined as the process of collecting and processing data acquired from Internet users' devices (tablet, and smartphones). There are two kinds of online tracking direct tracking and third party tracking.
- In direct tracking, the tracking is conducted by the web site or application the user is accessing
- In third party tracking, there is a third party (other than the web site/application the user is accessing) that tracks user browsing activities over multiple web sites (the user is the second party).
- A tracking log can be stored either on the user computer (for example, using cookies) or on the third party server.

The Danger of Online Tracking

1. **Mass Surveillance:**
    - Facebook has the ability to maintain a complete log of online activities about each user. This log will be connected to a user profile on Facebook (usually his or her real identity)

- This is a large amount of personal information stored in one place about each user. Let's now consider the consequences on this privacy what will happen if the Facebook servers get hacked by an outside party (Russia or China, for example)? What if Facebook hands this information to a security service agency?

2. **Service/Price Discrimination:**
   - Using profiling and tracking techniques, companies can customize service and price discrimination to each individual. In other words, people can be charged different prices based on a certain demographic factor, including location and/or socioeconomic status.
3. **Content Personalization Risks:**
   - Content personalization can be embraced in many ways. For example, when searching for sexual items, Facebook will show related ads on your Facebook profile, and the same will appear on search engine result pages.
   - Search engines also track and profile users according to their previous searches. This is not always good because it will return homogeneous results and even discard some. Such results can also be biased in some way.

Benefits of Online Tracking

- Online tracking is also used to fight against online fraud.
- It is used to detect online payment fraud by looking at some technical indicators that may raise suspicion.
- When the billing country and the IP country (IP determines physical location) do not match.
- When a proxy server is used to change the user's real IP address.
- If your connection originates from a high risk country.

Online tracking:

- **Online tracking** is used extensively in web analytics an measurement techniques Such techniques are used for analyzing web site data such as number of visitors, their origin country, which pages they visit, and how long they stay on each page.

- The compilation of this data helps web site owners to better develop relevant and effective ad campaigns in addition to identifying key performance to achieve the highest return possible.
- Web site owners (first party trackers) can develop their own analytical techniques However, the majority prefers to use third party services like Google Analytics, Alexa and Bing Webmaster Tools, to name a few.
- Web analytics track users online using different techniques (described next) and store their browsing activity across many web sites. This information helps them to create aggregated statistics to measure the effectiveness of their advertisements and to optimize web site contents accordingly.
- Finally, web tracking is also beneficial to stop certain kinds of attacks against web sites, for example, to stop a particular machine (or machines) from launching continual brute force attacks or to recognize attackers when they return.

Privacy Laws

- Data protection laws are commonly defined as laws designed to protect your personal information, which is collected, processed, and stored by automated means or intended to be part of a filing system
- Data protection laws cover safeguarding personal information stored in physical or electronic records.
- Data protection laws are important in today's digital world.
- As the majority of people begin to shift many of their activities online, Business organizations also record key information about their clients, staff, and business partners.
- All this data should be handled and stored according to strict rules to ensure that people's private information is kept safe. Data protection laws are not alike in all countries.
- For example, EU laws are different from those implemented in the United States.
- **General Protection Principles**: Collect only the data allowed by the laws Do not collect more information than you actually need for your purpose Do not keep the data for longer than you need, Assure that the information stored can be made available instantly on request, Make sure that personal information is stored in an encrypted format.

Types of Computer Security risks

- The Internet is full of risks! Whenever you go online, there is a possibility that you will encounter a risk.
- There are different types of computer threats with varying associations of damaging effects.
- For example, some threats may damage or corrupt your installed operating system and force you to reinstall it.
- Another type may steal your credentials and saved passwords.
- Still other threats may not bring any harm to your PC instead, they will track your online activities and invade your privacy.
- Today, criminals are smarter than ever before, and malicious programs are more sophisticated. Modern malware can infect a target PC and remain undetected for a long time.
- The motive behind the majority of cyber attacks nowadays is not to damage your machine but instead to steal your money, to access your private information, or to acquire your login credentials.

Malware

Malware is short for “malicious software” and is any software employed to bring damage to computing devices (smartphones etc or the stored content (data or applications).

Malware corruption can manifest in different ways, such as formatting your hard disk, deleting or corrupting files, stealing saved login information, gathering sensitive information (your files and private photos), or simply displaying unwanted advertisements on your screen.

Many malware variants are stealthy and operate silently without the user’s knowledge or awareness.

Malware is a term used to refer to many types of malicious software such as computer viruses, worms, Trojan horses, spyware, ransomware, scareware and adware.

Hacking

Hacking is the process of invading your privacy by gaining unauthorized access to your computing device. Hackers usually scan your machines for vulnerabilities (such as unpatched Windows updates) and gain access through them. After gaining access, they may install a keylogger or a Trojan horse to maintain their access, to begin stealing information, or to spy on user activities.

Pharming

Pharming is a cyber attack intended to redirect users from a legitimate web site to a fraudulent site without their knowledge. Pharming can be conducted either by changing the hosts file on a victim's computer or by poisoning the Domain Name System (server records with false information to lead users to unwanted destinations. DNS servers are computers responsible for resolving Internet names into their real Internet Protocol (IP) addresses. If the Windows hosts file gets infected with malware, it can change its contents and insert redirects, so when the user types the legitimate URL, the browser may then redirect to a malicious web site that has the same look and feel. When the user enters his or her username and password, the malicious web site will receive them instead of the original one, thus resulting in a compromised user account and credentials.

To mitigate such attacks, you can prevent hosts file modifications by following these steps

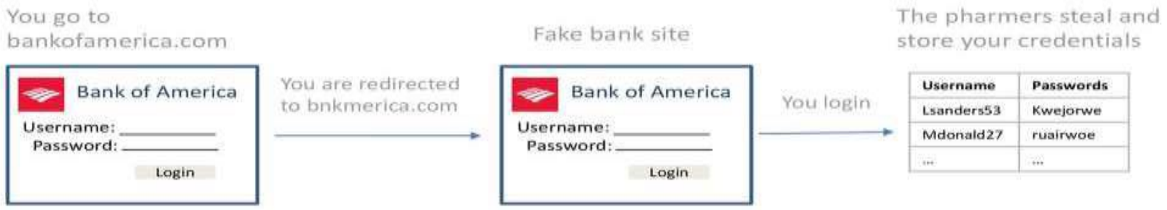
1. Navigate to the

%SYSTEMDRIVE%\Windows\Ssystem32\drivers\etc folder

(SYSTEMDRIVE is where you installed Windows, usually at **C:**\).

2. Right click the hosts file, select Properties, and select the Read only attribute;
3. finally click OK

Pharming Example


You go to bankofamerica.com
Bank of America
Username:
Password:
Login
You are redirected to bnkmerica.com
Fake bank site
Bank of America
Username:
Password:
Login
You login
The pharmers steal and store your credentials

Username	Passwords
Lsanders53	Kwejorwe
Mdonald27	ruairwoe
...	...

- Phishing is a technique using which attackers deceive a user into revealing sensitive details like passwords, PINs, credit card details, or other sensitive personal details.

- The attackers later exploit the collected information to perpetrate even more cyberattacks on the victim.

- Phishing messages come in different shapes, such as SMS messages, e mails, and web site links (all of which are designed to look genuine and use the same format as the legitimate company.

- Phishing aims to collect user sensitive details (such as banking information, passwords, and credit card details) by tricking the end user into handing the information to the attacker.

Phishing

- Phishing is a technique using which attackers deceive a user into revealing sensitive details like passwords, PINs, credit card details, or other sensitive personal details.
- The attackers later exploit the collected information to perpetrate even more cyberattacks on the victim.

- Phishing messages come in different shapes, such as SMS messages, e mails, and web site links (all of which are designed to look genuine and use the same format as the legitimate company.
- Phishing aims to collect user sensitive details (such as banking information, passwords, and credit card details) by tricking the end user into handing the information to the attacker.

Ransomware

- Ransomware is computer malware that installs silently on the user machine.
- Its objective is to deny access to user files, sometimes encrypting the entire hard disk drive and even all the attached external disk drives.
- It then demands that the user pay a ransom to get the malware creator to remove the restriction so the user can regain access to the system and stored assets.
- Most ransomware hits devices through phishing e mails and pop up advertisements.

There are three major types of ransomware

- The first one locks the system in a way that is not difficult for a technical person to reverse it displays a message requesting payment to unlock it
- The second type encrypts the whole disk drive, including any removable storage, and demand a ransom to decrypt it (but there’s no guarantee of getting any data back).
- The third is a variant that pretends to be ransomware but is actually trickware , which can easily be removed.

RANSOMWARE ATTACK

Your personal files are encrypted

You have 5 days to submit the payment!!!

To retrieve the Private key you need to pay

Your files will be lost

- Victims of ransomware usually pay the ransom through the bitcoin digital currency.
- Ransomware usually comes hidden in a legitimate file. When the user installs the legitimate program, the ransomware gets installed as well without the user's knowledge.
- Ransomware is now the number one security concern for organizations. As the number of attacks increase, it has become a global problem that threatens both individuals and companies.
- According to CNN,cyber criminals collected $209 million in the first three months of 2016, meaning that at the end of 2016 this number may reach $1 billion. This number may be even bigger than that, though, because some victims may choose to pay and not report the crime.

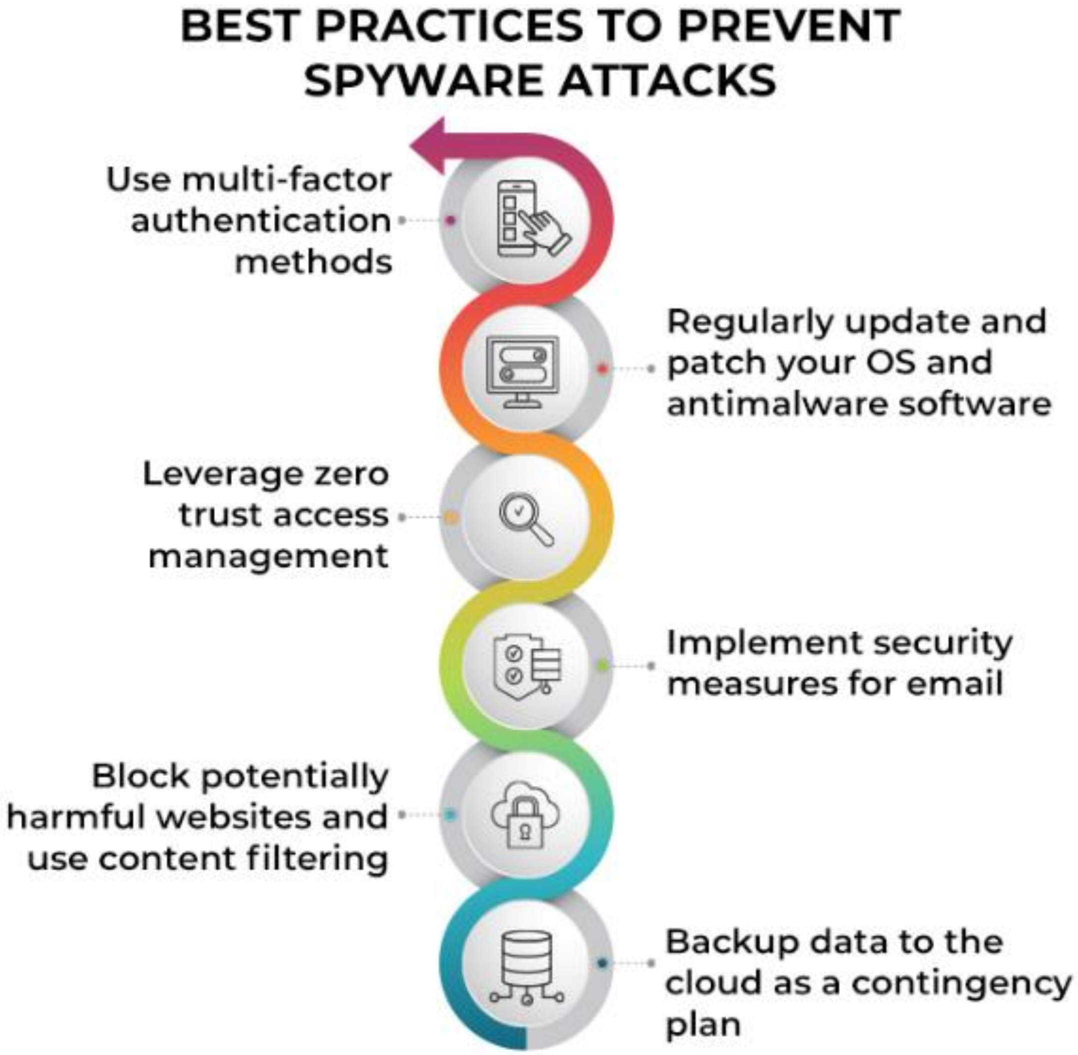
Adware

- Adware is used to collect information about you and your machine It usually comes with free software or useful plug ins or search bars for web browsers.
- Once installed, it begins tracking your online activities and may then send it to outside parties.
- Many free games and free system utilities contain adware.
- Few users read the end user license agreements (and simply click the "I agree" button without knowing that the freeware may contain adware (which is clearly stated in their EULAs).

Spyware

- Spyware in the form of a keylogger will seek to steal everything you type on your keyboard (usernames and passwords) and send it to its operator Some spyware can facilitate installing a virus on your operating system, rendering it inoperable.

- Spyware in the form of a keylogger will seek to steal everything you type on your keyboard (usernames and passwords) and send it to its operator Some spyware can facilitate installing a virus on your operating system, rendering it inoperable.


BEST PRACTICES TO PREVENT SPYWARE ATTACKS
Use multi-factor authentication methods
Regularly update and patch your OS and antimalware software
Leverage zero trust access management
Implement security measures for email
Block potentially harmful websites and use content filtering
Backup data to the cloud as a contingency plan

Rootkits

- A rootkit is a dangerous type of malware; it can potentially gain full access (administrative access) over the system and has the ability to prevent normal detection programs (antivirus and anti rootkit programs) from noticing its presence.

Juice Jacking

- In this attack, an intruder will steal your private data through the USB charging port of your smartphone tablet, or laptop when you connect your device to a public power charging station such as the ones available in airports, conferences, and restaurants.

- Malware can also get installed using this technique. To counter such risks, do not charge your computing device in public charging stations; use personal power bank units instead.

Scareware

- Scareware is a form of malicious software that uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.
- Scareware can report to a user that his or her machine is full of spyware and other infections and he or she must act promptly and purchase an anti malware solution (which is fake!).
- The idea here is to trick the user into purchasing something unnecessarily in order to take his or her money.

Trojan Horse

- A Trojan Horse Virus is a type of malware that **downloads** onto a **computer disguised as a legitimate program**.

- A simple way to answer the question “what is Trojan” is it is a type of malware that typically gets **hidden as an attachment in an email or a free-to-download file**, then **transfers onto the user’s device**.
- Once downloaded, the malicious code will execute the task the attacker designed it for, such as **gain backdoor access to corporate systems**, **spy on user’s online activity**, or **steal sensitive data**.

Distributed Denial-of-Service Attack (DDoS)

- DDoS is a cybercrime in which the attacker floods a server with internet traffic to **prevent users from accessing connected online services and sites**.
- A DDoS attack aims to **overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.**

Computer Virus

- A Computer **Virus** is a program written to **enter your computer** and **damage** or **alter your files** and **data**. A virus could **corrupt** or **delete** data on your computer. Viruses can also **replicate** themselves.
- A Computer Virus is more **dangerous** than a computer **worm** as it makes **changes** or **deletes** your files while **worms** only **replicate** themselves **without making changes** to your **files** and **data**.
- Viruses can enter to your computer as an **attachment** of images or as **audio** or **video files**.
- Viruses also enter through downloads on the internet. They can be hidden in free-trial software or other files that you download. It is wise not to download anything that you aren’t sure who the real sender is.
- Almost all viruses are attached to an executable file, which means the virus may exist on your computer, but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action or social engineering, such as running an infected program to keep it going.

Wi-Fi Eavesdropping

- No matter whether you are at home, at work, or at a public access point, hackers can intercept communication, communicate through unprotected wireless networks and access points.
- Such attacks can result in intercepting all your online communications, including your usernames and passwords, and of course may provide access to your online banking details.

Antivirus and Other Security solution

- Installing an antivirus program is considered the first line of defense for any computer user.
- However, keep in mind that having an antivirus solution does not mean you are covered on the whole Internet security front.
- Unfortunately, some antivirus products try to give the impression (for marketing purposes) that they will completely cover all security once installed.
- Traditional antivirus programs are useful against classical threats such as viruses, worms, some types of malware, phishing, and spam.
- But the end user may still need a specialist solution against spyware and ransomware in addition to a firewall solution for maximum protection.

How to Select Your Antivirus Program

Antivirus software usually uses three basic methods for **detecting, blocking,** and **removing viruses**.

1. Signature-based detection
2. Heuristics detection
3. Rootkit detection

- Most personal antivirus solutions use a combination of signature based detection and heuristic technology. Although most antivirus programs have a similar approach for detecting malicious software, some are better than others. To help you select the best one, we have created a number of criteria that should be met by your future antivirus solution.

Criteria to Select AntiVirus

1. The antivirus program should **detect** and **remove** malware of all kinds (including ransomware or any other financial malware).
2. It should be able to detect **phishing** attacks and **dangerous web sites** and **deny access** to them.
3. It should be able to **integrate** with major **e-mail clients** (such as Microsoft Outlook and Thunderbird) to **scan incoming** and **outgoing e-mails** automatically in addition to filtering spam e-mails.
4. It should be **compatible** with the currently installed **operating system** and **programs**.
5. It should come equipped with a **personal firewall**.
6. It should **update** itself **automatically**.
7. It should be **efficient** in terms of discovering **zero-day malware** and **updating** its **virus signature database instantly**.
8. If the antivirus has the **ability** to **detect rootkits**, this is an excellent extended feature.
9. It should have a **lower number of false positive alerts** or **false alarms** (this happens when antivirus software recognizes legitimate software as malware).
10. It should be able to **protect** your **browser** from **outside attacks**.
11. It should have a **DNS protection** feature.
12. It should be **lightweight** and **not consume high computing resources** when **scanning files** or **working** in the background.
13. It should **not renew its license automatically without explicit approval**.
14. It should be **affordable** to you.

Password

Create Secure Passwords:

- People’s choice of passwords continues to pose a huge security risk.

- Recent data breaches of user personal data and account passwords show that a large number of users are still using risky passwords to secure their Accounts.
- According to SplashData's 2015 "Worst Passwords List"List"(compiled from more than 2 million leaked passwords during the year), the two most commonly used passwords by online users were 123456 and password, both of which have remained at the top of the list since it first started in 2011.
- The report also shows that despite many users attempting to create more secure passwords, the majority are based on simple patterns that would be easily guessed by hackers.
- Data breaches and cyberattacks are becoming more and more common. In order to keep your online identity and private information safe, taking care of your passwords is as essential as ever.
- One of the key elements of a strong password is its uniqueness. But some passwords are anything but that. Here are the most commonly used passwords & phrases used in passwords by people around the world – collected by the Cybernews Investigation Team.

The top 10 most common passwords list in 2023:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

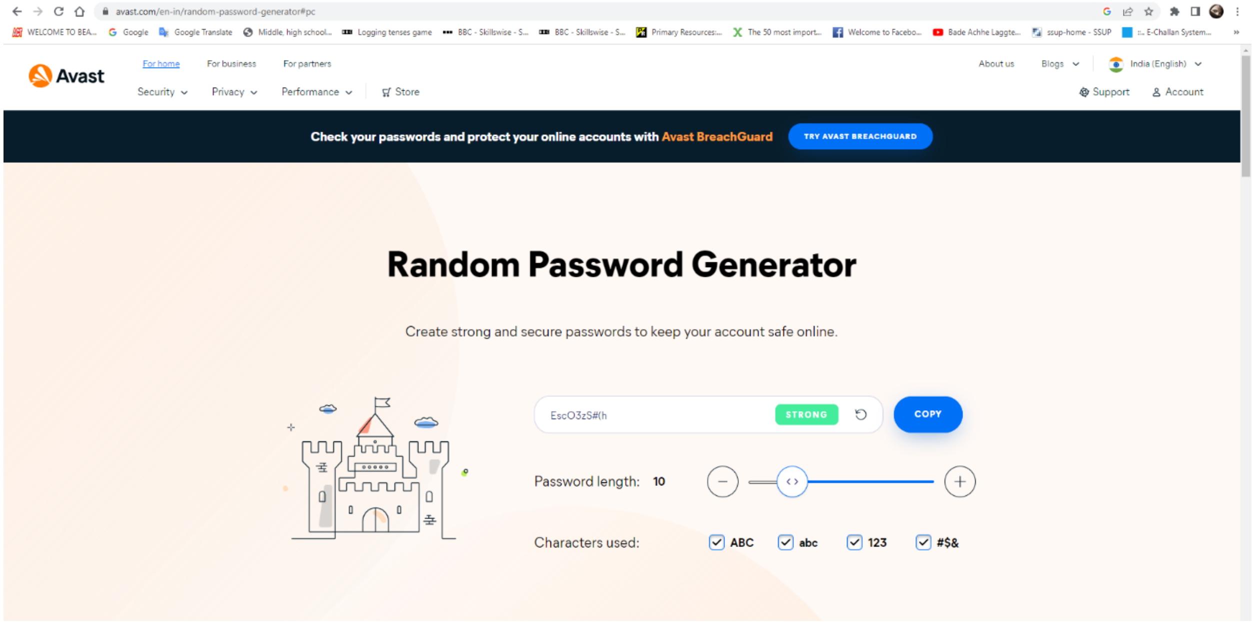
Tips to create secure passwords:

- The password should be at least 15 characters in length for maximum security.
- The password should contain at least one lowercase letter, one uppercase letter, one number, and one symbol (e.g., # % &).
- The password shouldn’t be your username or even part of it.
- Do not use your spouse’s, family member names (including your name), or pet’s name as part of your password.
- Do not share the same password between your spouse or friends (have two e mails with the same password).
- Do not use your gender or birth date/place as part of your password.
- Do not use places names for your password (country, city, street name, school, or university name).
- Do not use famous people’s names as your password (e.g., famous movie actors, political leaders, public figures, singers).
- Avoid sequences when creating passwords (consecutive letters, numbers, or keys on the keyboard such as 123456 or asdfghjkl
- Do not use the same passwords for two different accounts (e.g., your bank account password and your private e mail password should not be the same).
- Change your password once every three months.
- Do not use the same password again (e.g., when you change your e mail password, do not return and use any password you were using during the last year).
- Do not use dictionary words as your password or part of it.
- Do not use real words from foreign languages as your password.
- Use a password manager to organize and protect passwords, generate random passwords, and automatically log into web sites.
- Don’t store your passwords in an unencrypted text file or Microsoft Excel spreadsheet or any other file type that is not encrypted. Also, never write down your password on paper. If you want to take your password with you and you are afraid that you may forget it (because it is complex), then use a portable password manager and keep it on your smartphone or on your USB stick drive.

- Do not let your web browser save your entered passwords.
- Do not use tools to automatically generate your password for to important accounts (e g bank accounts and medical record accounts)
- For such important accounts, follow the rules already mentioned and create something from your mind.
- Do not send your password if someone requests it from you. Many social engineering attacks involve making users trust the attacker and getting them to share their passwords.
- Whenever you hear about a data breach in press, instantly change your affected account password.
- Do not ever type your password on a computer that does not belong to you.

Password Generation Tools

- It is important to change your passwords continually and to use strong, complex passwords that can be difficult or impossible to crack using brute force, dictionary, or guessing attacks. Many users may fail to create such complex passwords or may simply repeat and use a portion of the old password to create the new one, which is considered an insecure practice.
- **FreePasswordGenerator:** (https ::/www securesafepro com/pasgen html) is a free, lightweight tool for generating secure and complex passwords It has a portable version and can run on all Windows version.


avast.com/en-in/random-password-generator#pc
WELCOME TO BEA... Google Google Translate Middle, high school... Logging tenses game BBC - Skillswise - S... BBC - Skillswise - S... Primary Resources:... The 50 most import... Welcome to Facebo... Bade Achhe Laggte... ssup-home - SSUP :: E-Challan System...
Avast
For home For business For partners
Security Privacy Performance Store
About us Blogs India (English)
Support Account
TRY AVAST BREACHGUARD
COPY

Check your passwords and protect your online accounts with Avast BreachGuard

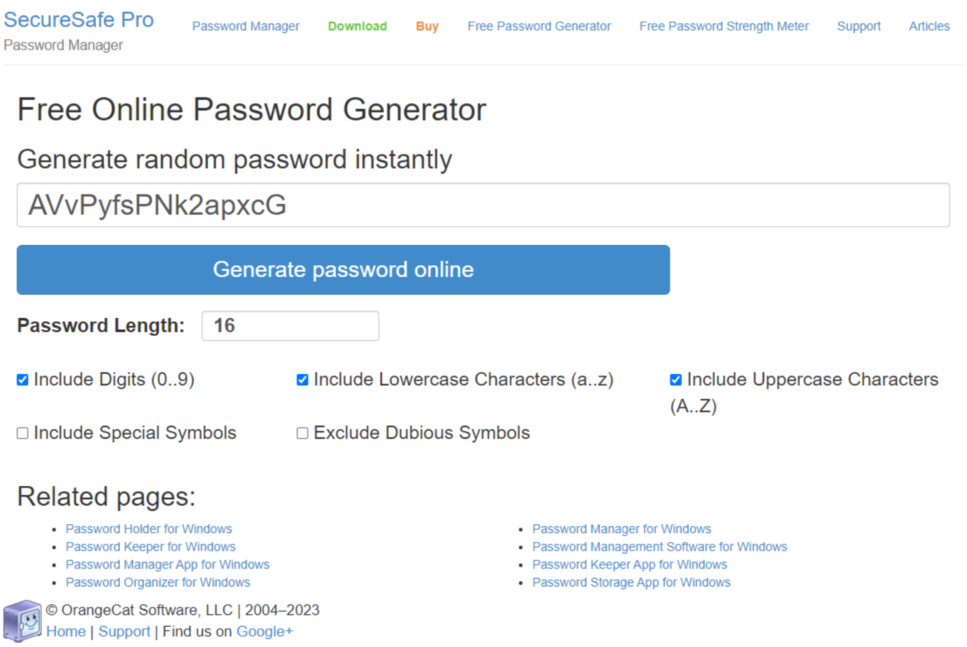
Random Password Generator

Create strong and secure passwords to keep your account safe online.

EscO3zS#(h STRONG

Password length: 10

Characters used: ☑ ABC ☑ abc ☑ 123 ☑ #$&


SecureSafe Pro
Password Manager
Password Manager Download Buy Free Password Generator Free Password Strength Meter Support Articles

Free Online Password Generator

Generate random password instantly

AVvPyfsPNk2apxcG

Generate password online

Password Length: 16

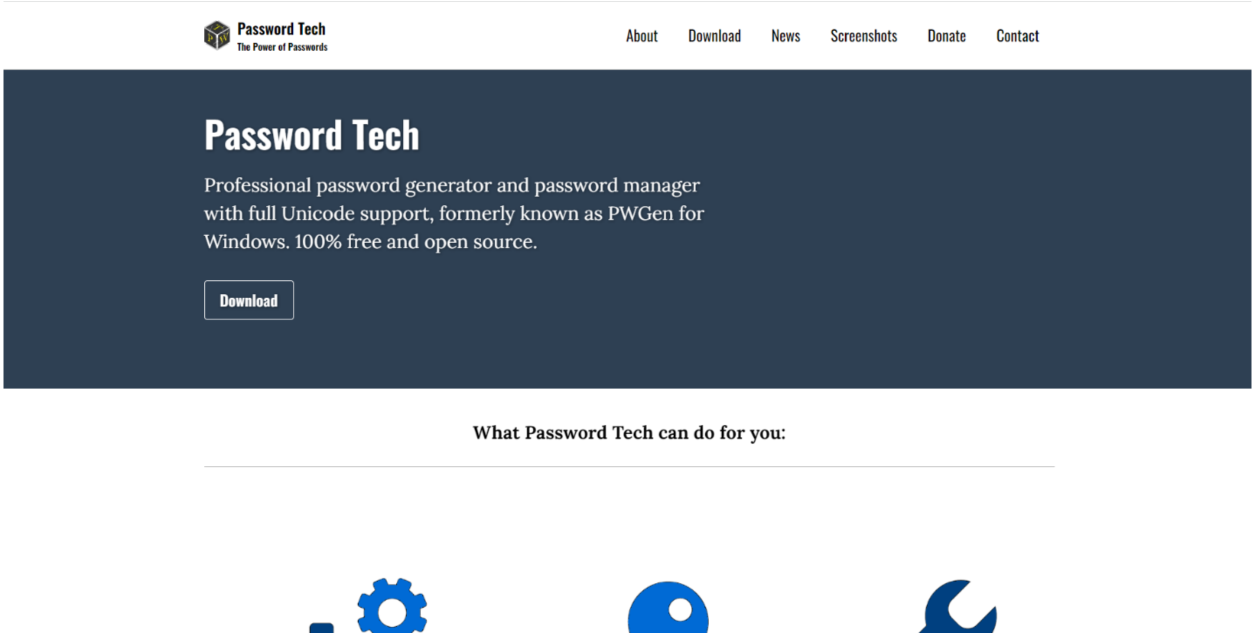
☑ Include Digits (0..9) ☑ Include Lowercase Characters (a..z) ☑ Include Uppercase Characters (A..Z)

☐ Include Special Symbols ☐ Exclude Dubious Symbols

Related pages:

- Password Holder for Windows
- Password Keeper for Windows
- Password Manager App for Windows
- Password Organizer for Windows
- Password Manager for Windows
- Password Management Software for Windows
- Password Keeper App for Windows
- Password Storage App for Windows

© OrangeCat Software, LLC | 2004–2023
Home | Support | Find us on Google+



Password Tech

Professional password generator and password manager with full Unicode support, formerly known as PWGen for Windows. 100% free and open source.

What Password Tech can do for you:

- **PWGen** (http ::://pwgen win sourceforge net) is an open source professional password generator capable of generating large numbers of cryptographically secure passwords, pronounceable passwords, pattern based passwords, and passphrases consisting of words from word lists.
- It uses a "random pool" technique based on strong cryptography to generate random data from indeterministic user inputs (mouse handling) and volatile system parameters.
- It also has some interesting features because it can encrypt, decrypt, and clear the clipboard so that no information is intercepted when copying passwords out of this program

Password Managers

- A **password manager** allows you to **store** all your **online accounts' login details** in one place. When you want to log in to any service/web site, all you have to do is copy the username/password to the login form.
- A password manager encrypts the database that contains your login information and protects it with a master password. This is the only password you have to remember.

KeePass Password Safe

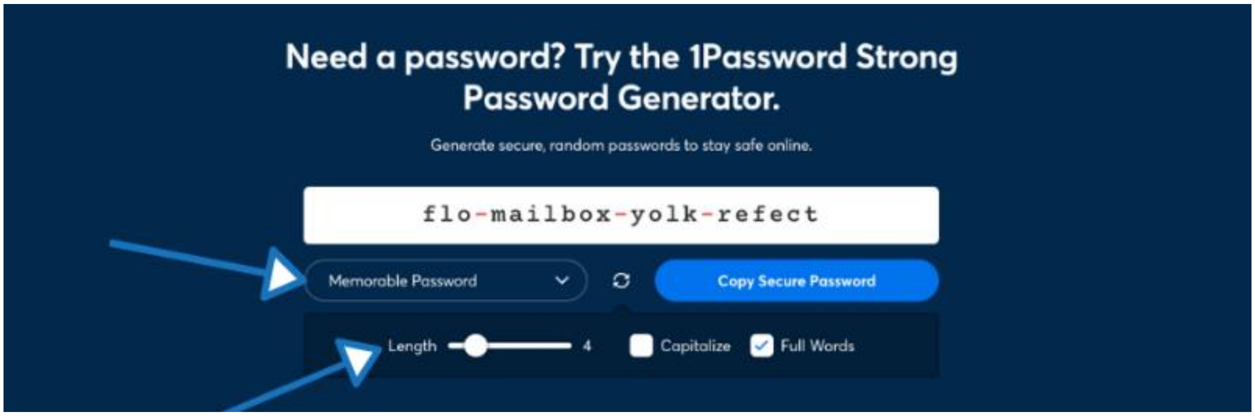
- KeePass Password Safe (http:://keepass info) is a free open source password manager.

- KeePass has a portable version so you can run it from your USB stick. It has been ported onto different platforms such as macOS iOS Linux, and Android

Master Password

- Master Password (https://ssl.masterpasswordapp.com) has a unique approach to generating user passwords.
- Its passwords **aren't stored** in an **encrypted database** or uploaded to a secure cloud service. Instead, they are generated on the fly using the following parameters **your name**, the **site** you are going to use the password for, and your **master password** (which is the main password used to log in to the Master Password program).
- This unique approach to password creation/management guarantees that your passwords will not get intercepted as you synchronize your account between devices (for example, your smartphone and PC).
- In addition, you do not need any repository to store these passwords. All you need to do is install the Master Password tool on each device you want to use and then enter your name and site names and you are ready to go.

Sample password generated using the Master Password tool



Need a password? Try the 1Password Strong Password Generator.

Generate secure, random passwords to stay safe online.

flo-mailbox-yolk-refect

Memorable Password

Length 4

☐ Capitalize ☑ Full Words

Password Safe

- Password Safe (https://www.pwsafe.org) is an open source program that allows you to easily and quickly generate, store, organize, retrieve, and use complex new passwords, using password policies that you control.

- The original version was designed by renowned security expert Bruce Schneier.
- Password Safe is designed to be extremely hard to crack using brute-force attacks, and it encrypts all user data in memory when using it.

Secure online browsing

- Your web browser is your window to the entire world.
- From here you can log in to your **social media accounts**, **access** your **bank account**, **buy products** and **services**, and **check** your **e-mails**, in addition to anything else you do online.
- The wealth of information that exists in web browsers makes them attractive for cyber-criminals. It is necessary to tweak your browser security settings to make it less vulnerable to outside attacks.
- There are many desktop browsers; the market share is mainly divided between Microsoft Internet Explorer (IE), Mozilla Firefox, Safari, Opera, and Google Chrome.

1. **Disable Location Information:**

    - It sounds like a great idea.
    - To disable the location service in the Facebook app (on Android), open the Facebook app, Tap the menu button, and select Account Settings ➤ Location ➤ Location Services ➤ Turn it OFF.

2. **Remove Metadata from Digital Files:**

    - Metadata is a data about data. In technical terms, it contains hidden descriptive information about the file it belongs to.
    - For example, some metadata included in a document file might include author name, date/time created, and comments.
    - It is advisable to check the metadata of all images before uploading it to the Internet to avoid leaking private information about yourself and the device.

3. **Turn On Private Browsing:**

- Most modern web browsers have a privacy feature called private browsing that lets you browse web sites without your history being tracked locally on your computer.
- When this is enabled in Firefox, Firefox will not record your visited pages, cookies, temporary files, and searches.

4. **Read Web Site Privacy Policies:**

Policy agreements will usually contain information on how the web site will collect data from your computer and how the web site will share it.

1. What type of information will the site/software collect about you?
2. Will your personally identifiable information (PII) or anonymous information be shared with third-party affiliates?
3. Will your information will be disclosed overseas?
4. Can you opt out from this agreement later?
5. Where will your information be stored

5. **Make Sure to Log Out:**

Whenever log in to your social networking account, your e-mail, or an online retail account, make sure to log out when finished.

- How to Know Whether a Web Site Is Secure? Check the Web Site SSL
- Certificate.
- SSL certificates are small data files that digitally bind a cryptographic key to web site details.

Secure online browsing

- When installed on a web server, the certificate activates a padlock and the Hypertext Transfer Protocol Secure (HTTPS) and allows a secure connection between the company server and the client machines.

- Upon installing the SSL certificate, the URL of the web site will begin with

https:// instead of http://

Email Security

- E-mail is the most used service through the Internet; it is widely used for both business and private communications.

Important tips to consider when using your e-mail service:

- Do **not access** your primary e-mail account using **free**, **open Wi-Fi access** points in public places.
- Use encryption when using an e-mail client (e.g., **Mozilla Thunderbird**) and make sure to encrypt the connection between your computer and e-mail server.

1. Create **multiple** e-mail accounts.
2. Do not use **free e-mail service** for mission-critical work.
3. **Encrypt** all your mission-critical e-mails.
4. Do **not publish** your primary e-mail address online.

- Do not open e-mail attachments from unknown senders.
- Do not send sensitive documents.
- Do not reply to spam e-mails.

Social Engineering

- Social engineering is a kind of attack that uses psychological tricks (social tricks) over the phone or uses a computing device to convince someone to handle sensitive information about himself or herself or an organization and its computer systems.
- There are many techniques already employed to conduct social engineering attacks; the most common type is **phishing**.

- **Phishing:** an attempt by an individual or group to solicit personal from unsuspecting users by employing social engineering techniques.

Some countermeasure steps against phishing attacks:

1. Do not give your credit card, bank details, or other sensitive personal information over phone calls or through e-mails.
2. Refuse to answer calls from telemarketing people.
3. Do not give information to charity organizations that you do not know.
4. Do not give information about the company you work for.
5. Pay attention to the URL of a web site.
6. Do not click hyperlinks or links attached in the suspected phishing e-mail.
7. Check your bank account regularly to make sure it is safe.
8. Do not install programs or download files sent as attachments in e-mails from unknown senders.
9. Do not access your important accounts on public computers, and use a virtual keyboard where applicable.
10. Always discard pop-up screens.
11. Make sure the web site you deal with to enter your personal information is protected by an SSL certificate (HTTPS).

Enhance the security of your computer by keeping your antivirus software up-to date. Organizations should invest in educating their employees about cybersecurity attacks. Business organizations should have a data classification policy, where only the employees who really need to access sensitive data are given access to it.

Secure Home Wi-Fi Settings

- Most individual users connect to the Internet using a dedicated router (usually an ADSL router).
- All home computing devices and appliances are connected using this single device. Most users prefer to use a wireless connection instead of cables.

1. **Change the Network SSID Name:**

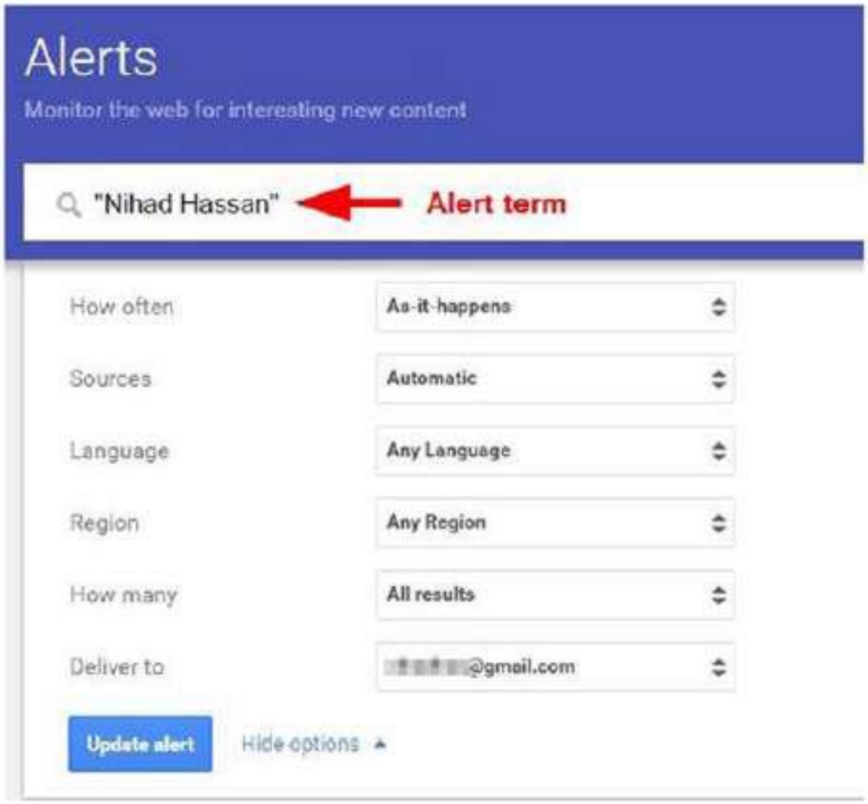
   - Each router comes with a default name (SSD or wireless network name), which is usually the name of the manufacturer (e.g., D-Link).
   - Changing this name to something else (don’t use your personal information; use something ordinary and not related to you personally) will help you to prevent outsiders from knowing which router belongs to you.
   - You can also hide your Wi-Fi SSID completely.
2. **Enable Wi-Fi Encryption:**
   - When you are at your router’s settings page, go to Wireless setup ➤ Wireless security and select a strong encryption standard to secure your Wi-Fi transmission.
   - For instance, WPA2 is the most secure one .
   - Finally, enter a passphrase to protect your Wi-Fi connection (this passphrase is used by all devices that want to use your Wi-Fi connection).
3. **Filter MAC Addresses:**
   - All computing devices (laptops, tablets, desktops, and smart phones) have a MAC address. This is a unique address.
   - It is hard-coded on the network interface card of each device capable of interacting with the Internet.
   - You can go into your router settings (usually the MAC filter area) and type in the MAC addresses of only those devices you want to allow on the network. This will effectively help you to restrict access to your local network.
4. **Update Firmware:** Make sure to update your router firmware continually. Manufacturers release updates to counter future vulnerabilities, and leaving your router without an update is a security hole.
   1. Cover Your Laptop Webcam
   2. Do Not Post Your Selfie Pictures
   3. Back Up Your Data

Track Yourself Online

- It is important to track yourself online on a regular basis. This helps you to find where you are showing up online and what others are saying about you.

Google Alerts

- Google Alerts is a notification service offered by Google; it works by sending an e-mail to the user when it finds new results such as web pages, newspaper articles, blogs, or scientific research that matches the user's entered search terms.
- You can set up a new alert at https://www.google.com/alerts.
- In the box at the top, enter a topic you want to follow. You can create as many alerts as you like and adjust the settings to be notified on a daily, weekly, or "as it happens" basis.



Alerts

Monitor the web for interesting new content

"Nihad Hassan" Alert term

How often: As-it-happens

Sources: Automatic

Language: Any Language

Region: Any Region

How many: All results

Deliver to: [redacted]@gmail.com

Figure 2-35. Setting up Google Alerts to get notified when your search terms are mentioned online

- The free people search engine at https://pipl.com is another web site to search about yourself and other people online.
- It allows you to search by name, address, or email and has the most comprehensive database of people profiles online.

Auditing Facebook Profile

- Many users have been using Facebook for a long time. Some people have thousands of likes and posts on their Timelines. Humans have a tendency to forget their previous online actions, though.
- For instance, any person who previously posted his or her political opinion or comment (aggressively) may find that it will be more suitable to hide previous online actions for many reasons. Performing a check on every post and action conducted on Facebook is a daunting task, especially if the user has been active on Facebook for a long time.
- Stalkscan (http://stalkscan.com/en/) is a free online service that allows anyone to look up any Facebook user's public information.
- It is a great auditing tool for Facebook profiles and allows any person to see previously posted images, comments, events attended in the past in addition to future events planning to attend, places where they "checked in," and everything they "like" online (posts, video, pictures, etc.).
- This tool shows you just how easy it is to find any public information on Facebook, so be careful before posting anything publicly online.

Check Whether Someone Has Taken Your Personal Picture

- Sometimes you may encounter a case where someone took your personal pictures (or your child's pictures) from your Facebook profile and used them on a profile or blog without your consent or even used them for the wrong reasons.
- Reverse Image Search helps you to find any photo you have uploaded to the Internet along with a list of all other web sites where this photo appears.
- TinEye (https://www.tineye.com) is a reverse search engine with more than 17.4 billion images indexed (at the time of writing).
- You can upload the image you want to search for online or simply enter its URL, and TinEye will find all the locations and web sites where this image is located.

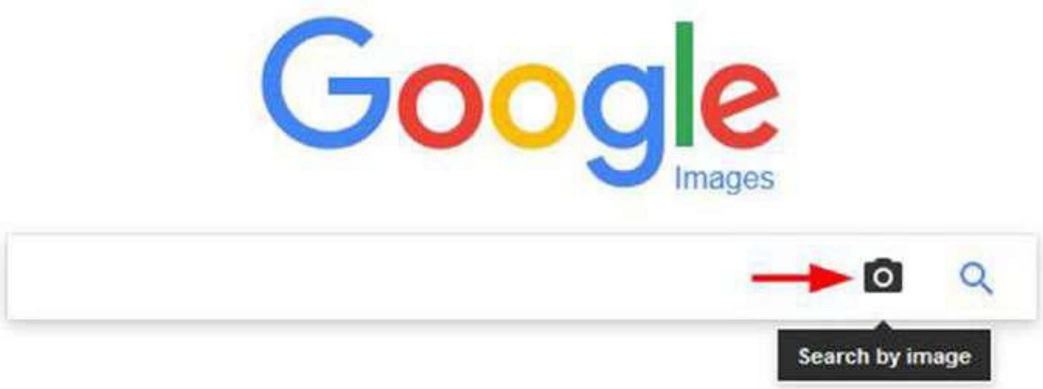
Google has a similar service to search for images online.

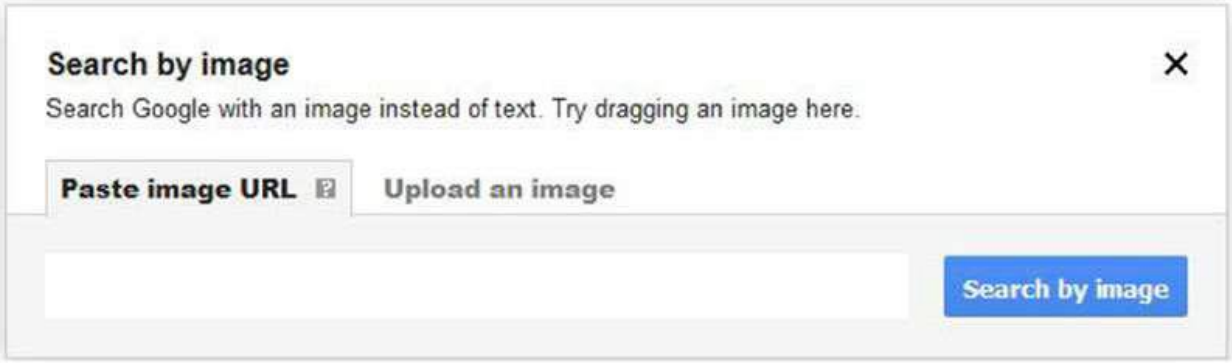
1. Go to https://images.google.com.

2. In the search bar, click the camera icon

3. You can either upload a picture from your computer or enter its URL to search for it.

4. Google will return every instance of that image it can find.




Search by image

Search Google with an image instead of text. Try dragging an image here.

- Another free service to conduct an image search is **https://www.imageraider.com.** This web site allows you to search popular search engines like Google, Bing, and Yandex to find all web sites using your photos.

- A good practice when publishing personal photos online is to watermark them. This allows you to prove ownership of your photos. There are many tools and online services that offer watermarking for free.

- https://www.watermarquee.com offers free online watermarking, as does Picasa (retired but available) at http://filehippo.com/download_picasa.

Check Your Data Breach Status

- Almost every week the press announces a data breach that hit a major web site. To tighten your security, it is essential to check whether your account was among the ones that got breached. Fortunately, there are many free services to check whether your account was compromised.
- https://haveibeenpwned.com is a free resource for anyone to quickly assess whether they may have been put at risk because of an online account being compromised or "pwned" in a data breach.
- It is run by security researcher Troy Hunt, who tracks data breaches. To use this web site, enter the e-mail address or username in the search box to check whether you have an account that has been compromised in a data breach.
- You can also sign up for alerts tied to your e-mail address so you can be notified as soon as another breach is detected by clicking "Notify me" at the top of the page.
- It is highly advisable whenever you hear about a data breach in the press and you have accounts at a company that has been breached that you change your affected account's password.
- Checking the previously mentioned sites to see whether your account was stolen is a good thing, but it is important to act promptly and change your affected account's password.
- Remember, do not use the same password on two different accounts.

Delete All Your Online Profiles

- If you decide to delete your online presence from the Internet and return to the "offline age," there is a free service that can help you achieve this. Deseat.me is a service that lets you see all the web sites you're signed up for and asks if you'd like to delete them or unsubscribe.
- It asks for your e-mail address and password so it can scan for the sites you're signed up to.

Cloud storage security

- More and more companies are adopting cloud storage solutions to reduce the costs of storing and processing data locally.

- Cloud storage solutions help employees access data anytime and from anywhere using any device type with low IT overhead.
- To secure cloud storage accounts, the following security measures should be implemented:
  1. Use **strong passwords** to secure your cloud accounts.
  2. Enable **two-factor authentication** to access your cloud account.
  3. Use **antivirus/anti-exploit software** and keep them **up-to-date** like OS.
  4. **Cloud storage** providers allow you to **revoke** when sharing is not required.
  5. It is highly advisable to keep a **backup** copy of all data in a safe location.
  6. **Do not upload** anything to the cloud **without encrypting** it first locally.
  7. Even after encrypting your data, it is not preferable to use cloud storage to store sensitive data.
  8. Encrypt the connection between your machine and the cloud storage provider.

Internet of Things Security

- While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation.
- To enjoy the benefit of IoT devices, a set of security measures must be implemented by individuals and companies to avoid turning the IoT innovation into a catastrophe.
- Do not connect your device to the Internet unless there is a need for this.
- Isolate IoT devices in a separate network.
- Use a strong, complex password for each IoT device.
- Change the device’s default username and password. Businesses should prevent their employees from bringing their IoT devices to work.
- Read the manual of the IoT device before connecting it to the Internet.
- Keep your IoT device up-to-date by visiting the device settings.

- If your IoT device supports Telnet and SSH services, make sure to disable them. Purchase IoT devices from companies with a reputation for providing secure devices.

Physical Security Threats

- Physical threats are not only from theft; other threats include natural disasters, breakage, power surges, poured coffee over the computer, and anything else that can damage your computing equipment and prevent you from accessing the information stored on it.
- Performing an IT security risk assessment should be an important part.
- It helps businesses to understand and quantify the risks to IT and the possible consequences each could have.
- To counter such threats, business should create a plan to act promptly.
- IT equipment includes the following and more: Computers, Portable devices, Servers, Backup storage devices, Printers and multifunctional devices.
- You should assess how the following risks would affect each item.
- It will also help you to assess each item's importance on the overall business functions and continuity.