BECOME

NO ONE

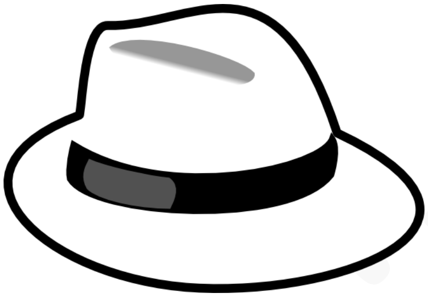
- INTERNET SECURITY AND ANONYMITY BOOK -

Written by: whiteSEC

ALL RIGHTS RESERVED.

Contents

Before you start reading, let's take a look on what kind of a user are you.



BASIC USER

You are casual PC user.

You browse the Internet.

You play games.

You use it for job or school.

ADVANCED USER

You are advanced user.

You use PC for hacking.

You visit restricted sites.

You use illegal software.

Choose which hat you belong to and get automatically sent to that part of a book.

INTRODUCTION

In this book I will pass through the all parts of online security and anonymity that every user needs to know. Beginning might be boring to you so feel free to skip it to the next page. Before we start, there is an important information that you should know: **YOU WILL NEVER BE 100% SECURED AND ANONYMOUS ONLINE.**

What is **Internet** and what is **Internet user**? **Internet** is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The **Internet** has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies.

Internet infrastructure

The communications infrastructure of the **Internet** consists of its hardware components and a system of software layers that control various aspects of the architecture. **Internet** service providers establish the worldwide connectivity between individual networks at various levels of scope. End-users who only access the Internet when needed to perform a function or obtain information, represent the bottom of the routing hierarchy.

At the top of the routing hierarchy are the tier 1 networks, large telecommunication companies that exchange traffic directly with each other via peering agreements.

Tier 2 and lower level networks buy Internet transit from other providers to reach at least some parties on the global Internet, though they may also engage in peering. An ISP may use a single upstream provider for connectivity, or implement multihoming to achieve redundancy and load balancing. Internet exchange points are major traffic exchanges with physical connections to multiple ISPs.

Large organizations, such as academic institutions, large enterprises, and governments, may perform the same function as ISPs, engaging in peering and purchasing transit on behalf of their internal networks. Research networks tend to interconnect with large subnetworks such as GEANT, GLORIAD, Internet2, and the UK's national research and education network, JANET. Both the Internet IP routing structure and hypertext links of the World Wide Web are examples of scale-free networks. Computers and routers use routing tables in their operating system to direct IP packets to the next-hop router or destination. Routing tables are maintained by manual configuration or automatically by routing protocols. End-nodes typically use a default route that points toward an ISP providing transit, while ISP routers use the Border Gateway Protocol to establish the most efficient routing across the complex connections of the global Internet.

Internet protocols

While the hardware components in the Internet infrastructure can often be used to support other software systems, it is the design and the standardization process of the software that characterizes the **Internet** and provides the foundation for its scalability and success. The responsibility for the architectural design of the Internet software systems has been assumed by the Internet Engineering Task Force (IETF).

The IETF conducts standard-setting work groups, open to any individual, about the various aspects of Internet architecture. Resulting contributions and standards are published as Request for Comments (RFC) documents on the IETF web site. The principal methods of networking that enable the **Internet** are contained in specially designated RFCs that constitute the Internet Standards. Other less rigorous documents are simply informative, experimental, or historical, or document the best current practices (BCP) when implementing Internet technologies.

The **Internet** standards describe a framework known as the Internet protocol suite. This is a model architecture that divides methods into a layered system of protocols, originally documented in RFC 1122 and RFC 1123. The layers correspond to the environment or scope in which their services operate. At the top is the application layer, space for the application-specific networking methods used in software applications. For example, a web browser program uses the client-server application model and a specific protocol of interaction between servers and clients, while many file-sharing systems use a peer-to-peer paradigm. Below this top layer, the transport layer connects applications on different hosts with a logical channel through the network with appropriate data exchange methods.

Underlying these layers are the networking technologies that interconnect networks at their borders and exchange traffic across them. The Internet layer enables computers to identify and locate each other via **Internet Protocol (IP) addresses**, and routes their traffic via intermediate (transit) networks. Last, at the bottom of the architecture is the link layer, which provides logical connectivity between hosts on the same network link, such as a local area network (LAN) or a dial-up connection. The model, also known as **TCP/IP**, is designed to be independent of the underlying hardware used for the physical connections, which the model does not concern itself with in any detail. Other models have been developed, such as the OSI model, that attempt to be comprehensive in every aspect of communications. While many similarities exist between the models, they are not compatible in the details of description or implementation. Yet, **TCP/IP** protocols are usually included in the discussion of OSI networking.

The most prominent component of the Internet model is the **Internet Protocol (IP),** which provides addressing systems, including **IP addresses**, for computers on the network. **IP** enables internetworking and, in essence, establishes the Internet itself. **Internet Protocol Version 4 (IPv4)** is the initial version used on the first generation of the Internet and is still in dominant use. It was designed to address up to ~4.3 billion (109) hosts. However, the explosive growth of the Internet has led to IPv4 address exhaustion, which entered its final stage in 2011, when the global address allocation pool was exhausted. A new protocol version, **IPv6**, was developed in the mid-1990s, which provides vastly larger addressing capabilities and more efficient routing of Internet traffic. **IPv6** is currently in growing deployment around the world, since Internet address registries (RIRs) began to urge all resource managers to plan rapid adoption and conversion.

Users

Internet usage has seen tremendous growth. From 2000 to 2009, the number of **Internet users** globally rose from 394 million to 1.858 billion. By 2010, 22 percent of the world's population had access to computers with 1 billion Google searches every day, 300 million Internet users reading blogs, and 2 billion videos viewed daily on YouTube. In 2014 the world's Internet users surpassed 3 billion or 43.6 percent of world population, but two-thirds of the users came from richest countries, with 78.0 percent of Europe countries population using the Internet, followed by 57.4 percent of the Americas.

The prevalent language for communication on the Internet has been English. This may be a result of the origin of the Internet, as well as the language's role as a lingua franca. Early computer systems were limited to the characters in the American Standard Code for Information Interchange (ASCII), a subset of the Latin alphabet.

The **Internet** allows greater flexibility in working hours and location, especially with the spread of unmetered high-speed connections. The Internet can be accessed almost anywhere by numerous means, including through mobile Internet devices. Mobile phones, datacards, handheld game consoles and cellular routers allow users to connect to the Internet wirelessly. Within the limitations imposed by small screens and other limited facilities of such pocket-sized devices, the services of the **Internet**, including email and the web, may be available. Service providers may restrict the services offered and mobile data charges may be significantly higher than other access methods.

Many people use the **World Wide Web** to access news, weather and sports reports, to plan and book vacations and to pursue their personal interests. People use chat, messaging and email to make and stay in touch with friends worldwide, sometimes in the same way as some previously had pen pals. **Social networking** websites such as Facebook, Twitter, and Myspace have created new ways to socialize and interact. Users of these sites are able to add a wide variety of information to pages, to pursue common interests, and to connect with others. It is also possible to find existing acquaintances, to allow communication among existing groups of people. Sites like LinkedIn foster commercial and business connections. YouTube and Flickr specialize in users' videos and photographs. While **social networking sites** were initially for individuals only, today they are widely used by businesses and other organizations to promote their brands, to market to their customers and to encourage posts to "go viral". "**Black hat**" social media techniques are also employed by some organizations, such as spam accounts and astroturfing.

Electronic business (e-business) encompasses business processes spanning the entire value chain: purchasing, supply chain management, marketing, sales, customer service, and business relationship. **E-commerce** seeks to add revenue streams using the Internet to build and enhance relationships with clients and partners. According to International Data Corporation, the size of worldwide e-commerce, when global business-to-business and -consumer transactions are combined, equate to $16 trillion for 2013. A report by Oxford Economics adds those two together to estimate the total size of the digital economy at $20.4 trillion, equivalent to roughly 13.8% of global sales.

INTERNET SECURITY

Internet resources, hardware, and software components are the target of criminal or malicious attempts to gain unauthorized control to cause interruptions, commit fraud, engage in blackmail or access private information.

Malware

Malicious software used and spread on the internet includes computer viruses which copy with the help of humans, computer worms which copy themselves automatically, software for **denial of service attacks**, **ransomware**, **botnets**, and **spyware** that reports on the activity and typing of users. Usually, these activities constitute cybercrime. Defense theorists have also speculated about the possibilities of cyber warfare using similar methods on a large scale.

Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. **Malware** is often disguised as, or embedded in, non-malicious files. As of 2011 the majority of active malware threats were **worms** or **trojans** rather than viruses.

Keyloggers

Keystroke logging, often referred to as **keylogging** or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. **Keylogging** can also be used to study human–computer interaction. Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis.

Rootkits

A **rootkit** is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term **rootkit** is a concatenation of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel;

reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.

DOS attacks

In computing, a **denial-of-service attack** (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. A **DoS attack** is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Criminal perpetrators of **DoS** attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

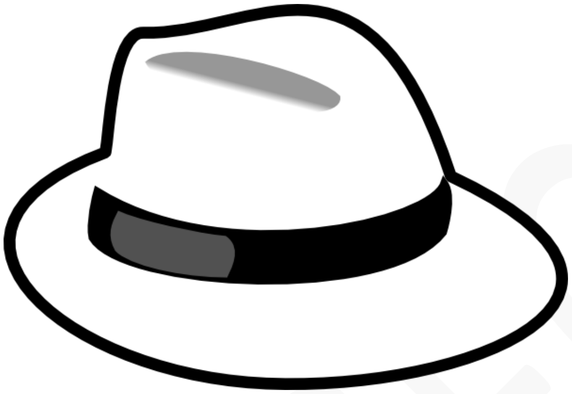
Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. According to the 3rd Microsoft Computing Safer Index Report released in February 2014, the annual worldwide impact of phishing could be as high as $5 billion.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. **Phishing emails** may contain links to websites that are infected with malware.

Phishing is an example of **social engineering** techniques used to deceive users, and exploits weaknesses in current web security. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

BASIC USERS



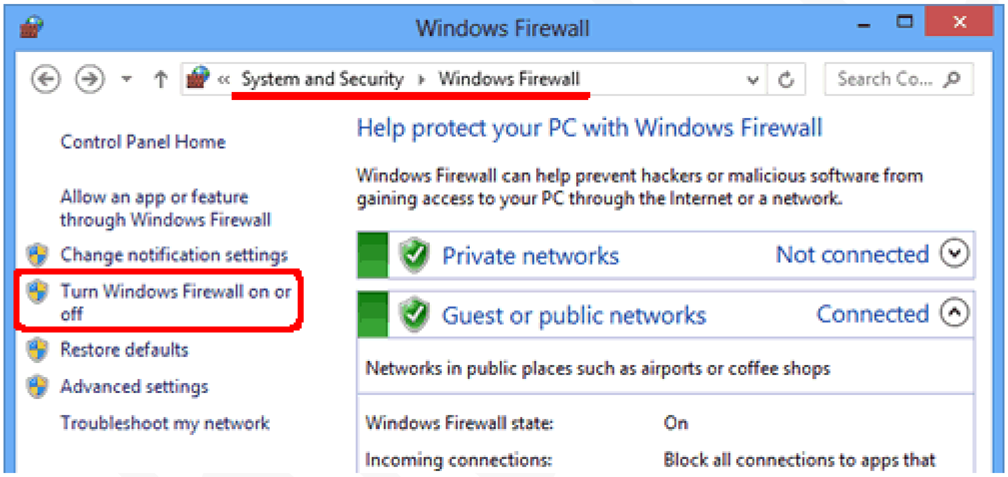
As a basic user you are going to learn how to make yourself safe from online threats. Imagine Internet as a deep ocean and imagine yourself as a small fish swimming into the deeps of this giant. As deeper you go, it becomes darker and colder and THREATS are all around you, just waiting for you to go wrong path.

This is why online security and anonymity is important for basic users. You might think: “Oh, I’m just a boring person surfing the Internet, they won’t hack me because I have nothing to be stolen.” It’s not like that, you might not have PayPal accounts full of money, important information or any other kind of worth. Hackers want anything that they see as valuable, it can be just an access to your PC so they can use it as bot for their botnet. In this topic, I will teach you how to secure yourself and how to surf internet anonymous.

Firewall

In computing, a **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A **firewall** typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. **Firewalls** are often categorized as either network firewalls or host-based firewalls. **Network firewalls** filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine.

To turn your **firewall ON,** go to **Control Panel**, **System and Security**, **Windows Firewall**, **Turn windows firewall on or off**.


Windows Firewall
« System and Security › Windows Firewall
Search Co...
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks Not connected

Guest or public networks Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to apps that

Antivirus software

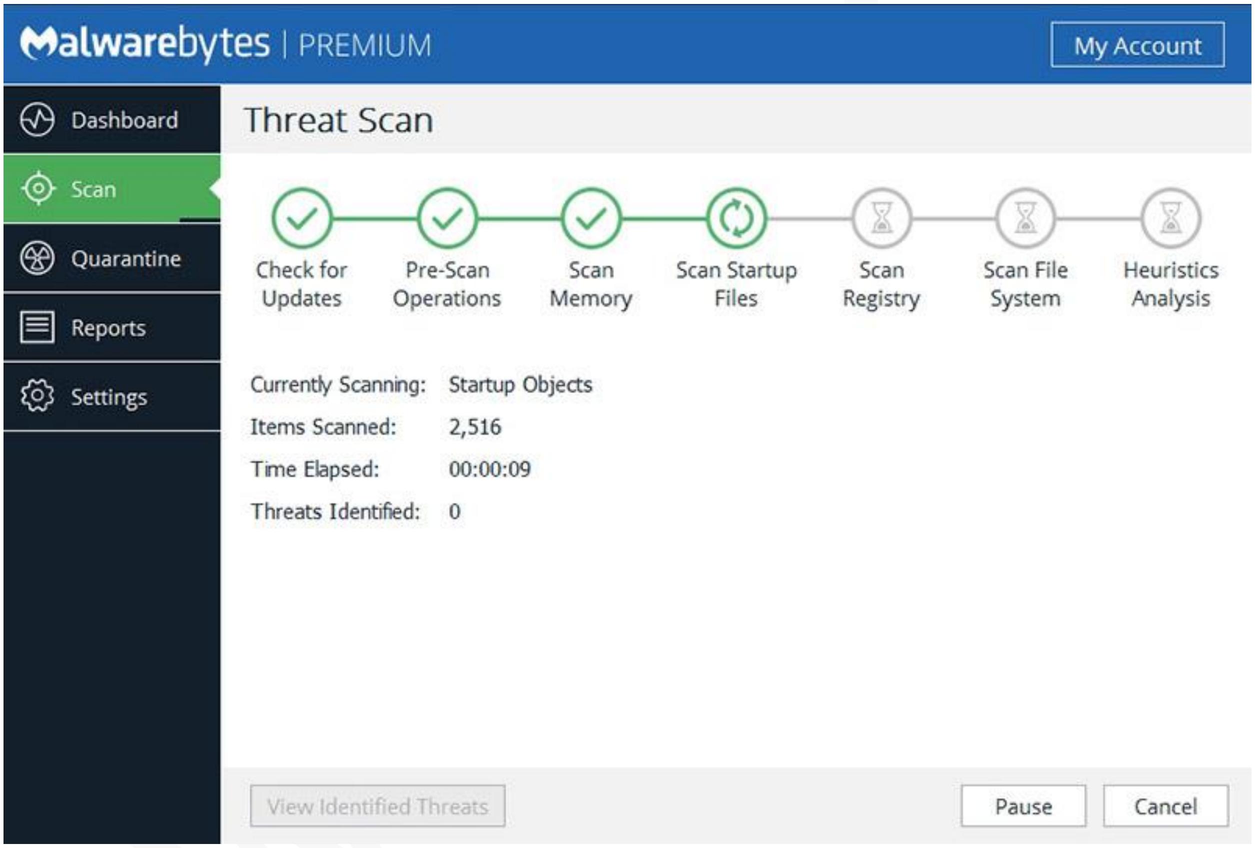
Antivirus or anti-virus software (often abbreviated as AV), sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern **antivirus software** can protect from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

I recommend you using one of those antivirus software: Kaspersky, Avast and Bitdefender. Each one of them has FREE and PAID version. Of course, it's better to have full (paid) version of antivirus, but if you lack money it's ok to use FREE version. The difference between paid and free is the number of available functions. Scan your PC at least twice a week.

Anti-malware software

Many Antivirus programs can’t detect malwares, that’s why we use anti-malware software. I would recommend using Malwarebytes – most famous anti-malware software. It has FREE and PAID version. It’s totally ok to use FREE version. It would be great if you scan your PC ever day.



Currently Scanning: Startup Objects
Items Scanned: 2,516
Time Elapsed: 00:00:09
Threats Identified: 0

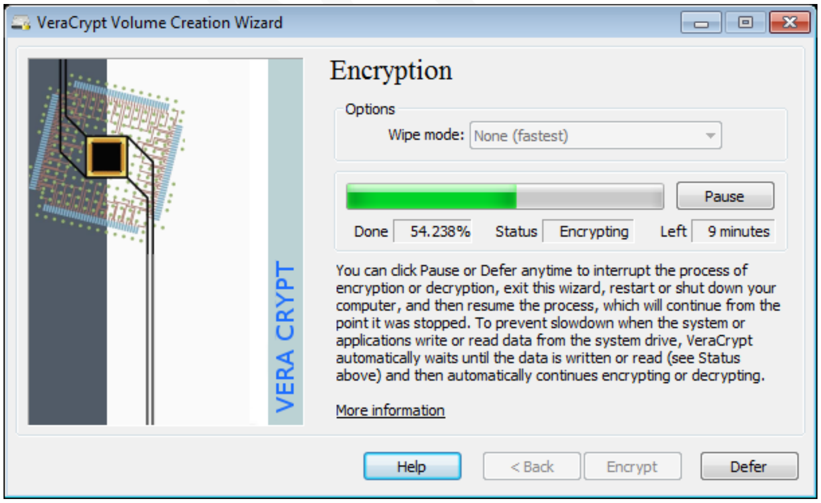
Encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. **Disk encryption** uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

Expressions full disk encryption (FDE) or whole disk encryption often signify that everything on disk is encrypted – including the programs that can encrypt bootable operating system partitions – when part of the disk is necessarily not encrypted. On systems that use a master boot record (MBR), that part of the disk remains non encrypted. Some hardware-based full disk encryption systems can truly encrypt an entire boot disk, including the MBR.

I recommend using Veracrypt disk encryption software. It's free and easy to use. There are some others too, like: Truecrypt and BitLocker.

Individual ciphers supported by **VeraCrypt** are AES, Serpent, Twofish, Camellia, and Kuznyechik. The Magma cipher was removed in version 1.19 in response to a security audit. Additionally, five different combinations of cascaded algorithms are available: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES and Twofish-Serpent. The cryptographic hash functions available for use in VeraCrypt are RIPEMD-160, SHA-256, SHA-512, Streebog and Whirlpool.



Wipe mode: None (fastest)

Done 54.238% Status Encrypting Left 9 minutes

You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, VeraCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.

Passwords

A **password** is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access.

If you want to stay safe you need to use complex passwords. Best passwords are those with signs in it (!@#$%^&*=+*) combined with letters(a-z) and numbers(1,2,3,n…). This is an example of a strong password "m#P52s@ap$V". You can test your password here. Also I recommend writing down your password on a piece of paper. DO NOT save your password into a .txt document on your PC.

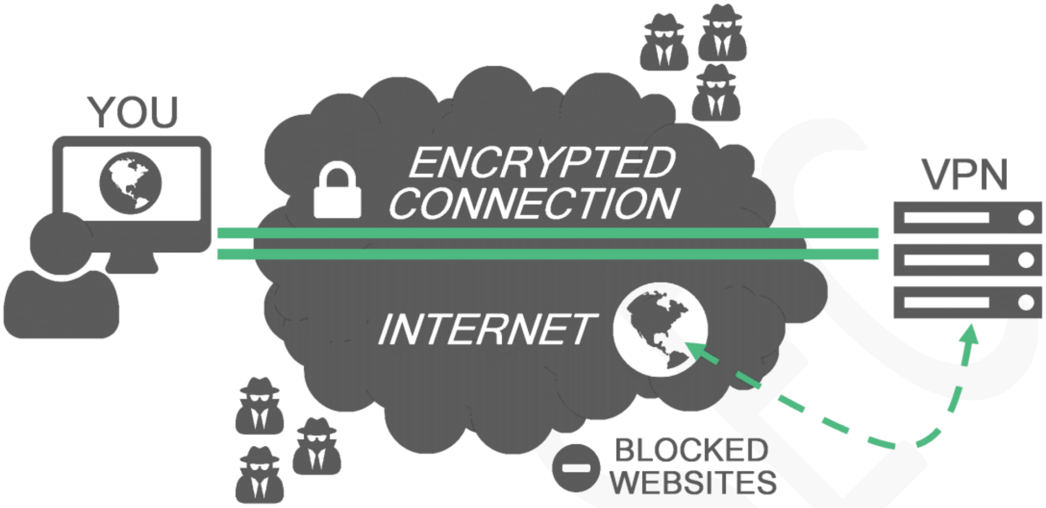
Virtual Private Network(VPN)

A **virtual private network** (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the **VPN** may therefore benefit from the functionality, security, and management of the private network.

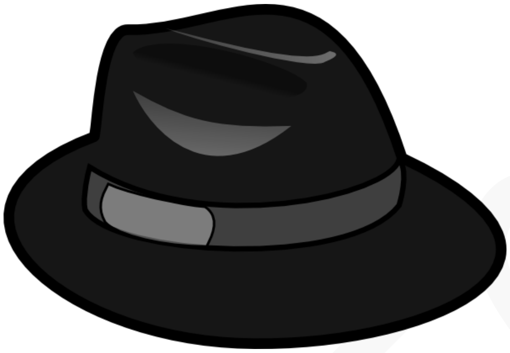
Virtual Private Networks may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a **VPN**, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions.

A **VPN** is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A **VPN** available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

I would recommend buying VPN because it's hard to find free ones that are good, and you often need to wait queue time to connect to the server or you have restricted time to spend on VPN. Here are some of the best VPNs you can get: IPVanish, Cyberghost, ExpressVPN, PureVPN.



ADVANCED USER



As advanced user, in this book you are described as a user who is engaged with illegal activities or legal ones such as penetration-testing, ethical hacking. In this eBook I will teach you how to perform perfect OpSec, how to stay anonymous and how to make your system bulletproof. I will talk about VPNs, Virtual machines, encryption, emails, web browsers and plugins, Linux, and security operations.

Linux(Kali)

You probably heard of Kali Linux. **Kali Linux** is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. Mati Aharoni, Devon Kearns and Raphaël Hertzog are the core developers.

Kali Linux has a dedicated project set-aside for compatibility and porting to specific Android devices, called Kali Linux NetHunter. It is the first Open Source Android penetration testing platform for Nexus devices, created as a joint effort between the Kali community member "BinkyBear" and Offensive Security. It supports Wireless 802.11 frame injection, one-click MANA. Evil Access Point setups, HID keyboard (Teensy like attacks), as well as Bad USB MITM attacks.

I recommend using Kali Linux not just because of it’s tools for penetration testing but for it’s security tools and simple protection. While using Kali, I recommend using a **VPN** through **TOR**. That means you first run **VPN** and then you connect to **TOR**. Here is the tutorial on how to install VPN and TOR to your Kali.

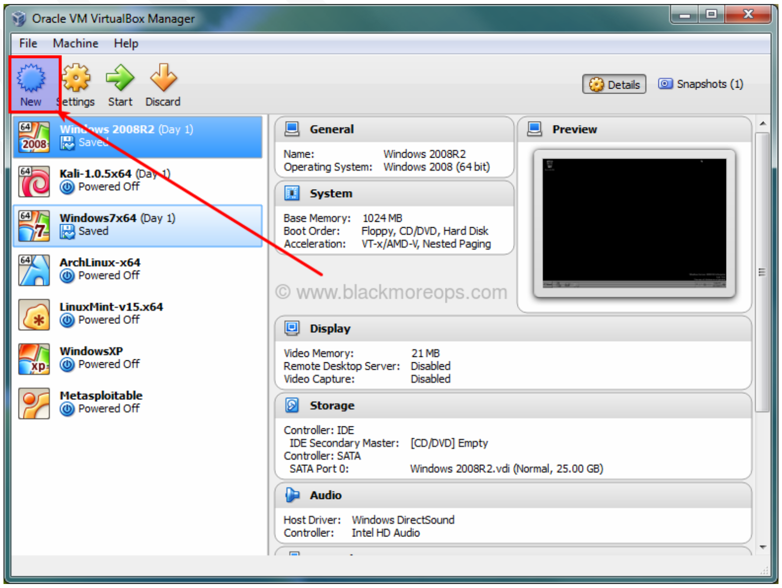
Virtual machine

Your browser isn't the only vector for third parties to invade your privacy. PDFs and other seemingly harmless files can serve as homing beacons, and potentially alert government entities when you're viewing planted contraband. To prevent unintended breaches of privacy, open suspect files inside of a virtual machine.

Load up your favorite Linux distribution inside of VirtualBox, configure it to your liking, and then save a snapshot of your VM.

Next, download your desired file (using the protections illuminated in this article), and then shut off your virtual machine's access to the Internet. Once you're sure that the VM is cut off completely from the network, you can now open the file safely. Read what you need, make notes, and then shut down the VM. Next time you need to view a file inside one, you'll have your snapshot ready to go.

I recommend using VirtualBox because it’s easy to use and it’s free. Here is also the link for tutorial about installing Kali Linux on VirtualBox.



Windows 2008R2 (Day 1)
Saved

Kali-1.0.5x64 (Day 1)
Powered Off

Windows7x64 (Day 1)
Saved

ArchLinux-x64
Powered Off

LinuxMint-v15.x64
Powered Off

WindowsXP
Powered Off

Metasploitable
Powered Off

General

Name: Windows 2008R2
Operating System: Windows 2008 (64 bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 21 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: Windows 2008R2.vdi (Normal, 25.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Virtual Private Netwok (VPN)

We already went through the VPN topic above. This time I will give you some VPNs that I personally use and that I'm sure they DO NOT distribute logs. It's important to find a VPN that is keeping their logs safe.

143VPN - 143VPN provides solutions to your security concerns by providing TCP and UDP protocol VPN services with industry level encryption. Their Lifetime license costs $49.99. It's great because of it's client. You can easy port-forward ports and change between few servers(UK, Netherlands, Chicago, Russia…).

RA4WVPN – This is also an amazing VPN from HackForums. They have high quality servers, I think 20 of them around the world. They encrypt your data and does not keep any logs. You can buy it for $2.5(monthly) and $18.5(1 year).

TOR

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "**The Onion Router**".

Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the destination IP address, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts a layer of encryption to reveal only the next relay in the circuit in order to pass the remaining encrypted data on to it.

The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.

As much as you think that **TOR** is safe, it is not. It was few years ago, but now there are a lot of people that control exit nodes same as **NSA**. However, it's great tool to have while hacking or browsing internet. HERE you can download TOR, and HERE is the tutorial on how to install TOR on Kali Linux.

BROWSERS

When we talk about Internet browsers, I can't tell much except – Use FIREFOX.

Mozilla Firefox is amazing web browser, it's fast and reliable and they respect your privacy. You can also install few useful plugins to your Firefox browser.

This is the list of some plugins:

HTTPS everywhere it's a extension that encrypts your communications with many major websites, making your browsing more secure.

Ghostery lets you enjoy a cleaner, faster, safer browsing experience by giving you the control to make informed decisions about the personal data you share with the trackers on the sites you visit.

uBlock Origin is a plugin that block all the ads featured on websites you visit.

Email

I personally do not trust any of those famous email providers like Gmail, Yahoo, Outlook and others. I recommend you to use ProtonMail or NeoMailBox or even CounterMail. I use **Protonmail** because it is incorporated in Switzerland and all of their servers are located in Switzerland. This means all user data is protected by strict Swiss privacy laws. It has End-to-End encryption and there are no personal information needed to register account.

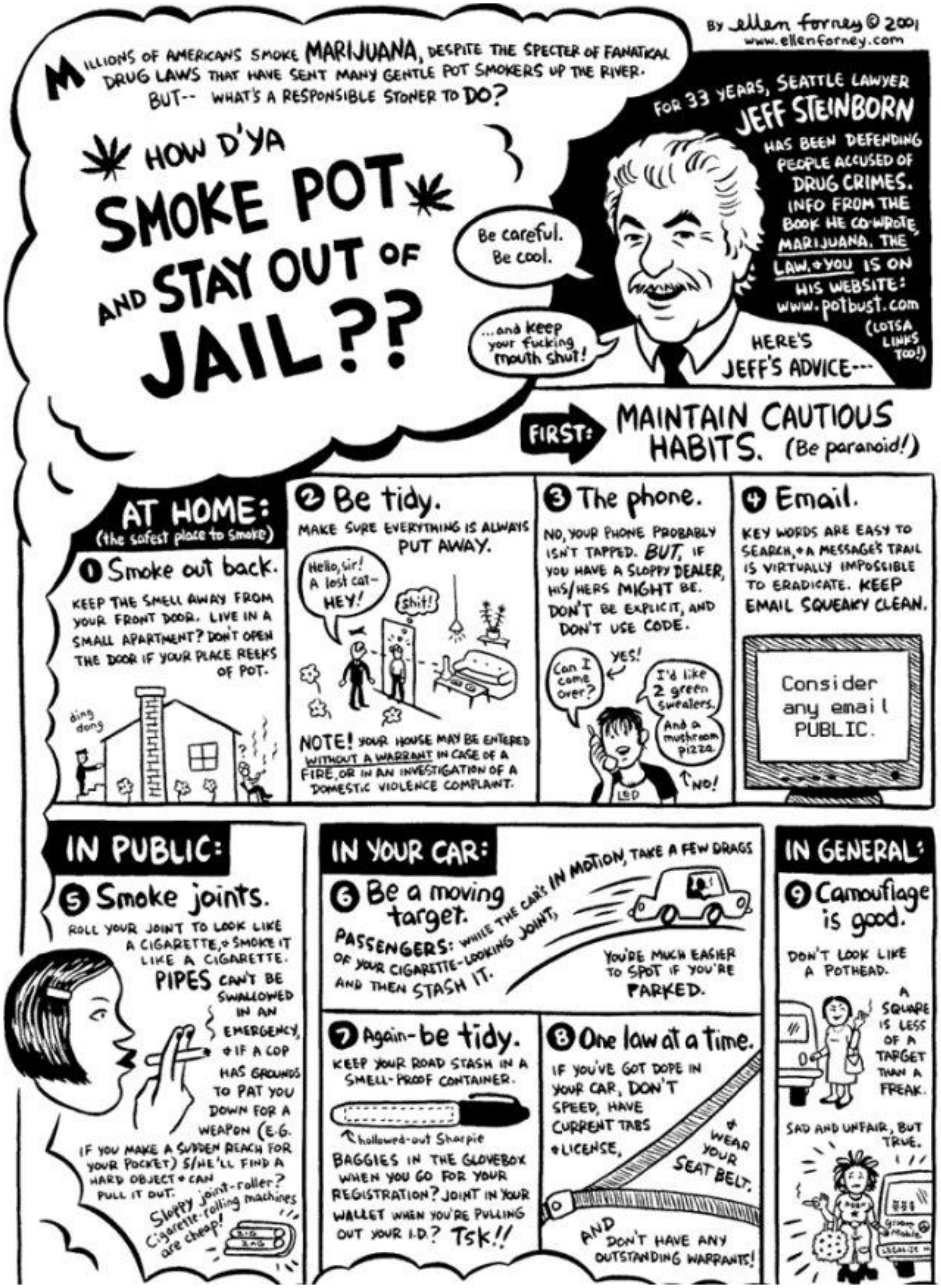
Anti-doxing

Have you ever heard of doxing? Doxing (from dox, abbreviation of documents) is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organization.

The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. It is closely related to internet vigilantism and hacktivism.

So, how do I remove myself from the Internet? First of all go to this site, it's called **JustDeleteMe**. There you can find all websites that required registration, click on one that you know you registered on and deactivate/delete your account. Next step would be to **remove your personal info** from websites. If there are any sites where you posted your email, security numbers or something like that, ask them to remove it if you can't by your own. The final step would be to **remove your email accounts** and make new one on ProtonMail with fake ID. Here you can generate completely new identity for free.

Example of OPSEC?


By ellen forney © 2001
www.ellenforney.com
MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER. BUT-- WHAT'S A RESPONSIBLE STONER TO DO?
HOW D'YA SMOKE POT AND STAY OUT OF JAIL??
FOR 33 YEARS, SEATTLE LAWYER JEFF STEINBORN HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, + YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)
Be careful. Be cool.
...and keep your fucking mouth shut!
HERE'S JEFF'S ADVICE---
FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)
AT HOME: (the safest place to smoke)
1 Smoke out back.
KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.
ding dong
?
2 Be tidy.
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.
Hello, sir! A lost cat— HEY!
shit!
NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.
3 The phone.
NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.
Can I come over?
YES!
I'd like 2 green sweaters. And a mushroom pizza.
NO!
LED
4 Email.
KEY WORDS ARE EASY TO SEARCH, + A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.
Consider any email PUBLIC.
IN PUBLIC:
5 Smoke joints.
ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, + SMOKE IT LIKE A CIGARETTE.
PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, + IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR YOUR POCKET) S/HE'LL FIND A HARD OBJECT + CAN PULL IT OUT.
Sloppy joint-roller? Cigarette-rolling machines are cheap!
ZIG ZAG
IN YOUR CAR:
6 Be a moving target.
PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.
YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.
7 Again-be tidy.
KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.
hollowed-out Sharpie
BAGGIES IN THE GLOVEBOX WHEN YOU GO FOR YOUR REGISTRATION? JOINT IN YOUR WALLET WHEN YOU'RE PULLING OUT YOUR I.D.? TSK!!
8 One law at a time.
IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS + LICENSE, + WEAR YOUR SEAT BELT.
AND DON'T HAVE ANY OUTSTANDING WARRANTS!
IN GENERAL:
9 Camouflage is good.
DON'T LOOK LIKE A POTHEAD.
A SQUARE IS LESS OF A TARGET THAN A FREAK.
SAD AND UNFAIR, BUT TRUE.
Groom Mobile
LEGALIZE

Now I will show you an example of how would I hack a website of a big company and not get caught.

First you need to make sure you really want to do this, once you start you can’t stop and you need to be ready for everything. Ok, let’s begin.

First, get yourself an old laptop. Why an old laptop? Because, in case you need to get rid of evidence, you don’t want to destroy $2000 laptop. Next step would be preparing tools and software on your laptop. Make sure to buy VPN or any other tool with your fake profiles, I recommend to pay it with Bitcoin. Now, go somewhere outside, find open WiFi and check if there are any cameras around you (hide from them). Next thing is, download VirtualBox, live boot Kali Linux, prepare everything you need for this attack. Run your VPN, TOR and start hacking. One IMPORTANT thing: DO NOT enter your personal social network accounts on that laptop or enter any kind of account or website associated with you. Let’s say you hacked that company, got the info you needed, transfer files to a USB and leave the place. Now I would recommend destroying that old laptop, smash it into the pieces and throw the pieces into the sea/river or burn it. That should be it, they can’t trace you unless you somehow forgot to do one of these steps.

Few tips/words for the end

If one wishes to cover one's tracks on the Internet, find a free WiFi access point, modify your WiFi card's MAC address, and boot your computer from a "live CD", running totally in RAM." And just to make a different opinion, TOR browser is an arsenal you should definitely use to stay anonymous. It will help you from not telling the website and servers about what agent you are using (browser) and also not projecting your IP address as well.

Also, while the Tor network is quite secure from traffic analysis, the Tor browser, like any other, is vulnerable to attacks and exploits. The Tor browser is, specifically, a modified version of Firefox, and as such is vulnerable to the same kinds of attacks as Firefox. By infecting an individual user's computer with malware, one can track their activity and even remotely access their device.

You should use this awesome tool from EFF to ensure you are browsing anonymously: Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques. We'll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software.

- If you're very serious about maintaining your anonymity, consider investing in a VPN solution like TorGuard or Private Internet Access. These services essentially allow you to disguise your traffic. Your real IP address will be hidden from the world, and your traffic will remain indecipherable to nosy ISPs or governments.

- Virtual machines: Keep in mind, your browser isn't the only vector for third parties to invade your privacy. PDFs and other seemingly harmless files can serve as homing beacons, and potentially alert government entities when you're viewing planted contraband. To prevent any sort of unintended breach of privacy, you should open suspect files inside of a virtual machine.

- DNS leak testing: Even if you're using a privacy service (like a VPN) to hide your IP address, it's still possible to give away clues to your identity via your DNS traffic. Thankfully, it's easy to detect if your configuration is leaking your DNS information. Simply head over to DNS leak test, and run the extended test.

Hacking through public schools:

Earlier this year, attackers exploited a vulnerable web application on public school servers and broke into them. After bouncing around the networks and installing backdoors, the gang used the school's computers to launch even more attacks. "Just another example of machines that are typically unprotected and appear innocuous,". – This is the example of hiding yourself behind the attack.

Rules!

1. Never reveal your true identity!
2. Never reveal your plans!
3. Never trust anyone!
4. Never operate from your own house!
5. Be paranoid!
6. Keep personal life and “hacker life” separated!
7. Don’t talk to the police!
8. Don’t discuss politics with strangers!

DISCLAIMER: This eBook is for education purpose only and as such is NOT recommendation to perform any of illegal activities. I am NOT responsible for your consequences.

Thanks for reading, I hope you learned something. Leave a comment on thread if you liked it.