**The Packet Game**

Hour of Code activity focused on computer networks and cyber security. The Packet Game is a role playing game designed to help students understand how information (“packets”) travels the Internet and teaches basic concepts of cyber security.

The Packet Game is a role playing game and does not require students to use a computer.

Inspired by: The Cynja. https://www.cynja.com/

MATERIALS

Designed for 20-30 students (modify as needed)

* 90 IP addressed packets (3-4 “packets” per student). Each packet is an envelope labeled with an IP address that contains a card inside that has a picture of the type of traffic being delivered. Most packets will contain safe pictures. Some will have pictures of cyber security threats.
* 3 Security protocol cards. Cards with pictures that represent a type of security protocol than can be used to prevent cyber attacks. (i.e. firewall, strong password, security preferences)
* 6 manila envelopes labeled with corresponding IP addresses each representing a network device
* 1 Timer
* 1 router card
* Large blackboard, white board or corkboard.   
  2 game moderators (volunteer/teacher)

RESOURCES

https://www.browserling.com/tools/random-ip

https://www.commonsense.org/education/digital-passport

OBJECTIVE

The objective of the game is for the students to work together to safely deliver all of the packets to the correct IP address by matching the IP address on the card with the IP address on the network device. Along the way they will need to learn to recognize cyber security threats , ‘quarantine’ malicious packets, and put in place security protocols to keep the network safe.

This role-playing game is designed to enable students to learn as they go. No advance preparation is needed and in fact knowing too much could ruin the fun!

MODERATORS

The game requires two moderators:

**Network Security Specialist**  
The role of the first moderator is to help students determine if the packet they are carrying is ‘safe’ or ‘unsafe.’ Students who have a question about the image on the back of their card should go to the ‘Network Security Specialist” for help. The Network Security Specialist will have a list of common cyber threats. (See ‘Game FAQ’). Their role is to guide the student in assessing whether or not their packet card is ‘safe’ and can be delivered or presents a ‘threat’ and should be quarantined. In doing so, the Network Security Specialist should take time to explain and help students understand the source of the threat and the different ways to protect against it. If a cyber attack occurs, the Network Specialist should help students trace and quarantine the threat and is tasked with announcing when the threat has been neutralized.

**Game Moderator (aka the ‘Hacker’)**   
The role of the second moderator is to play the ‘Hacker.’ This moderator, referred to in the game to students simply as the ‘Game Moderator’, is responsible for instigating and managing cyber attacks. The goal of the Hacker is to ensure that cyber attacks occur early (and if desired, often!) in the game. It is the Hacker’s job to discreetly slip one or more packets containing cyber threats into the hands of the players. How they do it is up to them. Once a threat is in play and is sent to the Router, the Hacker will announce that the network has been attacked. The Hacker then instructs the student who is playing the role of the Router to sit down and stop routing traffic. Once the network has been attacked, students can no longer deliver packets until the class has successfully traced the type of threat, placed the malicious packet in quarantine and put an appropriate security measure in place. Throughout the game, the Hacker should continually work to figure out the best and fastest way to take down the network all while keeping his/her true identity a secret. At no time during the game should the Hacker reveal to students that he/she is the Hacker.

SETUP

The classroom blackboard should be divided into three sections and labeled accordingly. The three sections are 1) network 2) quarantine and 3) security. The majority of the blackboard should be devoted to ‘network’ with smaller sections at student height demarcated for ‘quarantine’ and ‘protection’.

Place all the IP addressed packet envelopes into a brown bag. Or, if in table groups divide the packets evenly amongst the table groups, one bag per group. Students should draw packets at random should not open the envelopes until instructed to do so by the Router. Remember some packets will contain cybersecurity threats.

HOW TO PLAY

1. To start the game, students must first build the network. To do this, students can raise their hands, or if in table groups, one student from each table group picks out a ‘network device’ and tapes that manila envelope to the blackboard in front of the classroom. The student should very briefly explain/share what the device is to the class. Each device is labeled with an IP address. This is where ‘packets’ will be delivered. NOTE: As the students are building the network, the Network Security Specialist should explain basic concepts (i.e. that the Internet is a computer network, what an IP address is, and how information is sent in packets from one computer to another via a router.)
2. Next, one student is assigned the role of playing the Router. The Router is in charge of managing network traffic by pointing to students and letting them know when it is there turn to deliver their packet. The Router has only the time allowed on the timer to make sure all traffic is delivered safely to the correct IP address.
3. To start the game the student playing the role of the Router will point to a student and ask them to draw one packet from the brown bag containing packets and bring it to the Router. The timer is then started. The identified student must show the IP Address on the packet to the Router before continuing on to deliver the packet to device matching the correct IP address. Once the student has checked in with the Router and is sent by the Router to deliver their packet, the Router may point to another student to draw a packet from the brown bag and bring it to the Router.
4. After leaving the Router and before delivering the card, each student must open the packet and check the picture on the card inside to determine if it is ‘safe’ or ‘unsafe’ to deliver. If the card is ‘safe’ students should place it into the manila envelope on the blackboard that matches the IP address on the card. If the card is ‘unsafe’ they should ‘quarantine’ it by taping it to the quarantine section of the blackboard. If they have a question about whether or not the packet is safe they should check with the Network Security Specialist before delivering it! Be careful!
5. Play continues until all of the packets have been delivered. It is expected and encouraged that the Router will develop ever more efficient ways to direct traffic to enable all of the packets to be delivered in the time allotted. It is up to the Router to figure out how best to do that.
6. If at any point in the game it is announced that the network has been compromised by a cyber attack, the student playing the Router must lie or sit down on the floor and stop routing traffic. Students can no longer deliver packets until the class has successfully traced the type of threat, placed the malicious packet in quarantine and put appropriate network security in place to prevent future similar attacks. They should consult with the Network Security Specialist for help. If a threat has already accidentally been delivered to a network device, the students must track it down by checking through each of the envelopes and place it in quarantine. Once the Network Security Specialist announces that the threat is ‘neutralized’ , the Game Moderator instructs the Router to ‘restart’ and play continues.
7. Plan for each student to make 2-3 round trips to the blackboard.
8. The students collectively ‘win’ the game if all of the packets are delivered in the time allotted, all cyber threats are quarantined and no cyber threats are allowed to be delivered to any of the devices in the network. If not, the Hacker wins the game.

DISCUSSION

Several of the students will have had the unhappy fortune of having had to deliver cyber threats. After the game, these students should be invited to start a discussion by coming to the front of the classroom and one by one explaining to the rest of the class the name and nature of the threat and the best way to protect against it in real life.

Time permitting, students can guess the identify of the Hacker. Alternately, the Game Moderator (aka the Hacker) may announce his or her true identify.

The rest of the available time can be spent discussing cyber threats in real life and how best to protect themselves and their families as they browse the Internet.

KEY TAKE-AWAYS

1) A network is just a number of computers/devices that have each been assigned an IP address so that they can send information ("packets") to each other. The internet is an open, public network.

2) Most information on the internet is safe; some information is unsafe. Browsing the internet is just like walking on a city street. You need to be aware:

* + Don't click on ads. (malvertising is the most common cyber threat)
  + Look out for and read any popups that appear on your screen. (drive-by-downloads; malware)
  + Don't respond to emails from friends that don't quite sound like your friend. (phishing)
  + Don't share personal information by email or on social media (social engineering)
  + Use strong passwords and don't share passwords (spyware)
  + Look out for changes in how your computer works (i.e. new homepage) (worms, trojans, viruses)

1. If you see something, say something. Tell a parent or teacher.

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 from this bag and deliver them to the right device in the network by matching the IP address on the packet with the IP address on the network device. All the packets need to be safely delivered to the right network device as quickly as possible! You only have a limited amount of time, and you’ll need to work together to succeed.

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 from the bag. 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 and need to wait to be called on to draw a new packet.) 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.’ It’s a good idea to ask for help!

Watch out for 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 allotted, all cyber threats are quarantined and no cyber threats are allowed to be 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 THE INTERNET

WHAT IS AN ISP (INTERNET SERVICE PROVIDER)?

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 dependinf on the IP protocol used.

WHAT IS A ROUTER

WHAT IS A HACKER?

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.

In other cases, the cyber criminals show clean ads for a period of time and then replace it with malverts so that the websites and advertisements do not suspect. They display the malverts for a while and remove it from the site after meeting their targets. All this is so fast that the website does not even know they were used as a tool for cybercrime. Malvertising is one of the fastest, increasing types of cybercrime.

Our article on [Malvertising](http://www.thewindowsclub.com/what-is-malvertising" \o "What is Malvertising" \t "_blank) and [Badware](http://www.thewindowsclub.com/what-is-badware" \o "what is badware" \t "_blank) will tell you how you can stay safe.

**Protection**:

**PUPs**

PUPs, commonly known as [Potentially Unwanted Programs](http://www.thewindowsclub.com/potentially-unwanted-programs-pup" \o "Potentially Unwanted Programs or PUPs" \t "_blank)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.

**Protection**:

**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](http://www.thewindowsclub.com/drive-by-downloads" \o "Drive-by downloads" \t "_blank) to learn how to protect yourself.

**Protection**:

**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](http://www.thewindowsclub.com/remote-administration-tools-emerging-threats" \o "Remote Administration Tools" \t "_blank).

**Protection**:

**Exploit Kits**

A [vulnerability](http://www.thewindowsclub.com/what-is-vulnerability-in-computer-security" \o "What is a Security Vulnerability" \t "_blank) 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](http://www.thewindowsclub.com/darknet-deepnet" \o "what is darknet" \t "_blank).

Read our article on [Exploits and Exploit Kits](http://www.thewindowsclub.com/what-are-exploits-and-exploit-kits" \o "What are Exploits and Exploit Kits" \t "_blank) to know more about them.

**Protection**:

**Scams**

Notable among Internet scams are, scams which [misuse the Microsoft name](http://www.thewindowsclub.com/microsoft-scams" \o "microsoft scams" \t "_blank)and other general [tech support scams](http://www.thewindowsclub.com/avoid-online-tech-support-scams" \o "Avoid Online Tech Support Scams " \t "_blank). 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.

**Protection**:

**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.

**Protection**:

**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). It can also be spread through infected removable storage devices, such [USB drives](http://searchstorage.techtarget.com/definition/USB-drive). Once a virus has infected the host, it can infect other system software or resources, modify or disable core functions or applications, as well as copy, delete or [encrypt](http://searchsecurity.techtarget.com/definition/encryption) data. Some viruses begin replicating as soon as they infect the host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system.

Many viruses also include evasion or [obfuscation](http://searchsoftwarequality.techtarget.com/definition/obfuscation) capabilities that are designed to bypass modern [antivirus](http://searchsecurity.techtarget.com/definition/antivirus-software) and [antimalware](http://searchsecurity.techtarget.com/definition/antimalware) software and other security defenses. The rise of [polymorphic malware](http://searchsecurity.techtarget.com/definition/polymorphic-malware) development, which can dynamically change its code as it spreads, has also made viruses more difficult to detect and identify.

**Protection**:

**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.

**Protection**:

**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.

**Protection**:

**Computer Worm**

A computer worm is a standalone malware computerprogram 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.

**Protection**:

**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 cybercriminal's identity isn't known.

Ransomware [malware](http://searchmidmarketsecurity.techtarget.com/definition/malware) can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites. A growing number of attacks have used [remote desktop protocol](http://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP) and other approaches that don't rely on any form of user interaction.

In a lockscreen variant of a ransomware attack, the malware may change the victim's login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network devices.

While early instances of these attacks sometimes merely "locked" access to the web browser or to the Windows desktop -- and did so in ways that often could be fairly easily [reverse-engineered](http://searchsoftwarequality.techtarget.com/definition/reverse-engineering) and reopened -- [hackers](http://searchsecurity.techtarget.com/definition/hacker) have since created versions of ransomware that use strong, [public-key](http://searchsecurity.techtarget.com/definition/public-key) encryption to deny access to files on the computer.

**Protection**:

**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 cybercriminals, 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.

**Protection**:

**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.

**Protection**: