THE PACKET GAME

(Instructions for Students)

The Packet Game is all about learning how information travels the Internet. To play the game each of you will draw ‘packets’  of information and deliver them to the right device in the internet by matching the IP address on the packet with the IP address on the network device within the time allowed.

There are three special roles in this game. The Game Moderator who starts and stops play when there is a cyber attack or if traffic overloads the network. The Network Security Specialist who will help you identify and quarantine threats. And finally, the Router— one lucky student—who has the important job of managing network traffic.

If you are the Router, you are in charge of network traffic and get to tell students when to draw a packet. Your job is to make sure that all the packets are delivered in the time allowed. You can call on students one at a time or in groups— or come up with some other way to organize how students deliver information. Watch out. Traffic jams can overload the network and take it down. So, can cyber attacks. If the network goes down for any reason, you lose time. So, keep traffic moving.

The rest of you are in charge of delivering packets of information over the network safely. When the Router calls your name or points to you, pick one packet. Do not open the envelope yet. Bring your packet to the student playing the Router. He or she will check that your packet has an IP address. (If not, you skip a turn) Once you have checked-in with the Router, you may open your envelope and deliver your packet **but not before!**

But watch out! Not all packets are safe. After you have checked-in with the Router, open the envelope and take a look at the picture on the card inside before you deliver it. If your packet contains information that you think may be unsafe you need to place that packet in quarantine.  If it is safe, deliver the card to the device with the matching IP address. The Network Security Specialist can help you figure out if your packet is ‘safe’ or ‘unsafe.’ Ask for help!

Beware of cyber attacks!  If the Game Moderator announces that the network is attacked by a hacker, all traffic stops. No student can deliver any packets until the threat is identified.  You will have to work together to ‘trace’ the packet that caused the attack and ‘neutralize’ the threat. Find the card that caused the attack and put it in quarantine. Then tell the Network Security Specialist.  If the Network Security Specialist determines that the threat has indeed been neutralized, The Game Moderator will ‘restart’ the Router and students can continue to deliver packets until all the packets are delivered.

The class wins the game if all the packets are delivered in the time allowed, all cyber threats are quarantined and no cyber threats are delivered to any of the devices in the network.

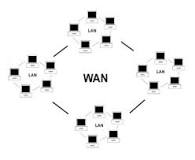
You have only 20 minutes to deliver all the packets.  Starting… now!

*BE CAREFUL. ONLY YOU CAN MAKE THE INTERNET SAFE.*

GAME FAQ

(for reference by Network Security Specialist)

WHAT IS A COMPUTER NETWORK?



[readanddigest.com](https://www.google.com/imgres?imgurl=http://readanddigest.com/wp-content/uploads/2012/08/WAN.jpg&imgrefurl=http://readanddigest.com/what-is-computer-networking/&h=286&w=350&tbnid=O2JOS-SbmoMKMM:&tbnh=160&tbnw=195&usg=__qFtMxPRHIlb4vP0aEFJ1eUnYs3A%3D&vet=1&docid=JoYAWtUSsyZB6M&sa=X&ved=0ahUKEwjfyeiSmZXYAhVX6WMKHfWWBMoQ9QEIKzAA)

A **computer network** is a set of **computers** connected together for the purpose of sharing information (data packets). Computers can be connected to the network by wires or wirelessly using Wi-Fi.

WHAT IS THE INTERNET?

The **Internet** is the global system of interconnected computer networks that use the **Internet** protocol suite (TCP/IP) to link devices worldwide. It is the world’s largest computer network.

WHAT IS AN ISP (INTERNET SERVICE PROVIDER)?

Internet Service Providers are companies that enable people to connect to the Internet. ISP’s employ a range of technologies to connect users to their network, ranging from f telephone lines, to television cable (CATV), [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi), and fiber optic cables. Once connected to the network, users can send information or access information on the internet.

WHAT IS AN IP ADDRESS

When successfully connected to an ISP, you are assigned an [IP address](https://www.computerhope.com/jargon/i/ip.htm), which is a unique address given to your computer or network and allows it to be found while on the Internet. An IP address is typically a series of numbers separated by a period or a colon depending on the IP protocol used.

WHAT IS A ROUTER

A **router** is a **networking** device that forwards data packets between computer networks. **Routers** perform the traffic directing functions on the Internet. A data packet is typically forwarded from one **router** to another **router** through the networks that constitute an internetwork until it reaches its destination node. The IP Address enables the router to identify the computer to which it should deliver the information.

WHAT IS A HACKER?

While "**hacker**" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security **hacker**", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems to gain access to information to which they would not otherwise have access, sometimes for criminal purposes.

WHAT ARE SOME KNOWN TYPES OF CYBER THREATS?

**Malvertising**

Malvertising is a method whereby users download malicious code by simply clicking at some advertisement on any website that is infected. In most cases, the websites are innocent. It is the cyber criminals who insert malicious advertisements on the websites without the knowledge of the latter. It is the work of advert companies to check out if an advertisement is malicious but given the number of advertisements they have to deal with, the malverts easily pass off as genuine ads.

**PUPs**

PUPs, commonly known as Potentially Unwanted Programs are less harmful but more annoying malware. It installs unwanted software in your system including search agents and toolbars. They include spyware, adware, as well as dialers. Bitcoin miner was one of the most commonly noticed PUPs in 2013.

**Drive-By-Downloads**

Drive By Downloads too, come close to malvertising. You visit a website and it triggers a download of malicious code to your computer. These computers are then used to aggregate data and to manipulate other computers as well.

The websites may or may not know that they have been compromised. Mostly, the cyber criminals use vulnerable software such as Java and Adobe Flash and Microsoft Silverlight to inject malicious codes as soon as a browser visits the infected website. The user does not even know that there is a download in progress.

You might want to have a look at our article on Drive By Downloads to learn how to protect yourself.

**Remote Administration Tools**

Remote Administration Tools are used to carry out illegal activities. It can be used to control the computer using shell commands, steal files/data, send location of the computer to a remote controlling device and more.

Read this post to learn more about how you can prevent the illegal use of RATs or Remote Administration Tools.

**Exploit Kits**

A vulnerability means some problem in the coding of a software that enables cyber criminals to gain control of your computer. There are ready to use tools (exploit kits) in the Internet market which people can buy and use it against you. These exploit kits are upgraded just like normal software. Only difference is these are illegal. They are available mostly in hacking forums as well as on the Darknet.

Read our article on Exploits and Exploit Kits to know more about them.

**Scams**

Notable among Internet scams are, scams which misuse the Microsoft name and other general tech support scams. Scamsters phone computer users randomly and offer to fix their computer for a fee. Every single day, scores of innocent people are trapped by scam artists into Online Tech Support Scams and forced to shell out hundreds of dollars for non-existent computer problems.

**Malware**

The term malware is a contraction of malicious software. Put simply, malware is any piece of software that was written with the intent of doing harm to data, devices or to people. When you hear talk of computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs, what you're really hearing is talk of different kinds of malware.

**Computer Virus**

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator. In contrast, a computer [worm](http://searchsecurity.techtarget.com/definition/worm) is stand-alone programming that does not need to copy itself to a host program or require human interaction to spread. Viruses and worms may also be referred to as [malware](http://searchsecurity.techtarget.com/definition/malware).

A virus can be spread by opening an email attachment, clicking on an [executable](http://searchsecurity.techtarget.com/definition/executable) file, visiting an infected website or viewing an [infected website advertisement](http://searchsecurity.techtarget.com/definition/malvertisement-malicious-advertisement-or-malvertising).

**Spyware**

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as keylogging), passwords, and other valuable data.

**Trojan Horse**

In computing, a Trojan horse is a [program](http://searchsoftwarequality.techtarget.com/definition/program) that appears harmless, but is, in fact, malicious. The term comes from Greek mythology about the Trojan War. According to legend, the Greeks built a large wooden horse that the people of Troy pulled into the city. During the night, soldiers who had been hiding inside the horse emerged, opened the city's gates to let their fellow soldiers in and then overran the city.

Attackers have long used Trojan horses as a way to trick end users into installing [malware](http://searchmidmarketsecurity.techtarget.com/definition/malware). Typically, the malicious programming is hidden within an innocent-looking email attachment or free program, such as a game. When the user downloads the Trojan horse, the malware that is hidden inside is also downloaded. Once inside the computing device, the [malicious code](http://searchsecurity.techtarget.com/definition/Malicious-Computer-Code-Glossary) can execute whatever task the attacker designed it to carry out.

Because the user is often unaware that he has installed a Trojan horse, the computing device's security depends upon its recognizing the malicious code, isolating it and removing it.

Unexpected changes to computer settings and unusual activity even when the computer should be idle are strong indications that a Trojan or other malware is residing on a computer. To avoid being infected by Trojan malware, users should keep their antivirus software up to date, never download files or programs from untrusted sources, and always scan new files with antivirus software before opening them.

**Computer Worm**

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

**Ransomware**

Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by [encryption](http://searchsecurity.techtarget.com/definition/encryption), and payment is demanded before the ransomed data is decrypted and access returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as [bitcoin](http://whatis.techtarget.com/definition/Bitcoin), so that the cyber criminal's identity isn't known.

**Phishing**

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.

Phishing is popular with cyber criminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than trying to break through a computer's defenses.

**Spamming**

Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.  It is named after [Spam](https://en.wikipedia.org/wiki/Spam_(food)), a luncheon meat, by way of a [Monty Python sketch](https://en.wikipedia.org/wiki/Spam_(Monty_Python)) about a restaurant that has spam in every dish and where patrons annoyingly shout spam over and over again.