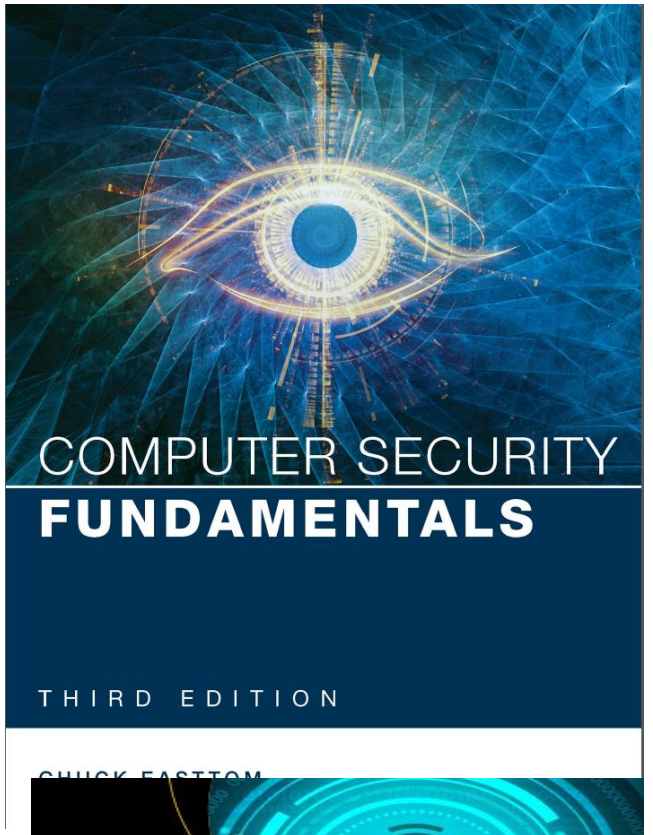
409 comp

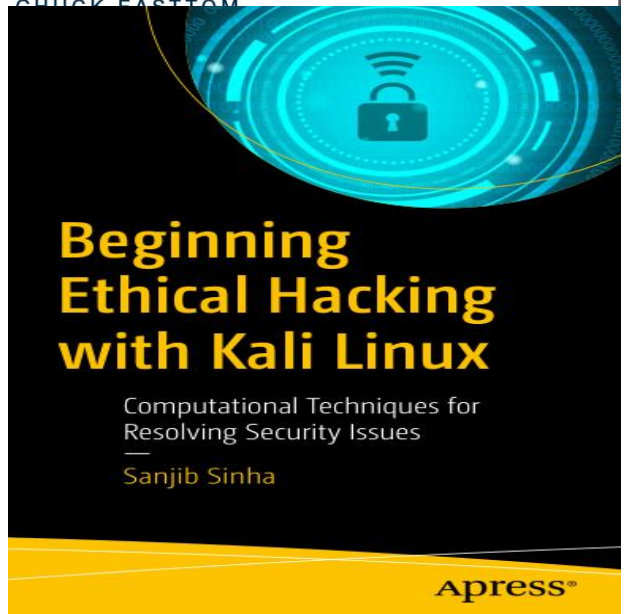
Cyber and information security

Dr. Dieaa I. Nassr

Reference:

1. *Chuck Easttom*, Computer Security Fundamentals, *Third Edition, Pearson, 2016.*
2. *Sanjib Sinha, Beginning Ethical Hacking with Kali Linux – Computational Techniques for Resolving Security Issues, 2018*





Advice:

In information security, "knowledge is power" is not only good advice, but also an axiom upon which to build your entire security outlook.

Alarm

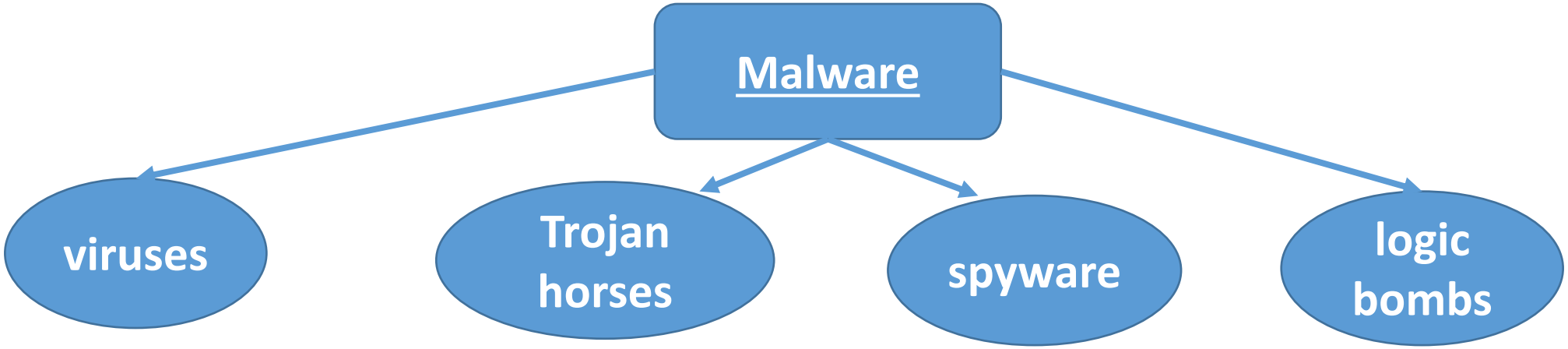
على كل طالب قراءة قانون مكافحة جرائم الإنترنت على الرابط الأتى:

https://www.cc.gov.eg/legislation_single?id=386006

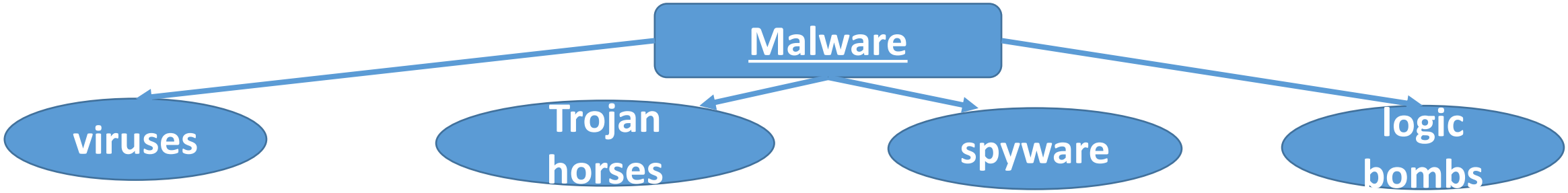
انا غير مسئول عن استغلال المعلومات التى تقدم فى المادة العلمية بطريقة غير قانونية مع العلم ان كل ما سيتم تقديمه اثناء دراسة المادة العلمية ليس سوى الخبرة الأكاديمية.

Most Known Types of Attacks

- **Malware:** This is a generic term for software that has a malicious purpose اغراض خبيثة. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger خطر منتشر to your system.



Most Known Types of Attacks (cont.)



viruses	Trojan horses	spyware	logic bombs
a small program that replicates and hides itself inside other programs A computer virus is similar to a biological virus;	Appearing to be benign حميدة software but secretly downloading a virus or some other type of malware onto your computer from within	Spyware is simply software that spies on what you do on your computer. EX) like cookie-a text file that your browser creates and stores on your hard drive. Ex) a key logger, records all of your keystrokes.	It is software that lays dormant يظل هادىء until some specific condition is met. That condition is usually a date and time. the software does some malicious act such as delete files, alter system configuration, or perhaps release a virus

Most Known Types of Attacks (cont.)

- **Security breaches** مخالفات امنية: This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges رفع الأمتيازات, breaking into a server…all the things you probably associate with the term *hacking*.

Most Known Types of Attacks (cont.)

- **DoS attacks (Denial of service) :** These are designed to prevent legitimate access to your system.

- **Web attacks:** This is any attack that attempts to breach يخترق your website. Two of the most common such attacks are SQL injection and cross-site scripting.

Most Known Types of Attacks (cont.)

- **Session hijacking: اختطاف التوصيلة**These attacks involve an attacker attempting to take over a session.
- **Insider threats:** These are breaches احتيالات based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

Compromising System Security (Attacks).

Cracking: is the appropriate word for intruding عنوة الدخول into a system without permission, usually with malevolent intent نية خبيثة . Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as **cracking**.

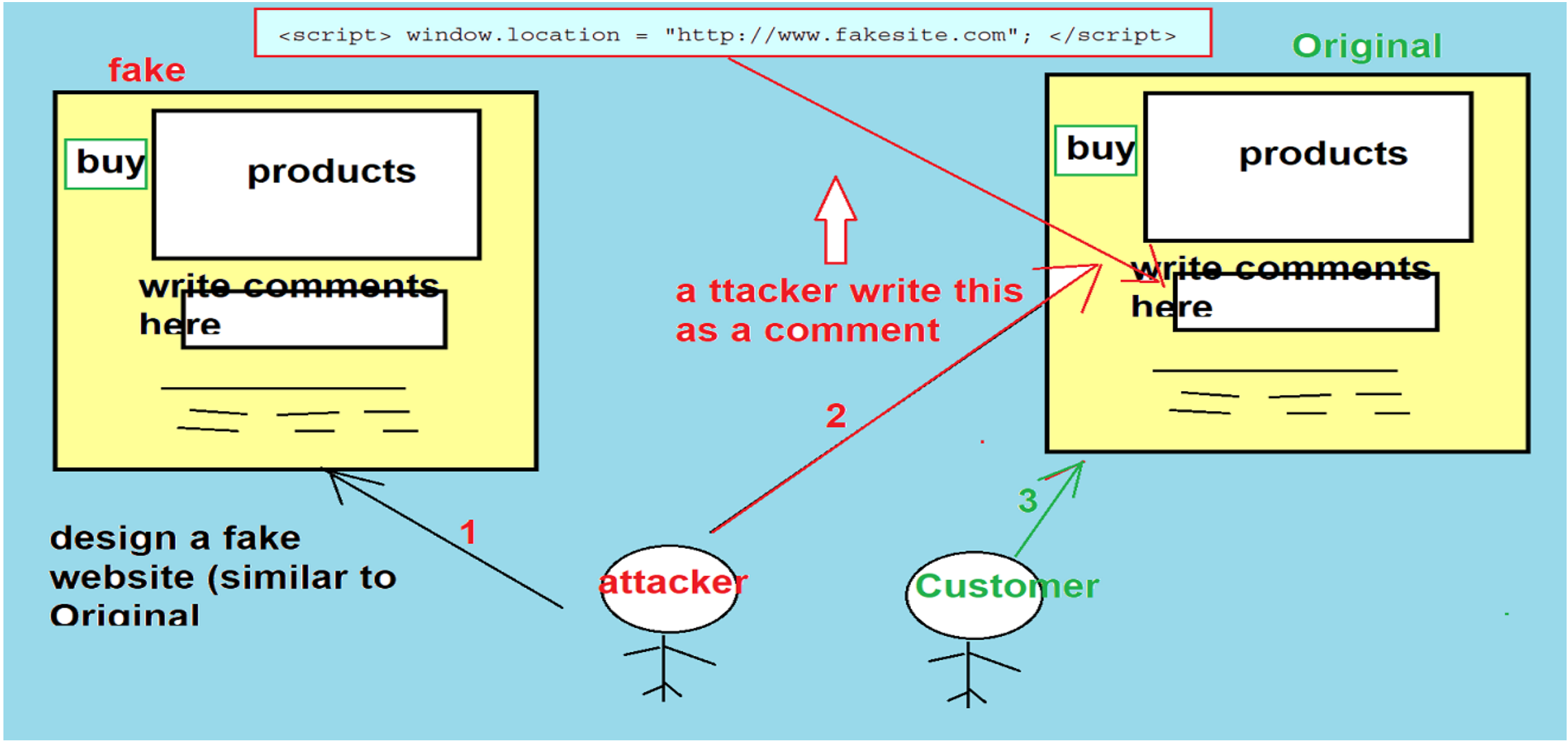
DoS Attack:

- The attacker does not actually access the system. Rather, this person simply blocks access from legitimate users. E.g, drop down the target server.
- Anyone can execute a DoS attack, even without technical skill. Many tools can be downloaded for free from Internet. E.g., Orbit Ion Cannon (LOIC)
- DDoS is a general (variant) of DoS Attack.
- Next Session we discuss in more details about DoS and DDoS attacks.

Web Attack:

- websites (Web server) allow users to interact with the websit
- User interaction is a potential point for attempting a web-based attack.
- **SQL Injection:** entering SQL commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands.
- **Cross-Site Scripting:** Like SQL Injection, it depends on the web programmer not filtering input. E.g., many websites of marketing allow users (or customers) to upload comments a bout products. Attackers try to upload malicious java script code instead of comments, when a user requests (reviews) the comments, the malicious java script code run on the user machine.

Web Attack: Cross-Site Scripting:



Web Attack:

- Session Hijacking: (may be complex to perform) the attacker monitors an authenticated session between the client machine and the server and takes that session over.
- Insider Threats: is simply when someone inside your organization either misuses his access to data or accesses data he is not authorized to access.

Ex) In 2009 **Edward Snowden** was working as a contractor for Dell, which manages computer systems for several U.S. government agencies. In March 2012 he was assigned to an NSA location in Hawaii وكالة الأمن القومي في هاواي .

He accessed and downloaded thousands of documents that he was not authorized to access.

Insider Threats: (another example)

- A hospital employee who accesses patient records to use the data to steal a patient's identity, or someone with no access at all who accesses records.
- A salesperson who takes the list of contacts with him before leaving the company.

DNS (Domain Name Service) Poisoning: تسمم - تلوث

- DNS is what translates the domain names (like, http://www.cbcbank.net) into IP addresses (like 204.12.73.100).
- DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit غير مشروع site, often for the purpose of stealing personal information.
- The attacker wants to trick users to steal their passwords (say Bank accounts) and use those on the real website.
- First the attacker creates a phishing website (similar to login in page of target bank website).
- Since many users are too smart to click on links, he will use DNS poisoning to trick them.

DNS (Domain Name Service) Poisoning: تلوث - تسمم

- The attacker creates his own DNS server.
- Then he puts two records, each record contains an IP and a relatively domain name) in his DNS server.
- The first is for the CBC Bank website, pointing to his fake site rather than the real bank site.
- The second for a domain name that does not exist (say for www.ElZa3baloy.com)
- The attacker sends a request to a DNS server on the target network about IP of www.ElZa3baloy.com.

DNS (Domain Name Service) Poisoning: تسمم - تلوث

- Since the domain name of www.ElZa3baloy.com does not exist. i.e., the DNS server does not have an entry for the www.ElZa3baloy.com domain.
- DNS starts to propagate the request up its chain of command eventually to its service provider DNS server.
- The attacker sends a flood of spoofed responses طوفان من الاستجابات المخادعة claiming to be from a DNS server that the target server is trying to request records from but are actually coming from his DNS server and offering the IP address for www.ElZa3baloy.com domain
- At that point the hacker's DNS server offers to do a zone transfer, exchanging all information with the target server. That information includes the spoofed address for CBC Bank.

New Attacks

- **Doxing**: which is the process of finding personal information about an individual and broadcasting it, often via the Internet. It is most often used against public figures. E.g., *the director* of the *CIA* was the target of doxing.
- **Hacking of medical devices:** Hacker Barnaby Jack first revealed a vulnerability in an insulin pump that could allow an attacker to take control of the pump and cause it to dispense صرف the entire reservoir احتياطی of insulin in a single does, thus killing the patient
- **Jeep vehicles** could be hacked and shut down during normal operation. A hacker could cause the Jeep to stop in the middle of heavy, high-speed traffic. This has the potential to cause a serious automobile accident.

Basic Network Utilities

- ❑IPConfig
- ❑Ping
- ❑Tracert
- ❑Netstat
- ❑NSLookup

Basic Network Utilities (cont.)

- IPConfig: gives you some information about your connection to a network (or to the Internet) like, IP address, IP address for your default gateway, MAC address, computer name.
- Most commands have a number of parameters, or flags, that can be passed to the commands to make the computer behave in a certain way. E.g., **IPConfig/all,**

To find out more about write “IPConfig ?”

Basic Network Utilities (cont.)

- ping: is used to send a test packet, or echo packet, to a machine to find out if the machine is reachable and how long the packet takes to reach the machine.
- Tracert: it not only tells you if the packet got to its destination and how long it took, but also tells you all the intermediate hops it took to get there.
- NetStat: It is an abbreviation for Network Status. It tells you what connections your computer currently has.

Basic Network Utilities (cont.)

- **NSLookup** (for Name Server lookup): It is used to connect with your network's DNS server. Often it can be used just to verify the DNS server is running. It can also be used to execute commands.

Protecting Yourself Against Cyber Crime

- **Protecting Against Investment Fraud احتيال:**

1. Only invest with well-known, reputable brokers سماسرة حسنة السمعة.
2. If it sounds too good to be true, then avoid it.
3. Ask yourself why this person is informing you of this great investment deal. Why would a complete stranger decide to share some incredible investment opportunity with you?
4. Remember that even legitimate investment involves risk, so never invest money that you cannot afford to lose.

Protecting Yourself Against Cyber Crime

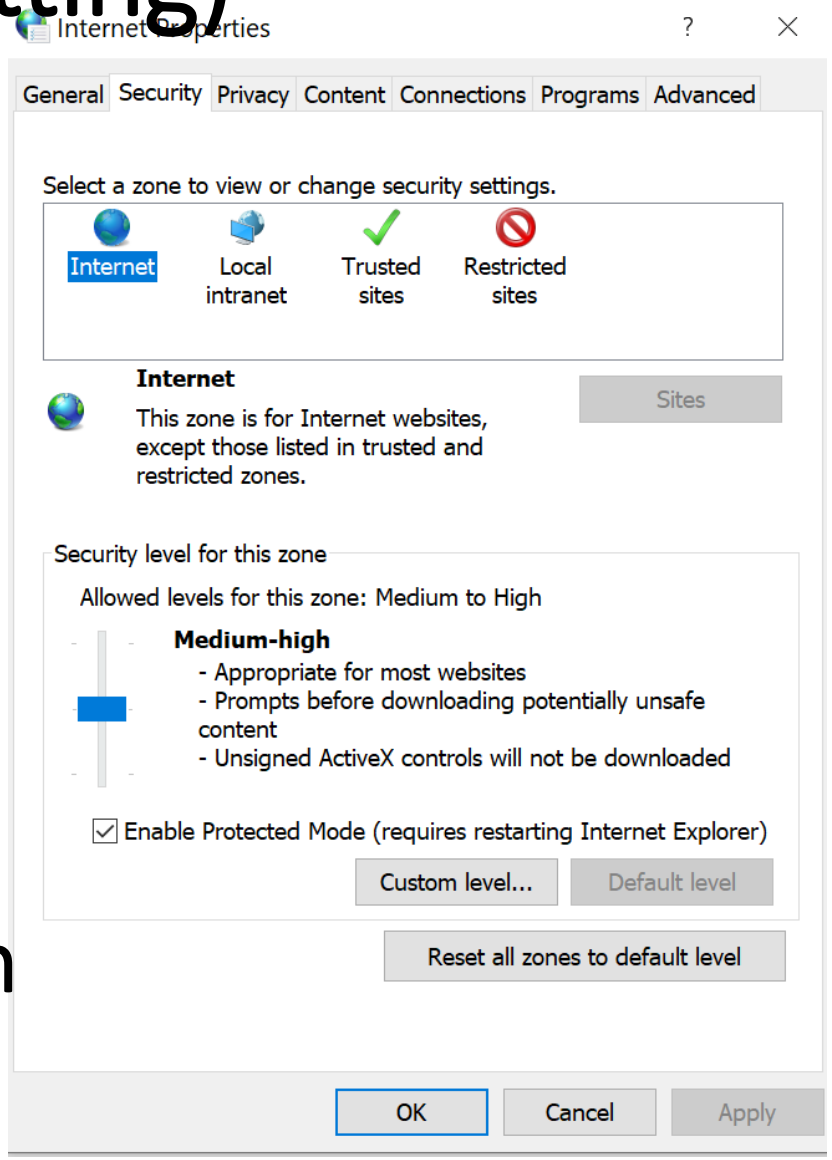
- Protecting Against Identity Theft:

1. Do not provide your personal information to anyone if it is not absolutely necessary.
2. Destroy documents that have personal information on them. If you simply throw away bank statements and credit card bills, then someone rummaging (searching) through your trash can get a great deal of personal data
3. Check your credit frequently

Protecting Yourself (browser Setting)

Secure Browser Settings

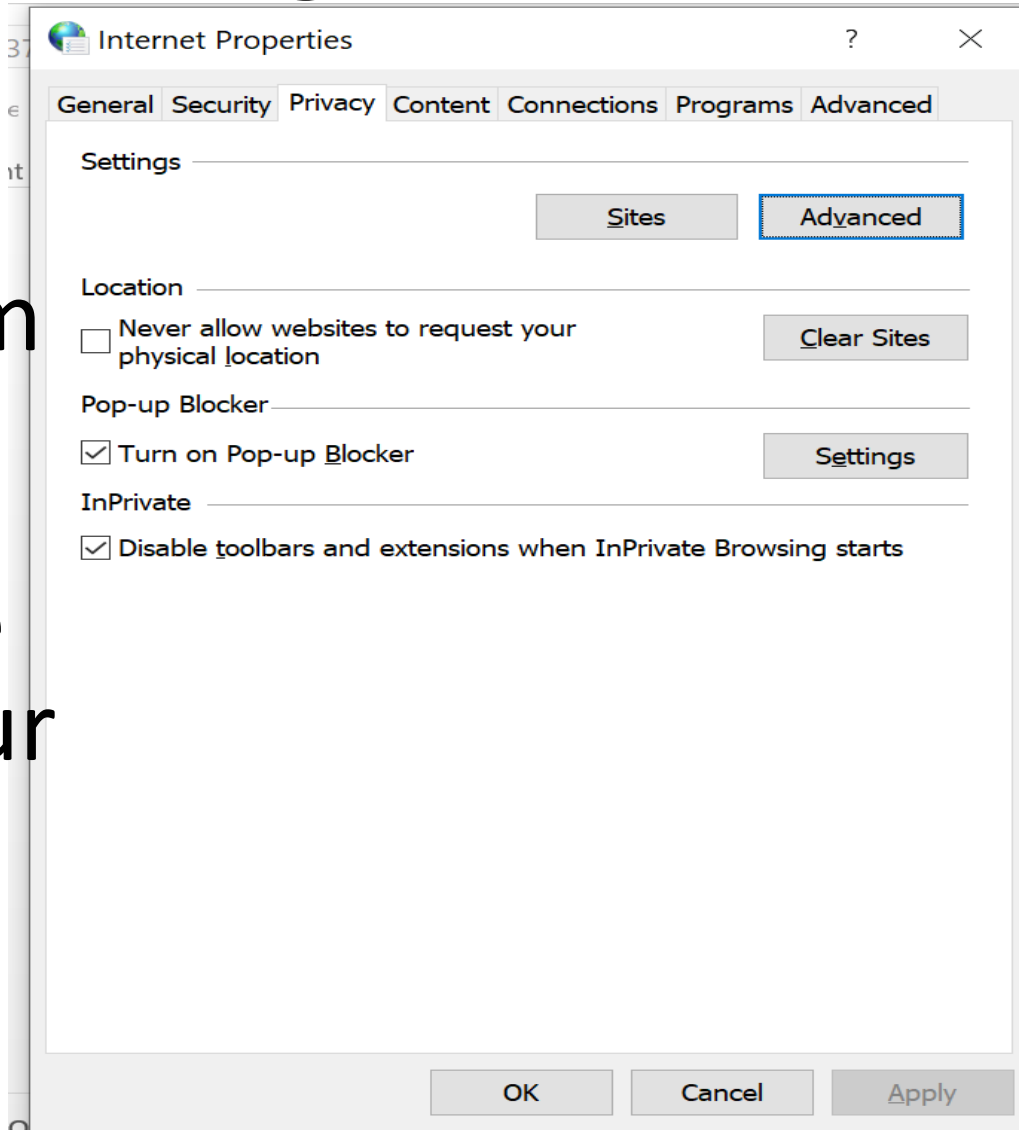
1. Open ->tools->option of your browser (say Microsoft Internet Explorer)
2. Select the Security tab.
3. The sliding bar on the left that lets you select various levels of general protection against cookies
4. Select privacy->Advanced button



Protecting Yourself (browser Setting)

Secure Browser Settings

- This button allows you to block or allow individual websites from creating cookies on your computer's hard drive. Altering cookie settings on your machine is just one part of protecting your privacy, but it is an important part.



Protecting Yourself (browser Setting)

Secure Browser Settings

- Select High Security.
- Allow first-party cookies.