MDKAMIL

DISCLIMER

THIS BOOK IS FOR EDUCATION PURPOSE ONLY .

DOWNLOAD TECHNOLOGY 1 FORM THE QR CODE FROM HERE.

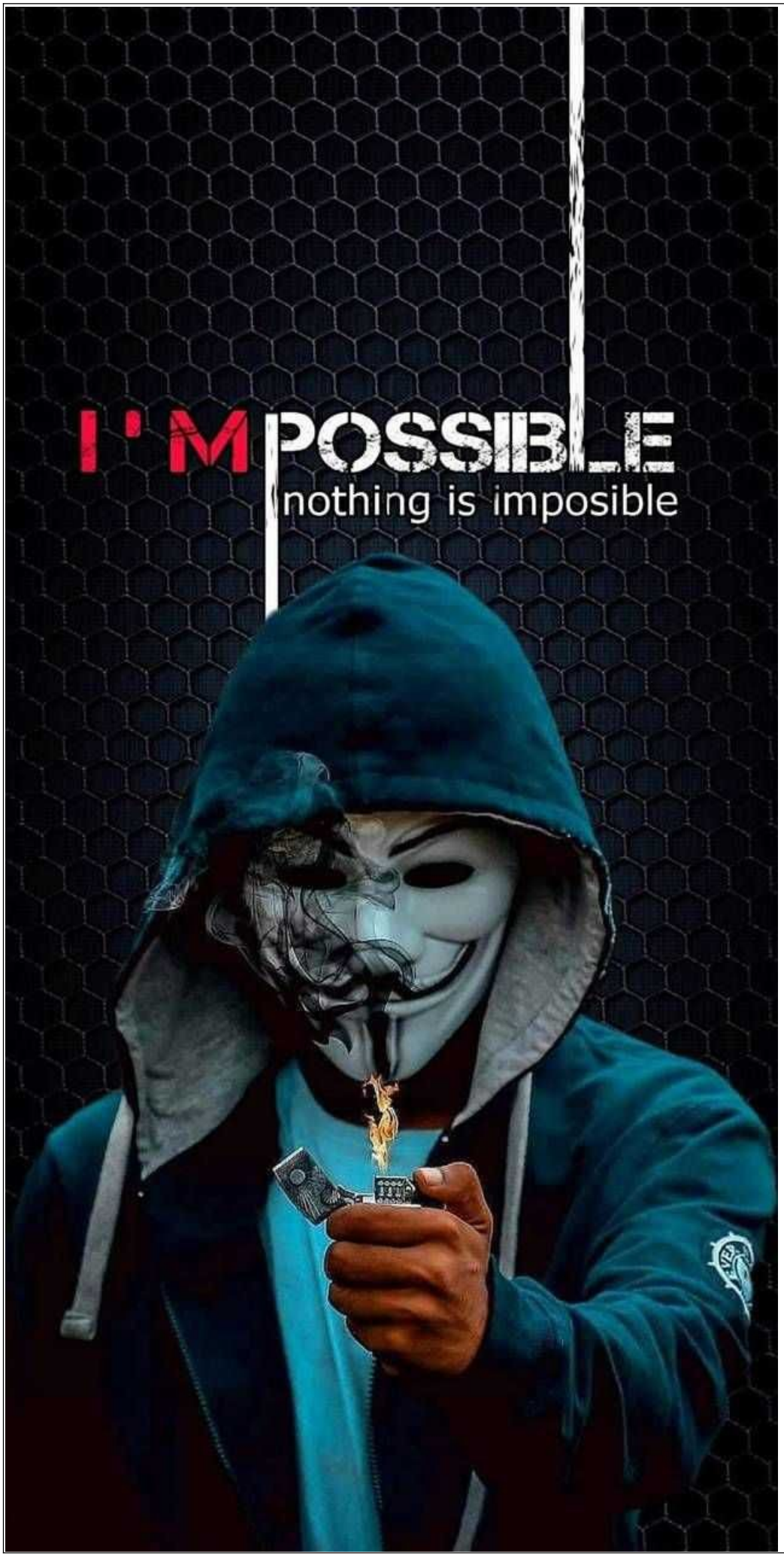
COPYRIGHT

THIS BOOK IS MY OWN CREATION AND AND WE ARE NOT RESPONSIBE AND WE ARE NOT SUPPORT FOR ANY KIND OF ILLIGAL ACTIVITIES ….

[SOCIAL ENGINEERING]

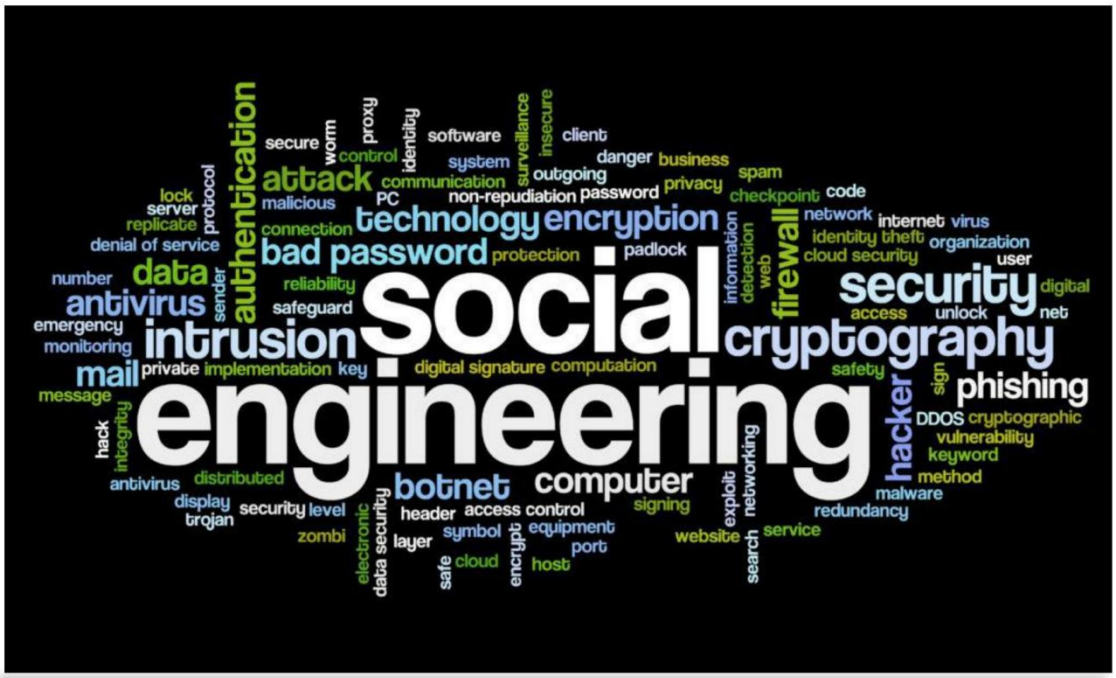
Volume-1

[MD KAMIL]


I'M POSSIBLE
nothing is imposible

DIGITAL SOCIAL ENGINEERING TACTICS

HERE ARE A FEW COMMON TACTICS USED
THROUGH EMAIL, WEBSITES AND SOCIAL MEDIA:



Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In Cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can

happen online, in-person, and via other interactions. How Does Social Engineering Work?

Prepare by gathering background information on you or a larger group you are a part of.

1. Infiltrate by establishing a relationship or initiating an interaction, started by building trust.
2. Exploit the victim once trust and a weakness are established to advance the attack.
3. Disengage once the user has taken the desired action.

Phishing Attacks

Phishing attackers pretend to be a trusted institution or individual in an attempt to persuade you to expose personal data and other valuables.

Attacks using phishing are targeted in one of two ways:

1. **Spam phishing,** or mass phishing, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.
2. **Spear phishing** and by extension, **whaling** , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.

Whether it's a direct communication or via a fake website form, anything you share goes directly into a scammer's pocket. You may

even be fooled into a malware download containing the next stage of the phishing attack. Methods used in phishing each have unique modes of delivery, including but not limited to:

Worm Attacks

The cybercriminal will aim to attract the user's attention to the link or infected file – and then get the user to click on it.

Examples of this type of attack include:

- **The Love Letter worm** that overloaded many companies' email servers in 2000. Victims received an email that invited them to open the attached love letter. When they opened the attached file, the worm copied itself to all of the contacts in the victim's address book. This worm is still regarded as one of the most devastating, in terms of the financial damage that it inflicted.
- **The Mydoom email worm** — which appeared on the Internet in January 2004 — used texts that

imitated technical messages issued by the mail server.

In some cases, the malware creators and distributors take steps that reduce the likelihood of victims reporting an infection:

Victims may respond to a fake offer of a free utility or a guide that promises illegal benefits like:

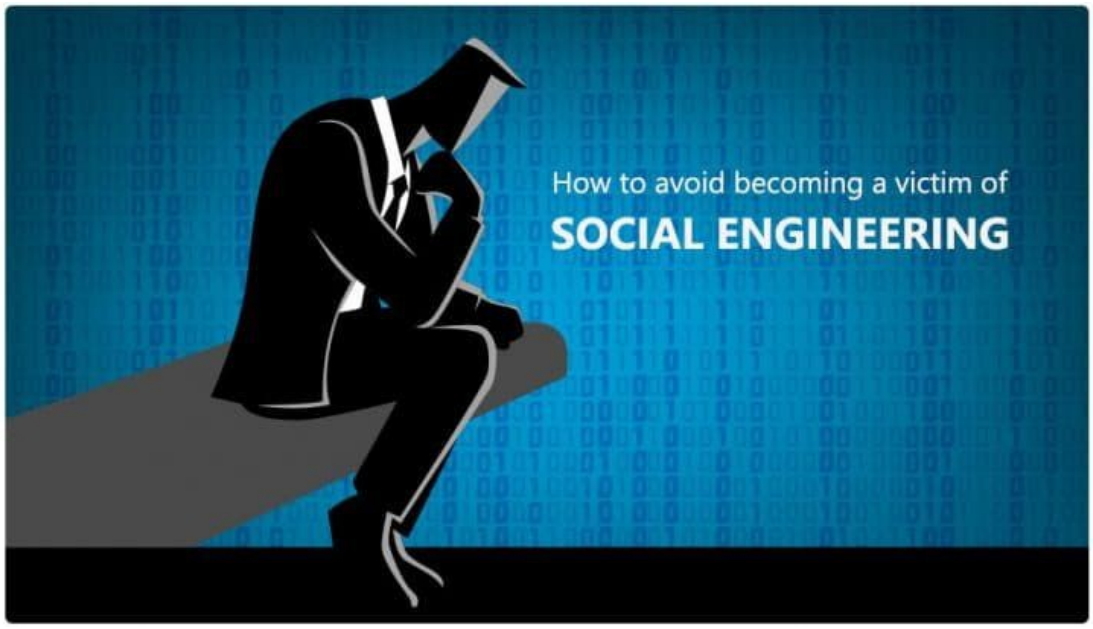
- Free Internet or mobile communications access.
- The chance to download a credit card number generator.
- A method to increase the victim's online account balance.

In these cases, when the download turns out to be a Trojan virus, the victim will be keen to avoid disclosing their own illegal intentions. Hence, the victim will probably not report the infection to any law enforcement agencies.

As an example of this technique, a Trojan virus was once sent to email addresses that were taken from a recruitment website. People that had registered on the site received fake job offers, but the offers included a Trojan virus. The attack mainly targeted corporate

email addresses. The cyber criminals knew that the staff that received the Trojan would not want to tell their employers that
they had been infected while they were looking for alternative employment.

How to Prevent Social Engineering Attacks



Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users.

Here are some important ways to protect against all types of cyberattacks:

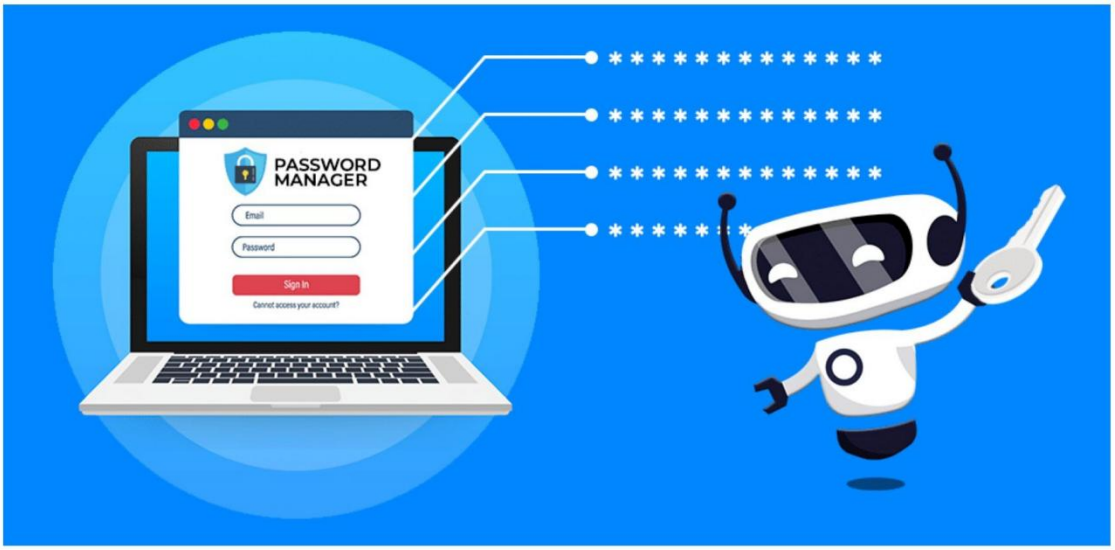
Safe Communication and Account Management Habits

Online communication is where you're especially vulnerable. Social media, email, text messages are common targets, but you'll also want to account for in-person interactions as well.

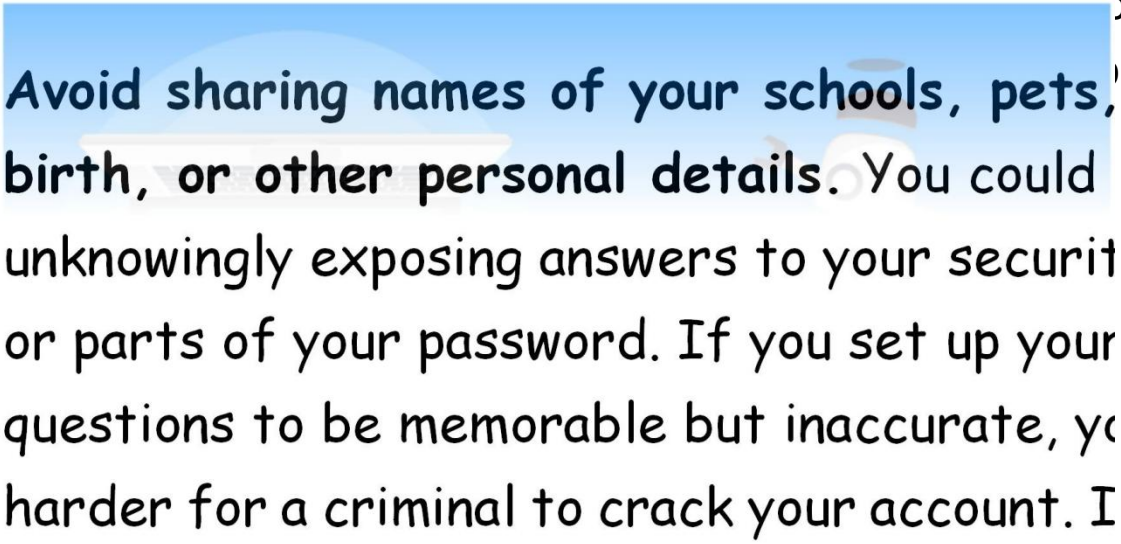
Never click on links in any emails or messages. You'll want to always manually type a URL into your address bar, regardless of the sender. However, take the extra step of investigating to find an official version of the URL in question. Never engage with any URL you have not verified as official or legitimate.

Use multi-factor authentication. Online accounts are much safer when using more than just a password to protect them. Multi-factor authentication adds extra layers to verify your identity upon account login. These "factors" can include biometrics like fingerprint or facial recognition, or temporary passcodes sent via text message.

Use strong passwords (and a password manager). Each of your passwords should be unique and complex. Aim to use diverse character types, including uppercase, numbers, and symbols. Also, you will probably want to opt for longer passwords when possible. To help you manage all your custom passwords, you might want to use a password manager to safely store and remember them.



n, or other
wers to your
o your security
harder for a
ota," writing a lie
rying hackers.



Be very cautious of building online-only friendships.

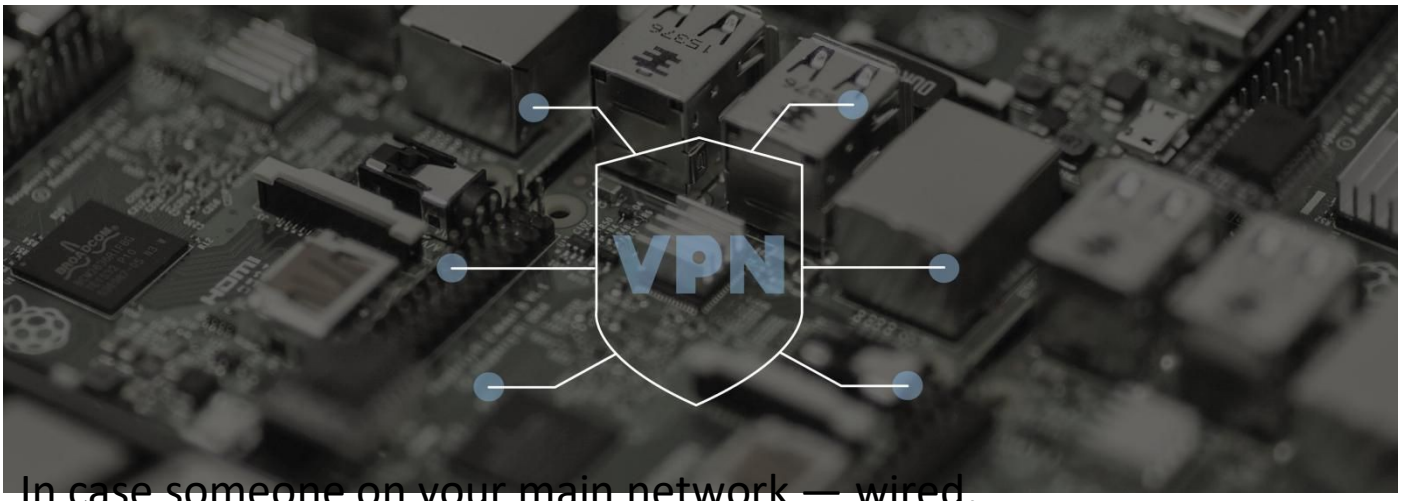
While the internet can be a great way to connect with people worldwide,
this is a common method for social engineering attacks. Watch for tells and red flags that indicate manipulation or a clear abuse of trust.

Safe Network Use Habits

Compromised online networks can be another point of vulnerability exploited for background research. To avoid having your data used against you, take protective measures for any network you're connected to.

Never let strangers connect to your primary Wi-Fi network. At home or in the workplace, access to a guest Wi-Fi connection should be made available. This allows your main encrypted, password-secured connection to remain secure and interception-free. Should someone decide to "eavesdrop" for information, they won't be able to access the activity you and others would like to keep private.

Use a VPN.



In case someone on your main network — wired, wireless, or even cellular — finds a way to intercept traffic, a virtual private network (VPN) can keep them out. VPNs are services that give you a private, encrypted “tunnel” on any internet connection you use. Your connection is not only guarded from unwanted eyes, but your data is anonymized so it cannot be traced back to you via cookies or other means.

Keepallnetwork-connecteddevicesandservicessecure.

Many people are aware of internet security practices for mobile and traditional computer devices. However, securing your network itself, in addition to all your smart devices and cloud services is just as important. Be sure to protect commonly overlooked devices like car infotainment systems and home network routers. Data breaches on these devices could fuel personalization for a social engineering scam.

Safe Device Use Habits

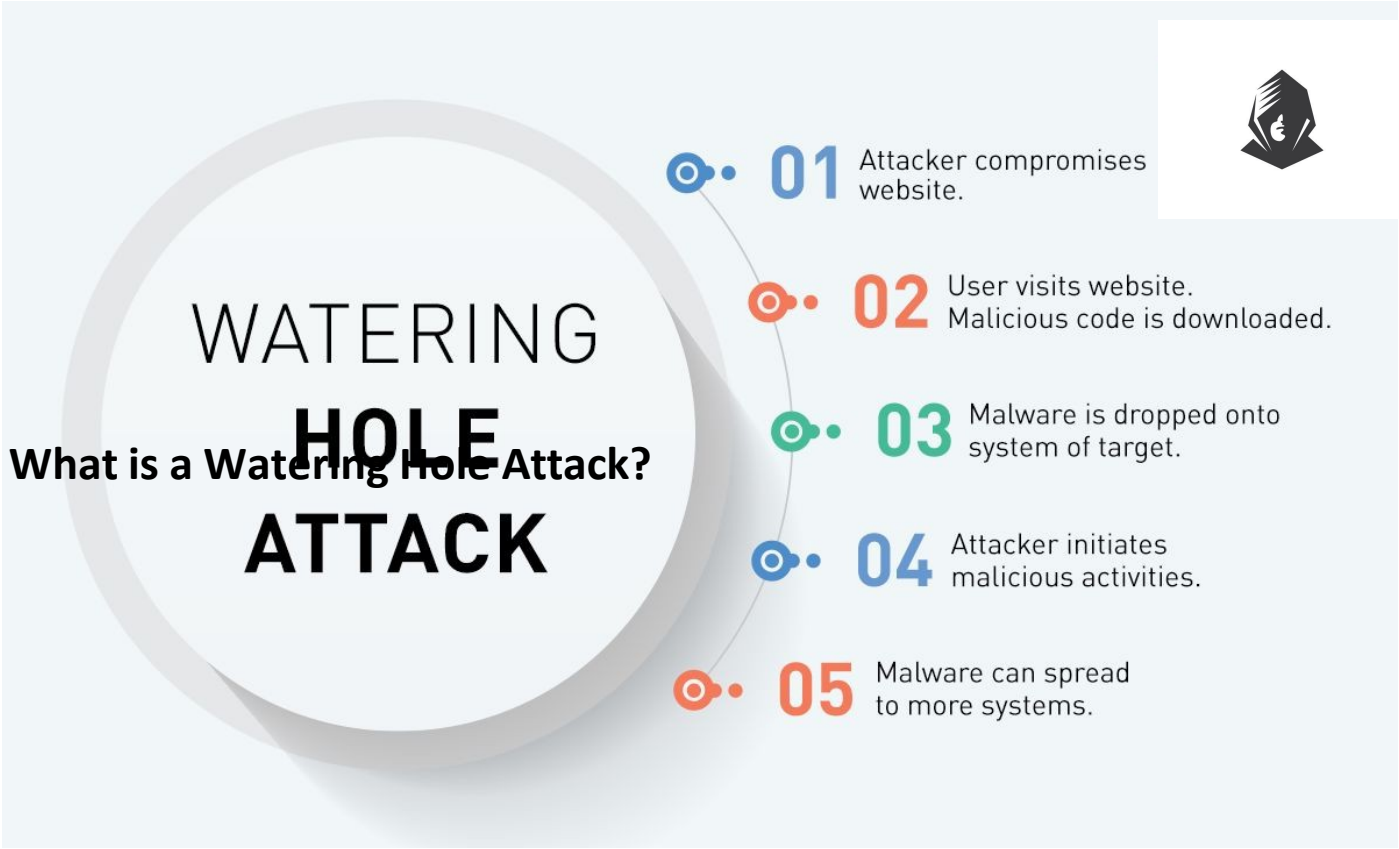
Keeping your devices themselves is just as important as all your other digital behaviors. Protect your mobile phone, tablet, and other computer devices with the tips below:

Use comprehensive internet security software. In the event that social tactics are successful, malware infections are a common outcome. To combat rootkits, Trojans and other bots, it's critical to employ a high-quality internet security solution that can both eliminate infections and help track their source.

Don’t ever leave your devices unsecured in public. Always lock your computer and mobile devices, especially at work. When using your devices in public spaces like airports and coffee shops, always keep them in your possession.

Keep all your software updated as soon as available.

Immediate updates give your software essential security fixes. When you skip or delay updates to your operating system or apps, you are leaving known security holes exposed for hackers to target. Since they know this is a behavior of many computer and mobile users, you become a prime target for socially engineered malware attacks.

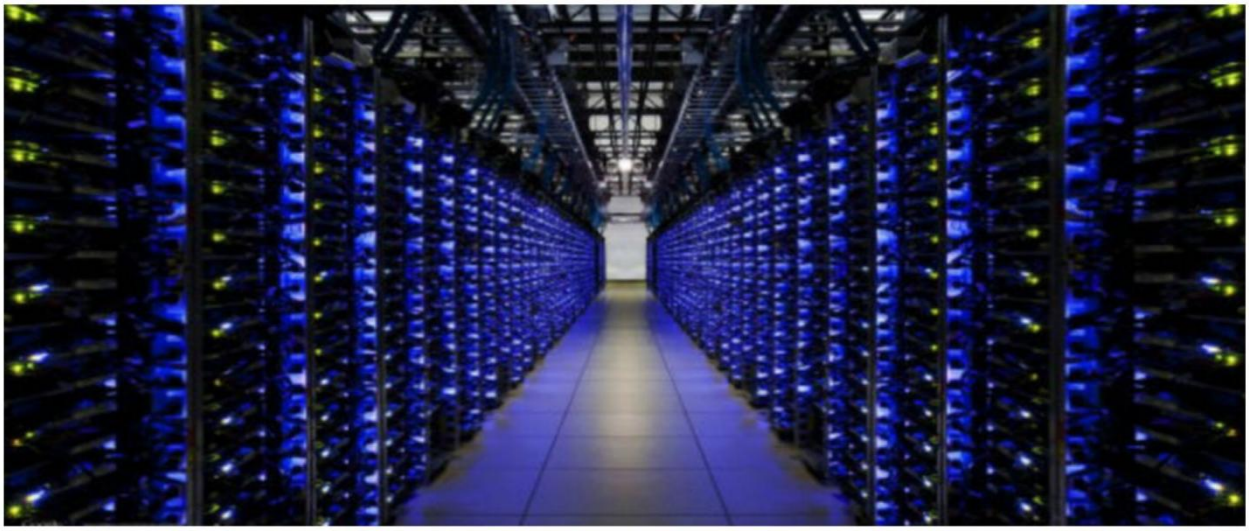


What is a Watering Hole Attack?

A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site. The end goal is to infect the users computer and gain access to the organizations network. Watering Hole attacks, also known as strategic website compromise attacks, are limitedinscopeastheyrelyonanelementof luck.They do however become more effective, when combined with email prompts to lure users to websites.Attackers thatareattempting opportunisticwateringholeattacks for financial gain or to build their botnet can achieve this by compromising popular consumer websites.

To defend against more sophisticated attackers, enterprises should consider more dynamic malware analysis solutions that check for malicious behavior on the most suspicious destination websites that user's browse to.

DO YOU HAVE SEPERATE PHONE FOR YOURSELF?



A server is **a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network**. In theory, whenever computers share resources with client machines they are considered servers. ... This means that a device could be both a server and a client at the same time.

Uses of server

The role of a server is **to share data as well**

as to share resources and distribute work. A

server computer can serve its own computer

programs as well; depending on the scenario, this could be part of a quid transaction, or simply a technical possibility.

Hacking the server

There are two primary ways a server may be compromised: **The hacker has guessed a password of a user on the server.** This may be a email, ftp, or ssh user. The hacker has gained access through a security hole in a web application (or its addons/plugins) such as WordPress, Joomla, Drupal, etc.

Hackers can remotely scan servers to determine vulnerabilities within that system. Once they find a vulnerability, they exploit it by sending a command or data to the server that will cause the application to crash and will then start executing code.

Nmap Hacking Tool

- Gordon Lyon created an open-source tool called Nmap stands for Network Mapper  in the year 1997, mainly used for Network Discovery and Security Auditing.
- Nmap is one of the best scanning tools for Ethical Hacking and supports all major OS such as Windows, Linux and, Mac OS.

Nmap Hacking Tool Feature

- Nmap is used for auditing to identify the target host.
- Hacking tool Identify new servers.
- Query a host for DNS and Subdomain search.
- Find Vulnerabilities on a network and Exploit them.

Using Nmap you can:

- Audit device security.
- Detect open ports on remote hosts.
- Network mapping and enumeration.
- Find vulnerabilities inside any network.
- Launch massive DNS queries against domains and subdomains.

Price: Free

Website: Nmap

2. Burp Suite Hacking Tool

- Burp Suite was developed by **Dafydd Stuttard** (Founder of Portswigger) widely used to perform security testing on web applications.
- Burp Suite hacking tools contain numerous powerful features which support both manual and automation

testing for efficiency and make it highly configurable to even the most experienced testers.

Burp Suite Hacking Tool Features

- HTTP message editor.
- Login Sequence Recorder permits the programmed filtering.
- Survey weakness information with built-in vulnerability management.
- Automate scan and filter.
- Effectively give a wide assortment of specialized and consistent reports.
- Identifies critical vulnerabilities with 100% accuracy.
- Target Analyzer.
- Content Discovery.
- Task Scheduler.
- CSRF PoC Generator.

Price:

1. Community edition – Free.
2. Enterprise edition – starts at $3999/ yr.
3. Professional edition- starts at $399/use/yr.

Website: Burp Tool

3. Netsparker

Netsparker was created by Ferruh Mavituna, Peter Edgeler, and Mark Lane in 2009, is one of the website hacking tools, capable of automatically finding SQL Injection, XSS, and other vulnerabilities.

Features of Netsparker

- Proof-Based Scanning Technology helps in vulnerability detection.
- Netsparker automatically detects custom 404 error pages, URL rules, etc.
- REST API for consistent combination with the SDLC, bug tracking systems, etc.
- Completely flexible solution. Scan 1,000 web applications in just 24 hours.

4. Acunetix

Acunetix was developed by Ferruh Mavituna, founder of Netsparx which is a fully automated Ethical Hacking solution that scans single-page applications, javascript, etc… It can prioritize the risk and audit complex, authenticated web apps through a single, consolidated view.

Features:

- Scans for all variants of SQL Injection, XSS, and 4500+ vulnerabilities.
- Identifies over 1200 WordPress core, theme, and plugin vulnerabilities.
- Fast & Scalable – thousands of pages without interruptions.
- Available On-Premises and as a Cloud solution.
- Integrates with mainstream WAFs and Issue Trackers to help in the SDLC.

Price: Pricing Model – Free trial for 14 days

Website: Acunetix

5. Metasploit

Metasploit was founded by H. D. Moore which is mainly used for penetration testing

Features:

- It is useful for knowing about security vulnerabilities.
- Helps in penetration testing.
- Helps in IDS signature development.

- You can create security testing tools.

Price:

1. Open-source tool – Free download.
2. Metasploit Pro is a commercial product- a Free trial available for 14 days.

Website: Metasploit

6. Aircrack-Ng

Aircrack is one of the trustable Ethical Hacking tools which is mainly used for vulnerable wireless connections.

Features:

- It can focus on de-authentication, fake access points, etc.
- It supports exporting data to text files.
- It can check Wi-Fi cards and driver capabilities.
- FMS, PTW attacks are used to crack WEP keys.
- Dictionary attacks are used to crack WPA2-PSK.

Website: Aircrack-Ng

7. Ettercap

Ettercap is an Ethical Hacking tool that supports cross-platform which is used for network and host analysis. Ettercap can help you in creating plugins.

- **Features:**
- Sniffing of live connections.
- Content filtering.
- Active and passive dissection of many protocols.
- Network and host analysis.
- Allows creation of custom plugins using Ettercap's API

Website: Ettercap

8. John The Ripper

John the Ripper is developed by the Unix Operating system and this is one of the popular password cracking tools. Most of the Pen testers and Ethical Hackers prefer John to ensure security due to its e ability to auto-detect password hash types.

Features:

- John the Ripper is mainly used for testing encrypted passwords.
- It performs dictionary attacks.

- It provides various password crackers in one package.
- It provides a customizable cracker.

9. Wireshark

- Gerald Combs, The founder wanted a tool for tracking network problems, so he started writing “Wireshark” (previously known as Ethereal).
  This tool helps in analyzing the packets and perform deep inspection of many protocols.

Features:

- Wireshark can decompress the gzip files.
- Protocols like IPsec, ISAKMP, etc can be decrypted by Wireshark.
- It can perform live capture and offline analysis.
- Wireshark captures network data using GUI or TTY-mode TShark utility.

10. Angry IP Scanner

This is an open-source and cross-platform Ethical Hacking tool that mainly helps in scanning the IP addresses and ports.

Features:

- This is a free and open-source hack tool.
- Random or file in any format.
- Exports results in many formats.
- Extensible with many data fetchers.
- Provides command-line interface.
- No need for Installation.

Conclusion

With the increase in technology, most of the industry prefers ethical hacking to secure their businesses with the help of **Ethical Hacking tools**. The above-listed tools are the top 10 ethical hacking tools to look for in 2022. If you wish to become an ethical hacker and build a promising career in cybersecurity, check Cyber Security Course offered by Sandford Universities.

CYBER SECURITY

8 Common Cybersecurity Responsibilities

- Access Controls. ...
- Application and Network Performance. ...
- Patch Management. ...
- Vulnerability Management. ...
- Endpoint Detection and Response (EDR) ...

- Business Continuity Planning (BCP) ...
- Backup and Disaster Recovery (BDR) ...
- Cybersecurity Training.

What Are the Different Roles in Cyber Security?

“Organizations are still working hard to accurately define the expectations of cyber security roles and how those roles fit into the bigger organizational picture,” said Backherms.

The specific job responsibilities for any given cyber security role can also depend on the size and resources of the employer. “At a smaller or mid-size firm, you might end up being a ‘jack of all trades,’ while at a larger firm you’re more likely to have specialists,” said Champion.

Cyber security professionals can benefit from starting as generalists and then specializing in an area of interest or strength, according to Champion. These areas can include:

- Application security
- Data loss prevention
- Forensics

- Incident response
- Network security
- Security architecture
- Threat intelligence
- Vulnerability management

Whether you're a generalist or a specialist, you'll need to keep up with cyber security's ever-changing changing technical requirements, latest legal regulations and best practices as well as the emerging trends in the industry in order to achieve your career goals. To that end, consider:

Taking coursework toward a degree (such as a bachelor's or master's in cyber security) or certification that aligns with your career aspirations

- Upskilling in virtual labs to practice industry applications and technologies
- Completing a cyber internship
- Joining a professional organization or association, such as ISACA, Information Systems Security Association (ISSA), (ISC)² or the SANS Institute
- Networking or finding a mentor to help you outline and achieve your medium- and long-term plans

Such opportunities are available to current college students, newly minted graduates and seasoned career-changers alike, said Champion.

Evans, for example, earned his undergraduate degree in information technology, worked in various IT roles (server administrator, database administrator, desktop support) and then earned his MBA before transitioning to a dedicated cyber security role.

"I didn't necessarily count myself as a security individual, but I've always been security-minded," he said. When the right cyber security career opportunity presented itself through his professional networks, Evans was upfront with the hiring managers about the training he would need to be successful in the role. "The company gave me

a trial run and said, 'You should probably get your CISO certification within a year.' I finished it within two months." He's now senior vice president and CISO at a large, full-service, regional bank and recently got certified as a data privacy solutions engineer.

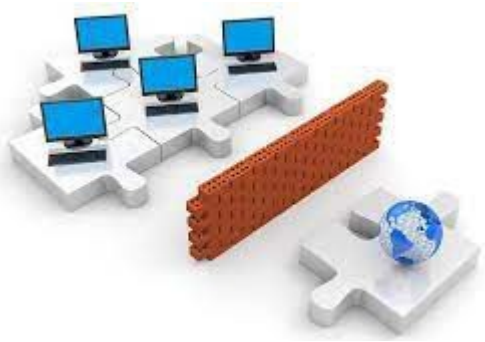
As you continue to gain experience and expertise during your career, you might set your sights on pursuing cyber security positions or opportunities in:

- **Leadership** – Senior- or executive-level roles typically require solving higher-order problems, making strategic decisions, building teams and processes while collaborating across business divisions. "Every day is different for a CISO," said Evans. "Sometimes it's a high-stress situation and everyone looks to you for direction and answers. That means you have to think fast and your decisions can have significant consequences."
- **Consulting** – According to Royster, the best cyber security consultants have not only the technical chops, but also considerable experience with recognized organizations across multiple industries – in addition to the presentation and interpersonal skills needed

to engage with IT-savvy clients. “You need to be able to talk the talk. So, find your niche, master those skills, and then see if consulting is the right fit for you,” he said.

- **Education** – Cyber security professionals can also explore opportunities teaching or mentoring, both formally and informally. “Teaching, for me, is a way to give back to the field,” said Champion. “It’s still a fairly small community and – perhaps selfishly – I want the next generation of people potentially working for me to keep moving our field in the right direction.”

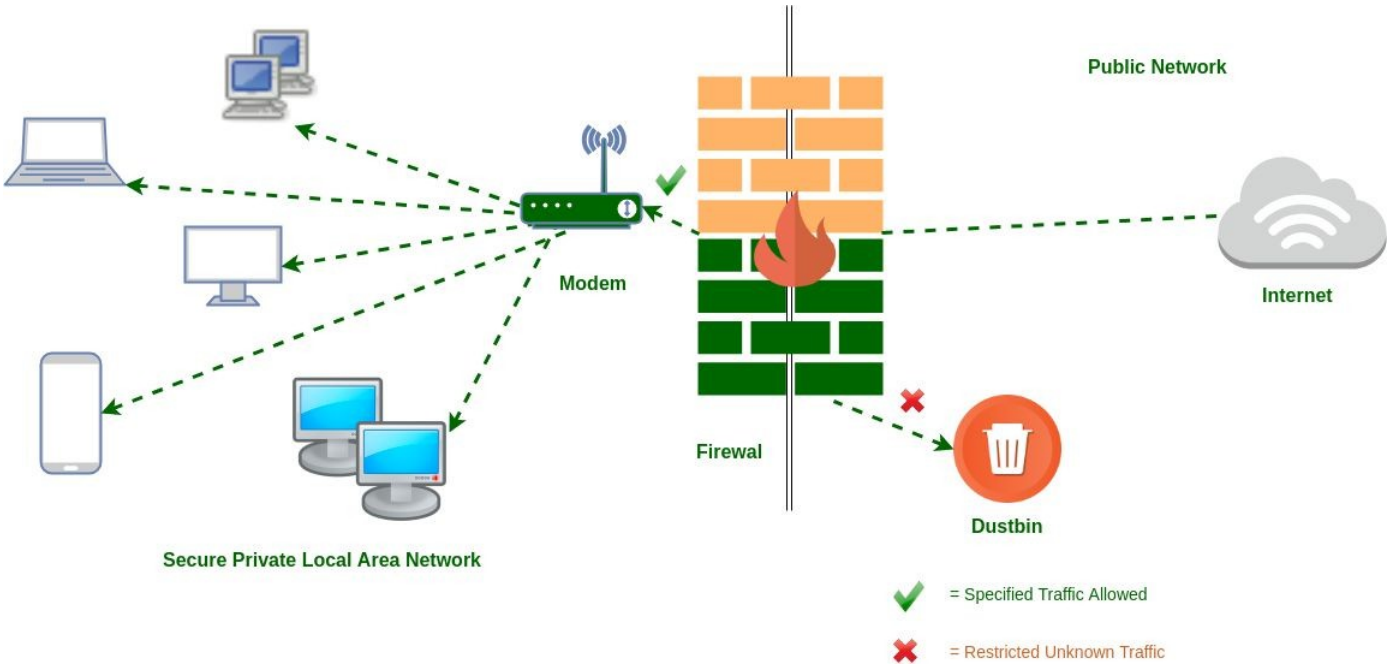
FIREWALL --CYBERSECURITY

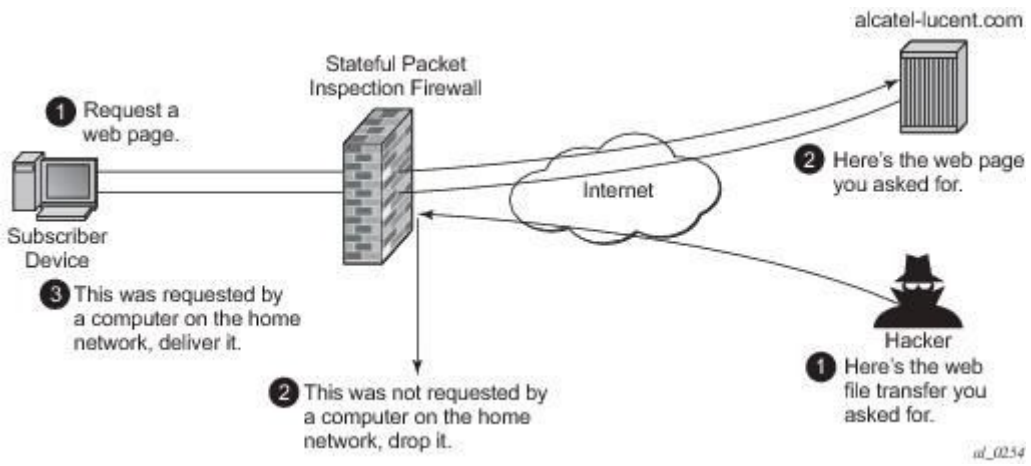


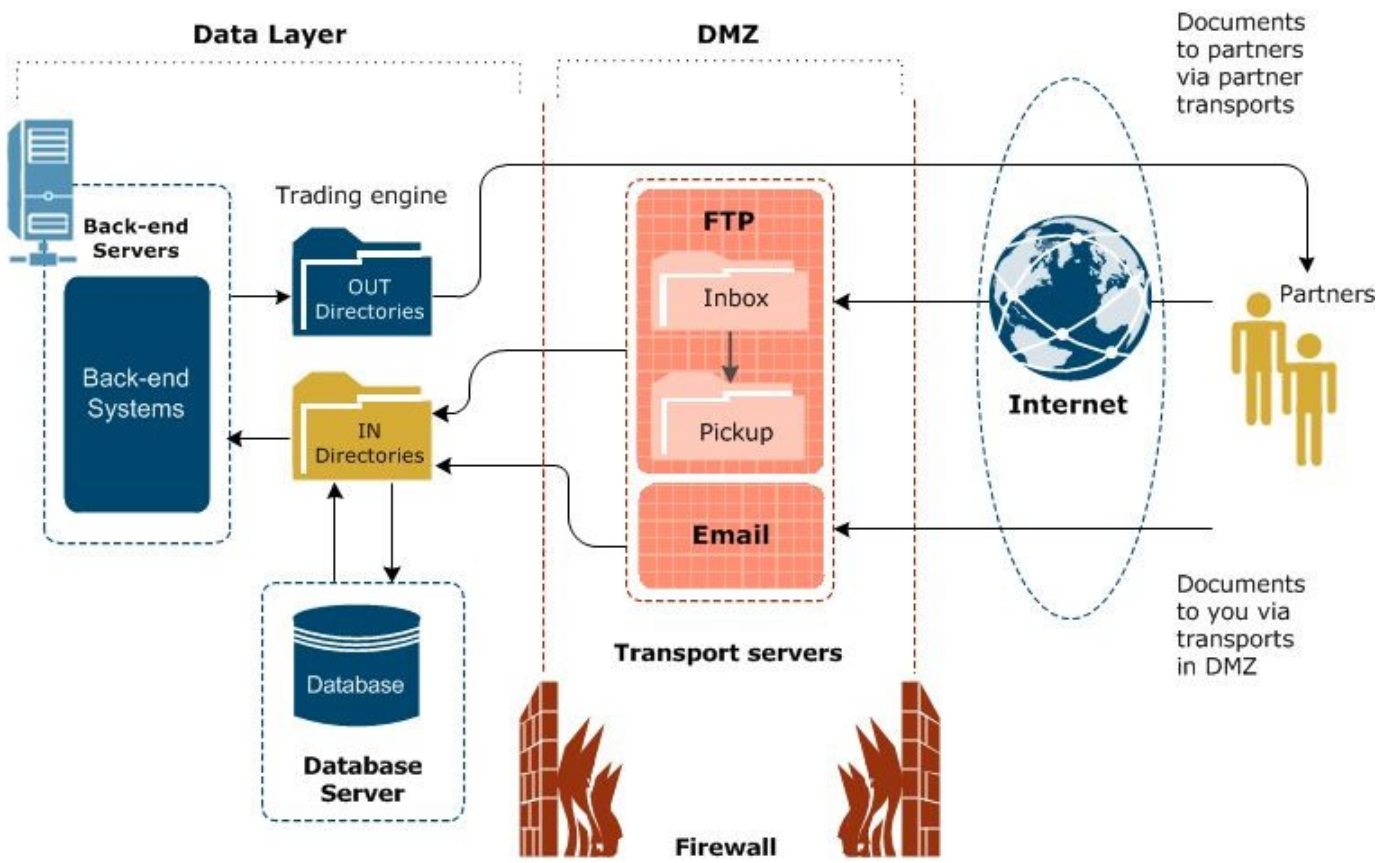
A firewall is **a network security device that monitors incoming and outgoing network traffic** and decides whether to allow or block specific

traffic based on a defined set of security rules.

There are three basic types of firewalls that are used by companies to protect their data & devices to keep destructive elements out of network, viz. **Packet Filters, Stateful Inspection and Proxy Server Firewalls**.







There are three basic types of firewalls that are used by companies to protect their data & devices to keep destructive elements out of network, viz. Packet Filters, Stateful Inspection and Proxy Server Firewalls. Let us give you a brief introduction about each of these.

- Packet Filters

Packet Filter Firewall controls the network access by analyzing the outgoing and incoming packets. It lets a packet pass or block its way by comparing it with
pre-established criteria like allowed IP addresses, packet type, port number, etc. Packet filtering technique is suitable for small networks but gets complex when implemented to larger networks. It is to be noted that these types of firewalls cannot prevent all types of attacks. They can neither tackle the attacks that use application layers vulnerabilities nor can fight against spoofing attacks.

- Stateful Inspection

Stateful Packet Inspection (SPI), which is also sometimes called dynamic packet filtering, is a powerful firewall architecture

which examines traffic streams from end to end. These smart and fast **firewalls** use an intelligent way to ward off the unauthorized traffic by analyzing the packet headers and inspecting the state of the packets along with providing proxy services. These firewalls works at the network layer in the OSI model and are more secured than the basic packet filtering firewalls.

- Proxy Server Firewalls

Also called the application level gateways, Proxy Server Firewalls are the most secured type of firewalls that effectively protect the network resources by filtering messages at the application layer. Proxy **firewalls** mask your IP address and limit traffic types. They provide a complete and protocol-aware security analysis for the protocols they support. Proxy Servers offers the best Internet experience and results in the network performance improvements.

This is all about the basic firewalls that are configured to protect a private network. No matter which firewall you choose, ensure a proper configuration as any loophole can cause more damage to you than no firewall at all. Create a secure network and deploy a suitable firewall to limit the access to your computer and network.

PENETRATION TESTING

C|PENT

Certified Penetration Testing Professional

Penetration testing, or pen testing, is the process of

attacking an enterprise's network to find any vulnerabilities that could be present to be patched

Ethical hackers and security experts carry out these tests to find any weak spots in a system's security before hackers with malicious intent find them and exploit them. Someone who has no previous knowledge of the system's security usually performs these tests, making it easier to find vulnerabilities that the development team may have overlooked. You can perform penetration testing using manual or automated technologies to compromise servers, web applications, wireless networks, network devices, mobile devices, and other exposure points.

Qualification

However, many pen testing jobs require bachelor's or master's degrees in Cyber security, computer science, or IT. Computer science or IT degree programs provide fundamental technical skills in operating systems, programming languages, network tools, and computer hardware and software.

Penetration testing is an unusual job. You break into companies through their technology and then show them where their weaknesses lie so they can fix them. It's a

jobforgoodpeoplewiththeabilitytodobad things.

AUTHOR BY,

MDKAMIL

HACKING WITH KALI

Kali Linux is mainly used for advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering

Reverse engineering is a process or method through the application of which one attempts to understand through deductive reasoning how a device, process, system, or piece of software accomplishes a task with very little insight into exactly how it does so.

ROBOTICS

Robotics is an interdisciplinary branch of computer science and engineering. Robotics involves design, construction, operation, and use of robots. The goal of robotics is to design machines that can help and assist humans. ... Robots can take on any form, but some are made to resemble humans in appearance.

As the field of robotics grows ever more sophisticated, a greater number of technicians are required to lend their talents to design, program, and maintain robots and robotic systems. Not surprisingly, the complexity of these machines and systems has spawned five specialized areas within the field of robotics:

1. **Operator interface**
2. **Mobility or locomotion**
3. **Manipulators & Effectors**
4. **Programming**
5. **Sensing & Perception**

Since the development of today's most advanced robotic systems is no easy endeavor, those tasked with their design, programming and maintenance often look to hone in on a particular field of expertise. This article will explore those fields in greater detail.

Operator Interface

A robot is only as good as its ability to effectively communicate with a human controller. The operator interface – commonly referred to as a Human Robot Interface – is the medium that allows the user and the robot to communicate.
Most specifically, it is the method by which a human operator can give pre-programmed commands for the robot to execute.

A gaming controller is an example of a basic Human Robot Interface (HRI). It allows a player to issue a set of commands to the system, which are then executed in the game. In manufacturing, an industrial touchscreen computer on a piece of equipment or in a centralized control room is also a form of HRI. The operator can issue commands to the conveyor or other device to execute on the factory floor.

A great deal of care needs to go into the design of HRIs. They must be intuitive to use, and enable operators to

communicate effectively with the robot, in order to execute tasks accurately and efficiently.

Mobility or Locomotion

In order for a robot to complete a task, it needs to be able to move in its environment. In robotics, this movement is called locomotion. Mobility in robotics is achieved in many different ways. For example, some robots mimic human movement, like those used on assembly lines or those whose design is based on human anatomy. Flying robots and drones make use of propellers and other propulsion systems. Other robots, such as the rovers deployed on Mars and other celestial bodies, require wheels to get around. In short, the environment a robot will be used in often determines how the engineer will design the mobility system.

Manipulators & Effectors

For any robot to be worthwhile, it must be able to interact with its environment; that's where manipulators and effectors come into play. These are the parts of the robot that allow it to pick up objects and move them, or manipulate items that are separate from the system. Human-like robots will employ appendages and digits that work like human hands, in

order to complete a given task. In industrial settings, manipulators and effectors are perhaps more commonly represented by pincers, claws, or pushers which are all uniquely suited to move heavy pieces of equipment or materials. Like the other disciplines listed in this article, having the foundational knowledge received from robotics technician training can prepare aspiring robotics engineers and technicians for specializing in this area of robotics.

Programming

Programming is essentially the language an operator uses to communicate with the robot. Traditionally, any action that a robot was required to perform had to be programmed. These days, advanced programming allows robotic systems to learn and adapt to changes within its environment, which is truly a remarkable feat of engineering.

Generally speaking, commands can be provided by the user in real time for the robot to perform, or the robot can be programmed to perform a series of tasks, in sequence, autonomously. Regardless of the method the commands are given, each robot can be programmed using one of more than a thousand different programming languages, so an engineer

looking to specialize in this particular field of robotics will have a lot to become proficient in.

Sensing & Perception

Robots use sensors to gather information. This information lets the robot know the physical space it occupies, where it needs to go, and if any obstacles block its path. Sensors also collect information to help the robot decide how to react to objects it encounters. The right sensor must be selected for each robot's specific application to ensure that the correct decisions are made.

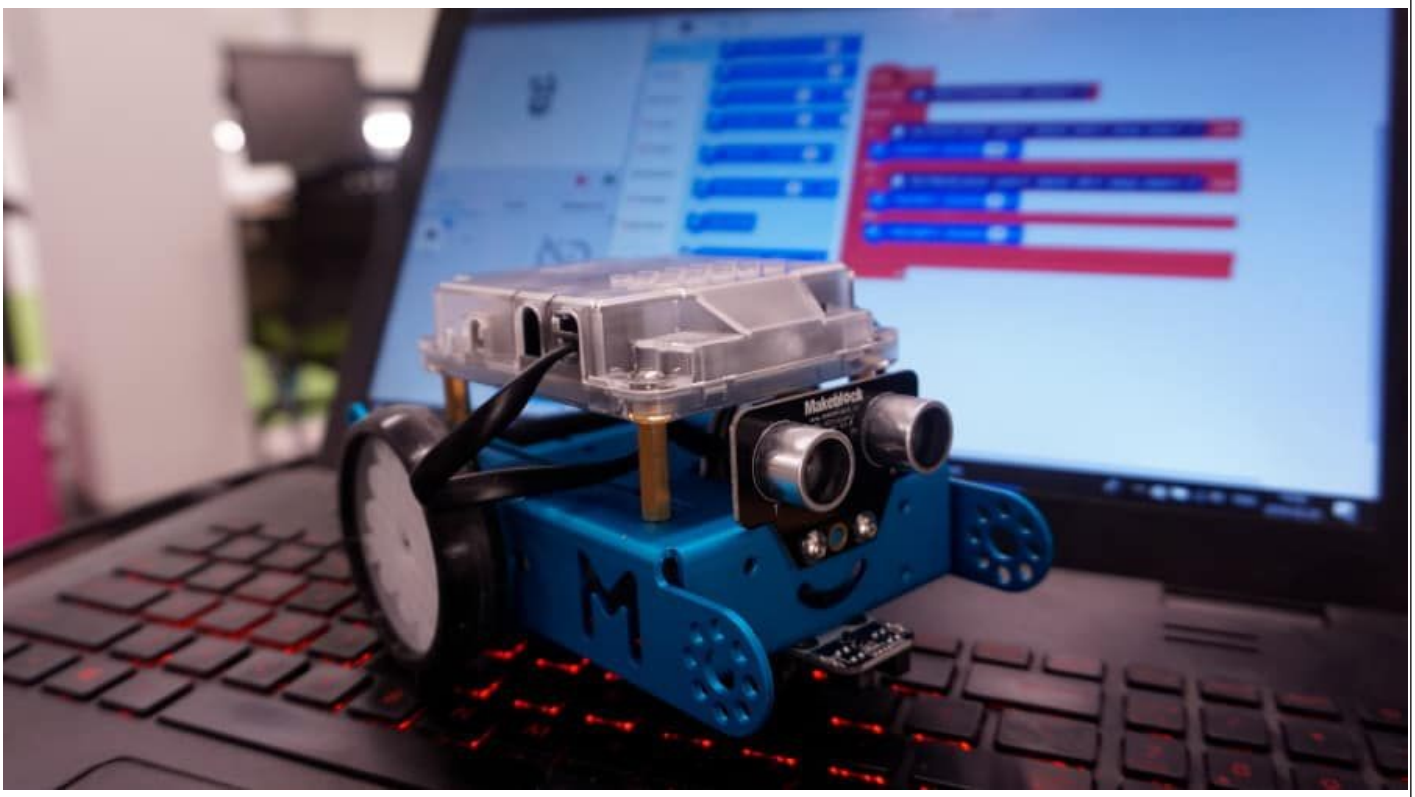
As the field of robotics expands with integration across industries, so too will the demand for experienced robotics technicians to maintain these technologies. Check out the complete Robotics Technician Training Program outline to decide if you're ready to kickstart an exciting career in this field.

Top Robotic Programming Languages

- **C/C++ The easiest way to get started with robotics is to learn C and C++……**
- **Python. Python is a powerful programming language that may be used to create and test robots. ...**
- **Java**

- **4**
- **MATLAB**
- **Lisp**
- **Pascal**

Top Robotic Programming Languages



There are about 1500 robotic programming languages accessible worldwide. They are all involved in robotic training. In this section, we will go through the top programming languages accessible today.

1.

C/C++

The easiest way to get started with robotics is to learn C and C++. Both of these are general-purpose programming languages with almost identical features. C++ is a modified version of C that adds a few features. You should now see why C++ is the most popular robotic programming language. It enables a low-level hardware interface and delivers real-time performance.

C++ is the most mature programming language for getting the greatest results from a robot. C++ allows you to code in three different ways. The Constructor, Autonomous, and OperatorControl methods are among these. In this constructor mode, the initializing code runs to build a class. It will execute at the start of the program in this scenario.

It aids in the initialization of sensors and the creation of other WPILib objects. The autonomous approach guarantees that the code is executed. It only works for a set amount of time.

The robot then moves on to the teleoperation section. The OperatorControl technique is used in this case.

2. Python

Python is a powerful programming language that may be used to create and test robots. In terms of automation and post-process robotic programming, it outperforms other

platforms. You may use this to build a script that will compute, record, and activate a robot code.

It is not necessary to teach anything by hand. This enables rapid testing and visualization of the simulations, programs, and logic solutions. Python uses fewer lines of code than other programming languages. It also includes a large number of libraries for fundamental functions. Python's primary goal is to make programming easier and faster.

Any item can be created, modified, or deleted. In addition, we may code the robot's motions in the same script. All of this is accomplished with very little code. Python is among the finest robotic programming languages as a result of this.

3.

Java

Java is a programming language that enables robots to do activities that are similar to those performed by humans. It also provides a variety of APIs to meet the demands of robots. Java has artificial language characteristics to a high degree.

It enables you to construct high-level algorithms, searching, and neural algorithmic algorithms. Java also allows you to run the same code on many computers.

Java is not built into machine code since it is an interpretative language. Rather, in execution, the Java virtual computer interprets the commands. Java has become quite popular in the field of robotics as a result of this. As a result, Java is

preferable to alternative robotic programming languages. Java is used by modern AIs such as IBM Watson and AlphaGo.

4. .NET

Microsoft's .NET programming language is used to create apps with Visual Studio. It provides a good basis for anyone interested in pursuing a career in robotics. .NET is primarily used by programmers for port and socket development.

It supports various languages while allowing for horizontal scaling. It also offers a uniform environment and makes programming in C++ or Java easier. All of the tools and IDEs have been thoroughly tested and are accessible on the Microsoft Developer Network.

In addition, the merging of languages is smooth. As a result, we can confidently rank this among the best robotic programming languages.

5. MATLAB

In robotic engineering, MATLAB and its open-source cousins like Octave are extremely popular. In terms of data analysis, it

is considerably ahead of many other robotic computer languages. MATLAB is not really a programming language in the traditional sense. Yet, engineering solutions based on complex mathematics can be found here.

Robotic developers will learn how to create sophisticated graphs using MATLAB data. It is quite helpful in the development of the complete robotic system. It also aids the development of deeply established robotic foundations in the robot business. It's a tool that lets you apply your methods to simulate the outcome. Engineers may use this simulation to fine-tune the system design and eliminate mistakes.

There have been cases when MATLAB has been used to build a complete robot. As a result, it must be included among the top ten languages. Kuka kr6 is one of the greatest instances of MATLAB application. MATLAB was also used to create and simulate this robot by the developers.

6. Lisp 

One of the first robotic computer languages was Lisp. It was introduced to the market to allow computer applications to use mathematical terminology. Lisp is an AI domain that is mostly used for creating Robot Operating Systems.

Tree data structures, automated storage management, syntax highlighting, and elevated-order characteristics are among the features available. As a result, it is simple to use and aids in the elimination of implementation mistakes after an issue have been identified.

This problem-solving procedure takes place at the prototype stage, not the manufacturing stage. It also includes capabilities like the read-eval-print loop and self-hosting compilation.

7. Pascal

One of the earliest programming languages to hit the market was Pascal. It's still quite useful, especially for newcomers. It is based on the Fundamental programming language and

teaches excellent programming skills. Pascal is being used by manufacturers to create robotic programming languages.

ABB's RAPID and Kuka's KRL are two examples. Nevertheless, most developers consider Pascal to be obsolete for everyday use. They've also highlighted its significance for newcomers.

It will assist you in learning other robot programming languages more quickly. This is only recommended for complete novices. When you've gained some expertise in robotics programming, you can transition to another language.

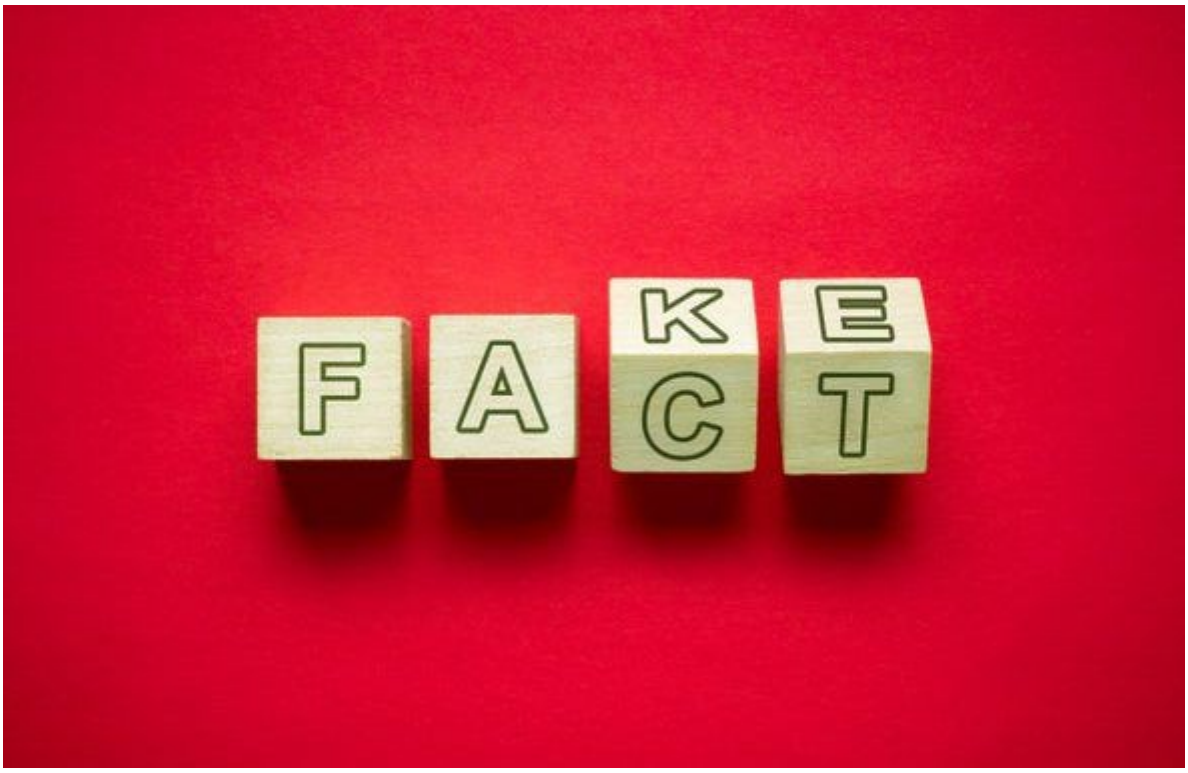
Remote Server Administration Tools

A Remote Access Trojan (RAT) is a tool used by malware developers to gain full access and remote control on a user's system, including mouse and keyboard control, file access, and network resource access.

Remote Access Trojans (RATs) use the victim's access permissions and infect computers to give cyberattackers unlimited access to the data on the PC. ... RATs include backdoors into the computer system and can enlist the PC into a botnet, while also spreading to other devices.

How to Protect Yourself from RAT Malware

#1. Never download something from unreliable sources



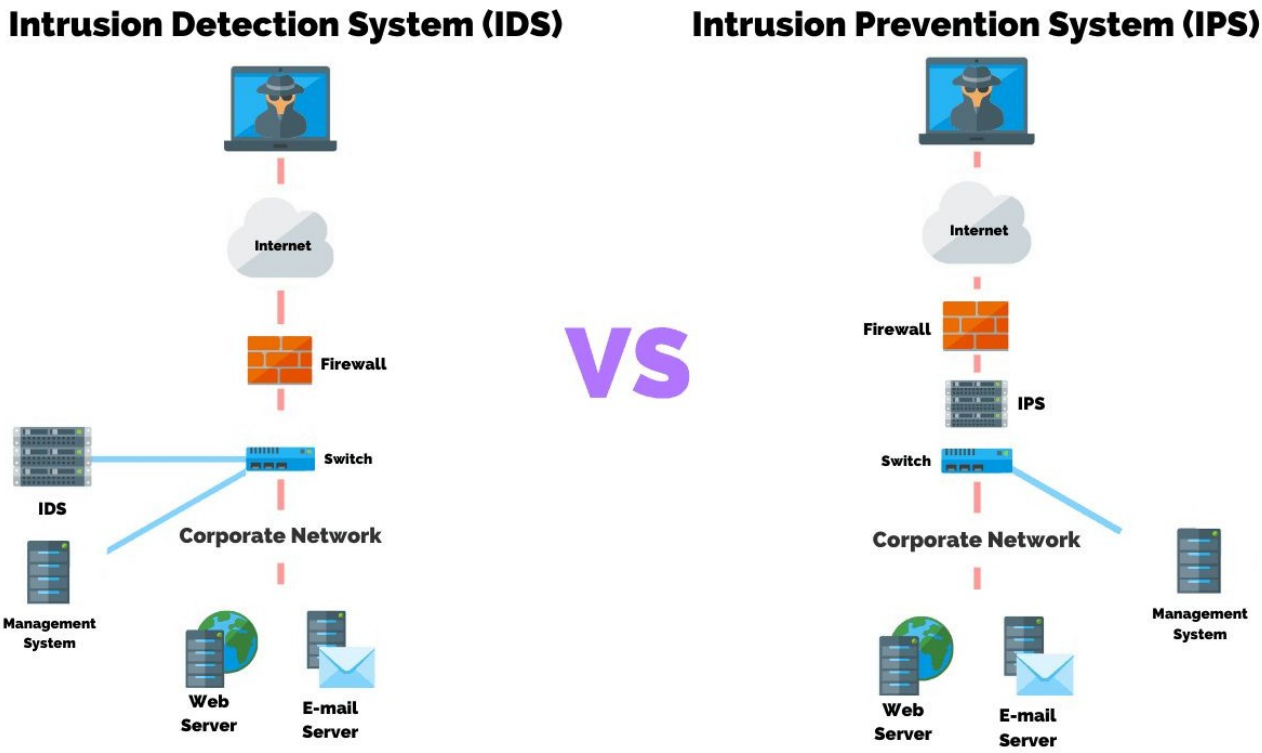
It may sound simple or obvious, but it’s the most effective way to avoid your system being infected with a Remote Access Trojan. Don’t open email attachments from people you don’t know (or even from people you do know if the message seems

off or suspicious in some way), or from untrustworthy websites. Additionally, always make sure your browsers and operating systems are patched and updated.

#2. Keep your antivirus software up to date

Home and small business networks can often benefit from antivirus software like our Heimdal™ Threat Prevention. If you didn't know about our product, Heimdal™ Threat Prevention is built to protect its customers from attacks like malware and ransomware traditional antivirus can't detect. It can block different malware infection sources such as malicious email attachments, infected links you may receive in your email, infected web pages or malicious web apps that appear legitimate at first, but aimed at spreading ransomware.
However, please keep in mind that antivirus software will not do much good if you are actively downloading files and installing programs you shouldn't.

#3. Use intrusion detection systems



This is the most efficient option for larger organizations. The intrusion detection system can be either host-based (HIDSs) or network-based (NIDSs). While HIDS is installed on a specific device and monitors log files and application data for signs of malicious activity, NIDS tracks network traffic in real-time seeking suspicious behavior. Used together, the two create a security information and event management system (SIEM), that can help block software intrusions that have slipped past firewalls, antivirus software, and other security solutions.

EDGE COMPUTING

Formerly a new technology trend to watch, cloud computing has become mainstream, with major players AWS (Amazon Web Services), Microsoft Azure and Google Cloud Platform dominating the market. The adoption of cloud computing is still growing, as more and more businesses migrate to a cloud solution. But it's no longer the emerging technology trend.

Edge is.

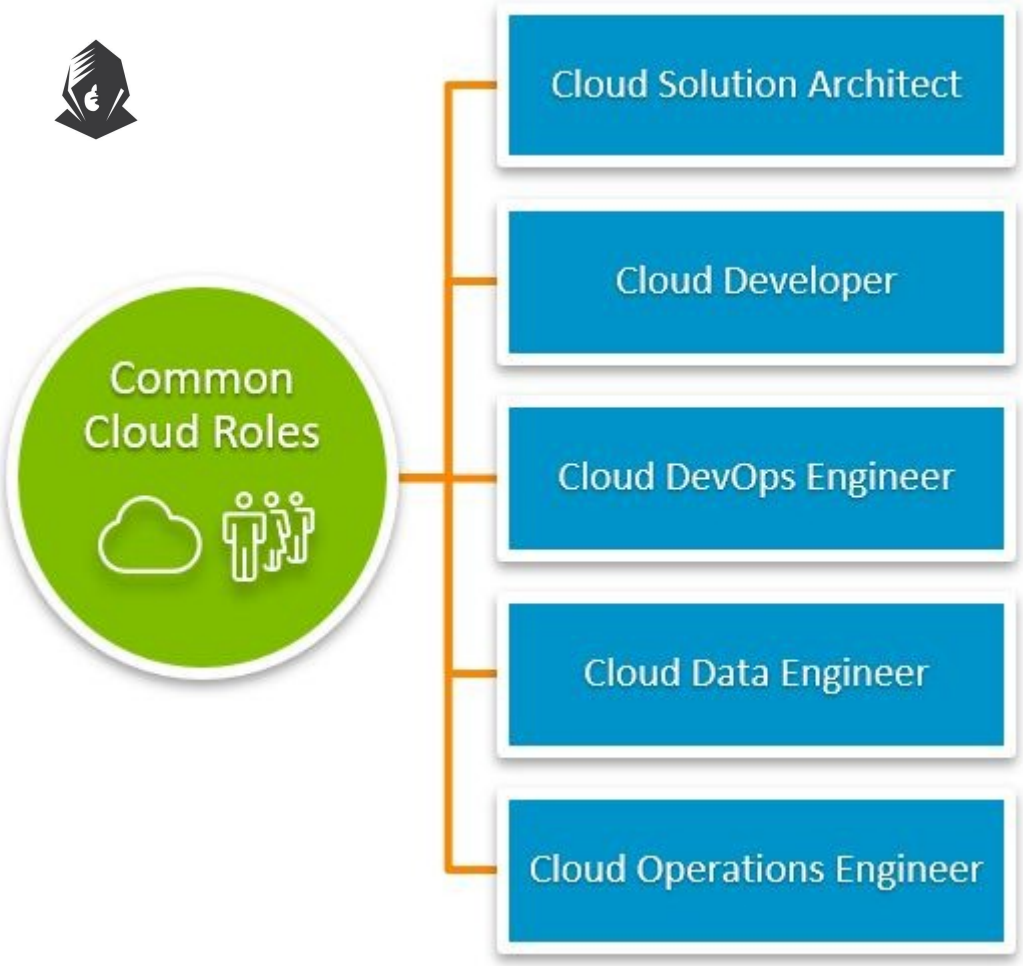
As the quantity of data organizations is dealing with continues to increase, they have realized the shortcomings of cloud computing in some situations. Edge computing is designed to help solve some of those problems as a way to bypass the **LATENCY CAUSED BY CLOUD COMPUTING AND GETTING DATA TO A DATA CENTER FOR PROCESSING.**

IT CAN EXIST "ON THE edge," if you will, closer to where computing needs to happen. For this reason, edge computing can be used to process time-sensitive data in remote locations with limited or no connectivity to a centralized location. In those situations, edge computing can act like mini data centers.

Edge computing will increase as use of the Internet of Things (IoT) devices increases. By 2022, the global edge computing market is expected to reach $6.72 billion. And this new technology trend is only meant to grow and nothing less, creating various jobs, primarily for software engineers.

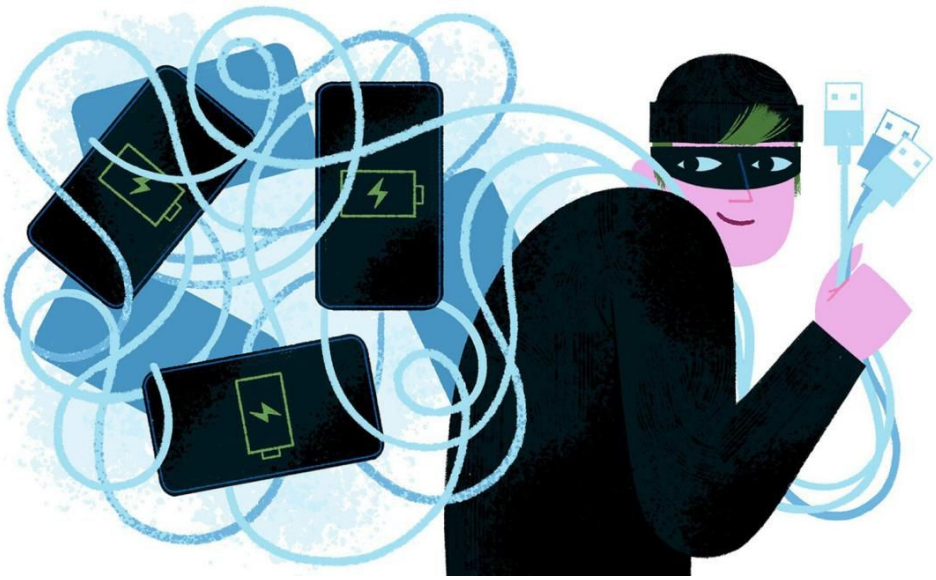
Keeping in line with cloud computing (including new-age edge and quantum computing) will help you grab amazing jobs like:

- **Cloud Reliability Engineer**
- **Cloud Infrastructure Engineer**
- **Cloud Architect and Security Architect**
- **Dev Ops Cloud Engineer**


Common Cloud Roles
Cloud Solution Architect
Cloud Developer
Cloud DevOps Engineer
Cloud Data Engineer
Cloud Operations Engineer


UPLOAD
SOCIAL NETWORK
INTERNET
$50
E COMMERCE
CLOUD COMPUTING
DOWNLOAD
INTERNET MEDIA
SECURITY SYSTEM
VPN ROUTER

OMG CABLE ATTACK



attacker can access the O.MG cable from as far as 100 meters using Wi-Fi from a regular phone, but a suitable booster antenna connected to your computer or phone could enable a connection from even further away

1The O.MG app brings up a menu with a selection of different payloads including opening a Terminal on the user's machine. Another payload allows the attacker to kill the O.MG cable's functionality remotely, perhaps to cover your tracks after an attack. Other goodies in the O.MG cable include the ability to reflash the computer, and to chain payloads together.

Custom payloads

There is also an editor and parser for Duckyscript – the scripting language used by the Rubber Ducky offensive USB

drive – which acts as a virtual keyboard and launches keystroke injection attacks. That alone opens up a wide array of custom payloads for the O.MG cable. There also appear to be attack payloads for Windows and Ubuntu systems.

In April 2019, when the video was released, MG and the team of hackers working on the embedded cable were also developing extra functions such as detecting user activity/inactivity. According to the Hak5 listing, they also appear to have cracked another key problem: USB enumeration.

When you plug in a USB device, your computer normally tries to detect it and install drivers, which can involve displaying a window. If a victim plugged in the cable without a device connected to it, that would alert them that something was amiss. However, Hak5 says that O.MG features no USB enumeration until payload execution, suggesting that the design team has achieved true stealth mode.

What to do?

- **Beware offers for cables that seem too good to be true.**
- **Don't leave your bag or computer unattended in public places.**

- **Keep your cables safe, and mark them somehow for extra-easy identification.**
- **Exercise caution when using other people's cables and chargers.**

- **the hacker.**

JUICE JACKING

Juice jacking is a security exploit in which an infected USB charging station is used to compromise connected devices. The exploit takes advantage of the fact that a

mobile device's power supply passes over the same USB cable the connected device uses to sync data.

Juice jacking exploits are a security threat at airports, shopping malls and other public places that provide free charging stations for mobile devices. At the time of this writing, the risk of becoming the victim of a juice jacking exploit is thought to be low, but the attack vector is real and is often compared to ATM card skimming exploits from years past. Both juice jacking and card skimming rely on the end user feeling confident that the compromised hardware is safe to use.

How juice jacking works

Juice jacking is a hardware-focused Man in the Middle (MitM) attack. The attacker uses a USB connection to load malware directly onto the charging station or infect a connection cable and leave it plugged in, hoping some unsuspecting person will come along and use the 'forgotten' cable.

Juice jacking exploits work because the same port used for charging a device can also transfer data. A USB connector has five pins, but only one is necessary for charging a connected device and only two of the five

pins are used to transfer data. This architecture is what allows an end user to move files between a mobile device and a computer while the mobile device is connected to the charging station.

USB ports and phone charging cables are the most common devices used in juice-jacking attacks. Other less common devices that may be used in this type of exploit include USB ports in video arcade consoles and portable battery power banks.

How to protect against juice jacking

Juice-jacking allows an intruder to copy sensitive data from a mobile device, including passwords, files, contacts, texts and voicemails. People may not realize they have been a victim of an attack or may have no way of knowing how the attack happened once they realize their device is infected. Users can guard against juice-jacking attacks by purchasing a protective attachment called a USB condom. A condom is a device that connects to a charging cable and sits between the device's charging cable and the public USB charging station.

The condom works by blocking connections to all the pins in the USB male connection except one – the pin that transfers power. The condom prevents the pins that transfer from establishing a connection, while still allowing the device to charge.

Another way to prevent this type of attack is to avoid using chargers that are left plugged into wall sockets. In addition, it is a best practice to keep devices and software programs updated and never accept free promotional charging devices or devices from unverified sources or people.

Types of juice jacking attacks

- **Data theft. In data theft juice-jacking attacks, the user is not aware that his or her sensitive information has been stolen. Depending how long a device is left plugged into a compromised cable or port, very large amounts of data may be compromised. Given enough time and storage space, hackers may even be able to make a full backup of the data on a device.**
- **Malware installation. When malware installation juice-jacking attacks occur, the malware placed on the device may do a great deal of damage, including**

manipulation of a phone or computer, spying on a user, locking the user out of the device or stealing information.

- **Multi-device attack. On top of harming the device plugged into a compromised charger, a device charged by infected cables may in turn infect other cables and ports with the same malware as an unknowing carrier of the virus.**

MDKAMIL

How to Avoid Juice Jacking

Suspendisse potenti. Vivamus non sagittis dolor. Mauris varius lorem a malesua euismod, rhoncus congue. Praesent in urna diam.

1 Cras massa neque, tristique eget

Maecenas aliquam condime risus non elementum. Vesti-bulum dui massa, molestie ac metus a, sagittis.

2 Morbi a nisl mattis, dignissim mollis

Suspendisse volutpat sit amet est a aliquet. Mauris tempus tellus sem, ac ac-cumsan nisi pharetra.

3 Donec eleifend nulla nascetur tortor

Quisque egestas cursuser sed sagittis. Donec sodales, dui eget scelerisque place-rat, purus nisl semper.

4 Ut eget elit iaculis, fermentum

Quisque egestas cursuser sed sagittis. Donec sodales, dui eget scelerisque place-rat, purus nisl semper.

5 Aenean ac vulputate ex, blandit sapien

Proin vestibulum accumsan dui vel pharetra. Quisque egestas cursus eros sed sagittis.

6 Proin dictum rutrum massa, eu ferme

Morbi vestibulum consequat eros, condimentum massa aliquam vel.