Any fraudulent technique or activity that is done to gain money or some other valued thing from a person is referred to as a scam. A person who does a scam is known as a scammer. Scammers usually make unwanted phone calls or give deceptive pop-up ads so that they can distract unwary computer users, such as their machines have a critical problem that has to be treated right away. Scammers frequently impersonate officials of well-known computer and software firms. Once a person is on the phone with a fraudster or clicks the advertisement link, the scammer frequently requests remote access to the victim’s computer. The scammer then can steal passwords, install malware or try to sell superfluous services or products.

A **computer virus hoax** is a message warning the recipients of a non-existent [computer virus](https://en.wikipedia.org/wiki/Computer_virus) [threat](https://en.wikipedia.org/wiki/Threat_(computer)). The message is usually a [chain e-mail](https://en.wikipedia.org/wiki/Chain_e-mail) that tells the recipients to forward it to everyone they know, but it can also be in the form of a pop-up window. Virus hoaxes are usually harmless and accomplish nothing more than annoying people who identify it as a hoax and wasting the time of people who forward the message. Nevertheless, a number of hoaxes have warned users that vital system files are viruses and encourage the user to delete the file, possibly damaging the system.Basically,virus is using you to hack your system, you are doing it with your own hands.

Dictionary attacks is like bitcoin mining. Hashing function converts your file from gokturk.txt to 7645a and some bad people have the list of hashes made by your hash function. They observe which data results in which hash and they try to find gokturk.txt’s hash and reach it.

They ask money after they have encypted your harddrive . this is getting serious recently through the world including government, including companies. And company pays it in bitcoin. They are usually from unknown countries, Russia,china… If master computer is encrypted an can be reached by other people, backup computers can also be reached,if they are linked to each other in network. Some computers resilient and strong, after the attack, they continue operating normal stuff whereas some computers are not capable of doing it without human interference.

Slayt = Ransomware

\*This type of malware is deployed to system data and encrypts it, shutting out the user who then has to pay a ransom to get their files back.

\*Some will monitor your system activity for some time so they can understand the level of leverage they are dealing with before asking for a price.

\*Ransomware has brought down many large organizations and even big cities.

\*Therefore, you need to have tight malware prevention programs and reliable offline backups for any critical data.

\*Also,discuss possible risks and mitigation strategies to be prepared for such threats of ransomware.

Slayt = Hybrids

\*These are the worst kind of malware and are very common today. They combine various malware, commonly trojans and worms, to facilitate actions that are hard to reverse once the systems are hit.

\*For instance, malware can appear like trojans to the user, but in reality, it’s spreading the malicious code to the network using the worms. Botnets bear trojan and worm qualities and pose severe risks to systems.

\*Hybrids do a great job of concealing their workings from anti-malware programs. However, the first action to take when you suspect a hybrid infection is to scan the system with anti-malware.

--replicate itself in network, if you are connected to network, another infected computer tries to make connections to your computer and infect it so it is a network worm.

--these kind of programs are distributed on purpose or providing free downloads, free images,pdf files , game cracks etc.

Slayt = Malware

\*Malicious Software 🡪 malware’in kısaltması. Senin beklediğin şeyleri yapmaz, but it does something for its own benefit. Those software is done with intention , not by mistake.

\*The term “malware” refers only to software that is made for malicious purposes and works against users’ expectations – and so does not include applications that may do unintended harm due to software bugs.

Slayt = Spyware

\*Spyware is malware that collects some data,usually without the computer users’ knowledge.

\*Very often, this data is then sent over the internet to someone else.

\*very often, this is used for marketing.

\*spyware can also be used to steal data from computers.

\*one kind is a keylogger which can see whatever you are typing.

\*Keyloggers can steal important information like passwords that you type.

**\*Casus yazılım** veya **spyware** (İngilizce *spy* ve *software* sözcüklerinden), başlıca [zararlı yazılım](https://tr.wikipedia.org/wiki/Malware) (malware) türlerinden biridir. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.[[1]](https://tr.wikipedia.org/wiki/Casus_yaz%C4%B1l%C4%B1m#cite_note-1)

Bazı kaynaklarda dar manada "snoopware" (burun sokan yazılım) olarak da adlandırılan casus yazılımlar, diğer zararlı yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar.[[2]](https://tr.wikipedia.org/wiki/Casus_yaz%C4%B1l%C4%B1m#cite_note-2)

Casus yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımın amacı kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Bu bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi bile olabilir. Bunun dışında, Ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler.

Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir.

Slayt = Adware – advertising-supported software

\*Software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.

\*The software may generate two types of revenue: 1)the display of the advertisement 2)”pay-per-click” basis, if the user clicks on the advertisement

\*Some advertisements also act as spyware, collecting and reporting data about the user, to be sold or used for targeted advertising or user profiling.

\*The software may implement advertisements in a variety of ways, including a static box display, a banner display, full screen, a video, pop-up ad or in some other form.

\*All forms of advertising carry health, ethical, privacy and security risks for users. (it is generally accepted idea but advertising is a commertial activity, commercial activity is not a sin.) (announcing smt related to ürün with money is called as advertisement)

Slayt = Computer Security Issues

\*Vulnerability is a point where a system is susceptible to attack.

\*A threat is a possible danger to the system. The danger might be a person(a system cracker or a spy), a thing(a faulty piece of equipment), or an event (a fire or a flood) that might exploit a vulnerability of the system.

\*Countermeasures are techniques for protecting your system.

**Definition of a Buffer Overflow**

A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.

In some cases, an attacker injects malicious code into the memory that has been corrupted by the overflow. In other cases, the attacker simply takes advantage of the overflow and its corruption of the adjacent memory. For example, consider a program that requests a user password in order to grant the user access to the system. In the code below, the correct password grants the user root privileges. If the password is incorrect, the program will not grant the user privileges.

However, there is a possibility of buffer overflow in this program because the gets() function does not check the array bounds.

Here is an example of what an attacker could do with this coding error:

|  |  |
| --- | --- |
|  | $ ./bfrovrflw |
|  | Enter the password : |
|  | hhhhhhhhhhhhhhhhhhhh |
|  | Wrong Password |
|  | Root privileges given to the user |

In the above example, the program gives the user root privileges, even though the user entered an incorrect password. In this case, the attacker supplied an input with a length greater than the buffer can hold, creating buffer overflow, which overwrote the memory of integer “pass.” Therefore, despite the incorrect password, the value of “pass” became non zero, and the attacker receives root privileges.

Slayt = Vulnerabilities in Systems

\*How do viruses, rootkits enter a system? -even without the user doing smt “stupid”.

\*There are vulnerabilities in most software systems:

-Buffer Overflow is the most dangerous and common one .

-How does it work?

-All programs run from memory.

-Some programs allow access to reserved memory locations when given incorrect input.

-Hackers find out where to place incorrect input and take control.

-Easy to abuse by hackers, allows a hacker complete access to all resources.

Slayt = How can you achieve security

\*Many techniques exist for ensuring computer and network security : cryptography, secure networks, antivirus software, firewalls.

\*In addition, users have to practice “safe computing”(good behaviour) : - not downloading from unsafe websites, -not opening attachments, -not trusting what you see on websites, -avoiding scams(if smt is too good to be true, probably it is not true.)

Slayt = Cryptography

\*Simply – secret codes

\*Encryption

-Converting data to unreadable codes to prevent anyone form accessing this information.

-Need a “key” to find the original data – keys take a few million- trillion years to guess.

\*Public keys

-An ingenious system of proving you know your password without disclosing your password. Also used for digital signatures

-Used heavily in SSL connections.

\*Hashing

- Creating fingerprints of documents.

Slayt = Cryptographic Protocols

\*In the symmetric encryption, both sides have private key so, security is provided between these two. So, communication cannot be listened or intersected bc each side knows the private key.

\*In the Asymmetric encryption, one side has public key, one side has private key, messages encrypted using public key and sent to the recipient , recipient opens it only with the private.

Slayt = Why Care?

\*Online banking,trading,purchasing may be insecure o credit card and identity theft

\*Personal files could be corrupted -All school work,music,videos,etc. may be lost

\*Computer may become too slow to run -If you aren’t part of the solution you are part of the problem

\*Upon discovery,vulnerabilities(incinebilirlik) can be used against many computers connected to the internet.