

SEEK18 Cybersecurity Module Teacher Guide

Day 1: Living in Cyberspace	5
Security	5
Cybersecurity = Security in Cyberspace	7
Computer is like a Three-layered Cake	9
Raspberry Pi 3 Computer	12
Review Vocabulary	12
Activities:	12
Design Challenge Stage One	12
Day 2 Attacks and Defense	13
Be Smart online, Be Cybersmart	13
Exercise: T.A.D. (Threat, Attack, and Defense) Smart	14
Exercise: Protect your cell phone from a “Shoulder-Surfer” Attack	15
Targets, Threats, Attacks, Vulnerabilities, and Defense	16
Vocabularies	16
Targets, Threats, Attacks, and Defense in Cyberspace	18
Common Threats to a Computer	18
Common Cyber Attacks	18
Attack Types	19
KEYLOGGER ATTACK	19
PHISHING ATTACK	19
SOCIAL ENGINEERING ATTACK	19
BRUTE FORCE ATTACK	20
DICTIONARY ATTACK	20
EAVESDROP ATTACKS	20
DENIAL OF SERVICE ATTACK (DoS)	21
Common Defense	21
Group Activities:	22
Charades	22
Review Vocabulary	22
[Extra] How can someone guess your password?	23
[Extra] A Computer Network Under Attack	24
Day 3 Online Activities	25
Identity Theft	28
Accounts - Your Online Identities	28
Protect Your Accounts	28
Good Passwords	28

Account Authentication	29
“What You Are” Authentication	29
“What You Know” Authentication	30
“What You Have” Authentication	30
How to Protect Your Account	31
Diceware	32
How does Website Work	33
Day 4 Network Attacks and Defense	34
Online Data	34
Computer Data Type	34
What does Data Security Mean?	35
To Protect Data Security	36
Review Vocabulary	37
Computer Network Model	38
Build a Computer Network	38
EAVESDROP ATTACKS - Unsecured Interfaces	38
Defense Against Eavesdrop Attack: Encryption	40
Cyber Codes	42
DENIAL OF SERVICE ATTACK (DoS)	44
DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS)	45
BotNet and Distributed Denial of Service Attack	46
DEFENSE Against Denial-of-Service Attacks from Individual User	46
DEFENSE Against Denial-of-Service Attacks from a Company - Advanced	48
DEFENSE Against Denial-of-Service Attacks and Gate Rush	49
Internet-of-Things Devices	49
Class Activity: Infection (Zombie Net; Coordinated Network Attack)	50
Class Activity: DDOS Demonstration	51
Day 5 Games and Competition	53
Design Challenge Game - Model for Cyber Security	53
Artistic Competition	53
Physical Competition	53
Word Swap	53
Collect Them All (Decryption Race)	54
Oral Presentation	54
Physical Competition	54
References:	55
For Parents:	55
For Future Cybersecurity Experts	55

Summer Engineering Experience for Kids

System Engineering

Engineering Design Challenge



Cyber Security

Teacher Instructional Guide



Dear Mentors,

Over the course of the week, our young engineers will be taking on the Cyber Security Challenge. Engineers will work in teams of 4-5 to apply the Engineering Design Process (EDP) and the scientific concepts related to simple

machines, force, energy and motion. Below you will find your week -at-a-glance, a materials list, and some background information that will help you prepare for the challenge topic area. Also included is a copy of the challenge letter as well as the end of week challenge expectations.

Student Challenge Letter: Dear Young Engineers,

Recent hacking activities in Cyberspace have caused communities, companies, and nations around the world billions of dollars. Many users also fall victim to identity theft and account takeover. The National Society of Black Engineers (NSBE) is giving you a special challenge to work together to build a physical model of Cyberspace for an unknown society. Each group would create a computer network model for an important function in this society. These functions include law enforcement (police station), public health (hospitals), transportation (air travel, ocean, and land roads), energy (power plant), and finance (banks and stock market). Each computer network model support a function, and the networks are connected together by the Internet, controlled by the mentors. The young engineers need to design their network to survive the various attacks from the Internet.

End of Week Challenge Activities

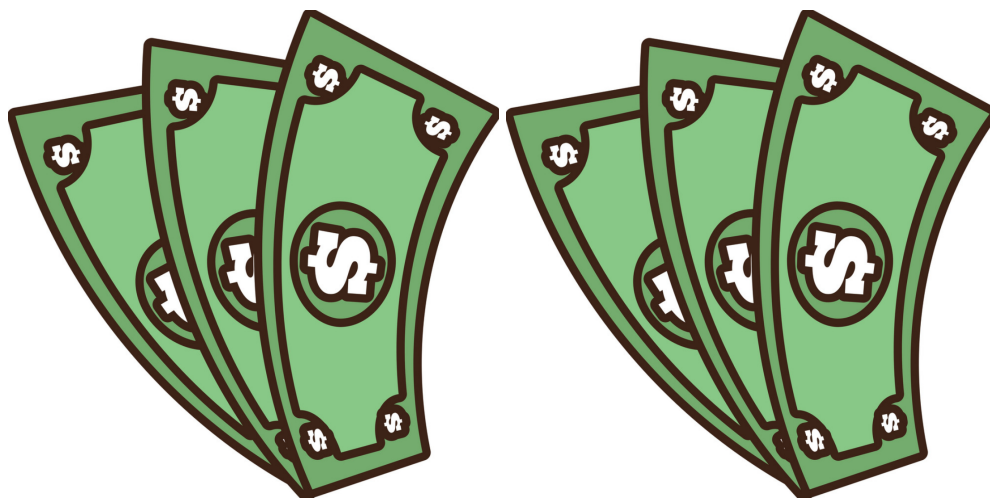
There are **five** competition categories that your teams will compete in: **Engineering Content Presentation, Artistic Design Presentation, and Target Challenge, Accuracy Challenge, and a Race Challenge.**

Respectfully,
Amanda Jones

Day 1: Living in Cyberspace

Security

At this camp, we will teach you about Cyber Security in Cyberspace. Before I explain what that means and why it is important, let's find out what you know. Who likes money? I want you to imagine that you have a whole chest full of money.



Do you think your money would be safe if you left it out on the street where everyone could see it? How about if you left it out in your school? How about in your house? Is it safe? I am talking about security.

Why wouldn't it be safe? (Answers: Because someone would take it).

If you left your money outside and you weren't watching it, how would someone take your money? (Right, they'd just walk up and take it). If someone wanted to take your money, but you left on the kitchen table at your house, how could they take your money? (Example answers: Sneak in, wait until no one was home, pretend they are a plumber coming over to fix the kitchen sink.) Your money is safer in some place.

Words to know:

SECURITY is "Free from danger or threat."

CYBER is computer.

CYBERSECURITY is the security in cyberspace.

CYBERSPACE is an online world created by the Internet.

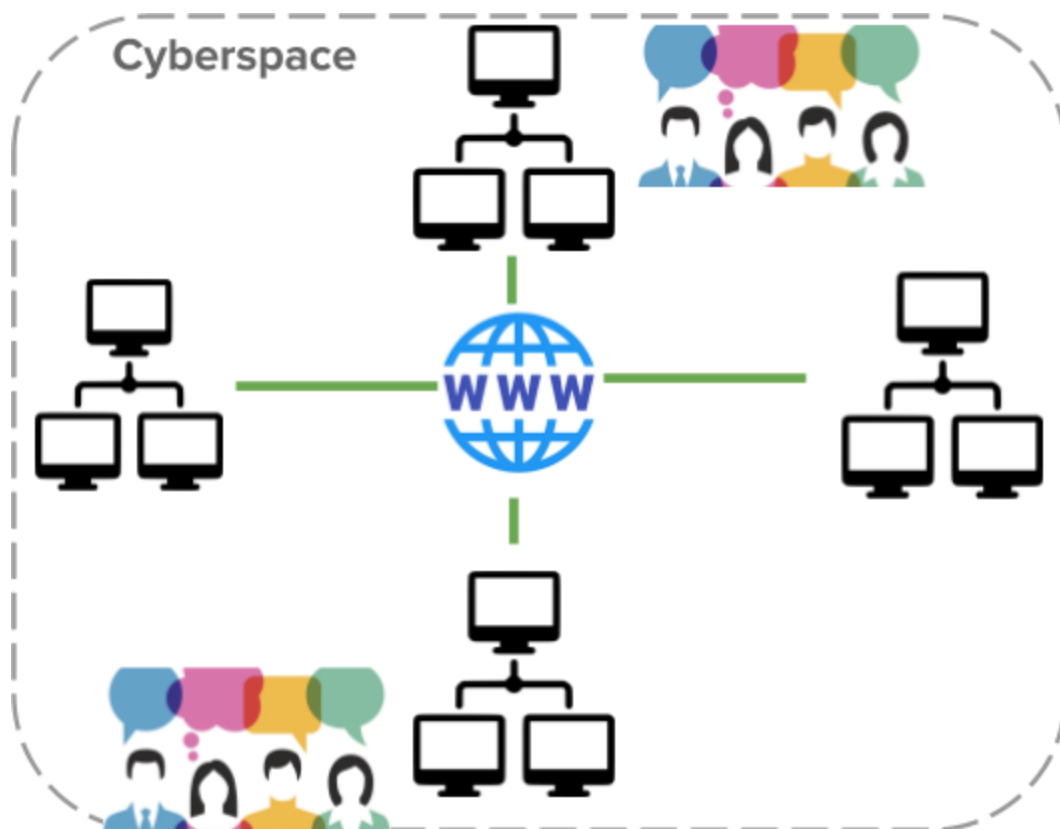
The INTERNET is a global computer network of public computer networks.

A COMPUTER NETWORK is a network of connected computers.

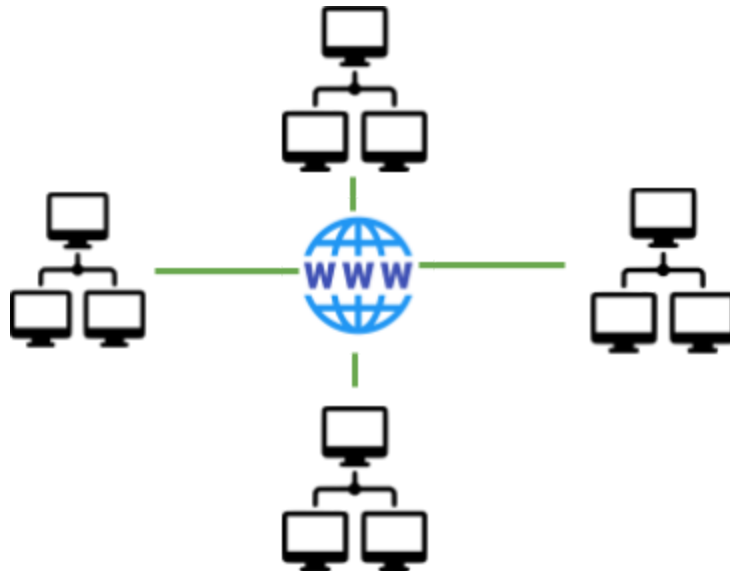
Cybersecurity = Security in Cyberspace

Cyber + Security is **Cybersecurity**, and it is to protect against attacks in **Cyberspace**.

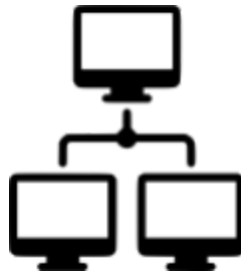
Where is **Cyberspace**? Cyberspace is the online world created by the Internet.



The **Internet** is a physical and global network consisted of connected computer networks.



Moreover, a **computer network** is a network of connected computers and devices.



Cybersecurity is the protection of the computer networks from attacks.



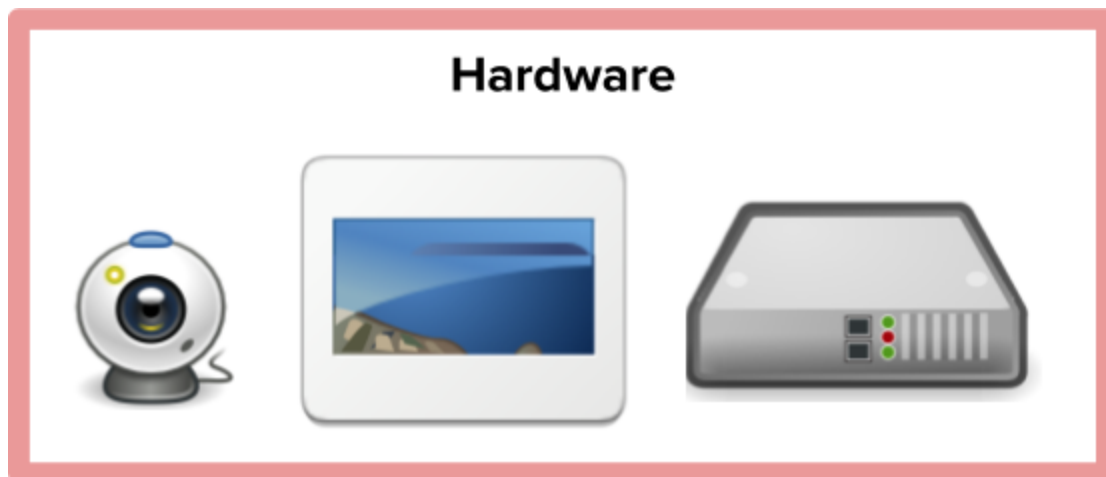
The job of Security Experts is to protect computer networks. It's an very important and challenging job. You could think of them as Space Galaxy Defenders. To become an Security Export, we need to learn more about computers. Let's dig deeper.

Computer is like a Three-layered Cake

You probably are pretty good with computers, but do you know that computers have layers? Like a piece of delicious three-layered cake, a computer to work, it has roughly three layers.



Let's start from the strawberry layer, or the hardware layer. The **hardware** is the physical device. It includes the screen, the speaker, the camera, radios, the GPS, the processor, the memory, and many more.



Next layer up is the lemon layer, or Operating System layer. The most important software on your hardware is the **operating system**. There are many different types of operating system, such as Windows (window), or Apple OS (apple), or Linux OS (penguin). The operating system is what connects the hardware to the apps and you. You are the user. When you turn on the computer, the first thing that starts up is the operating system. The operating system has to start working before it can show you all the apps. The operating system is what shows you the apps that you can run.

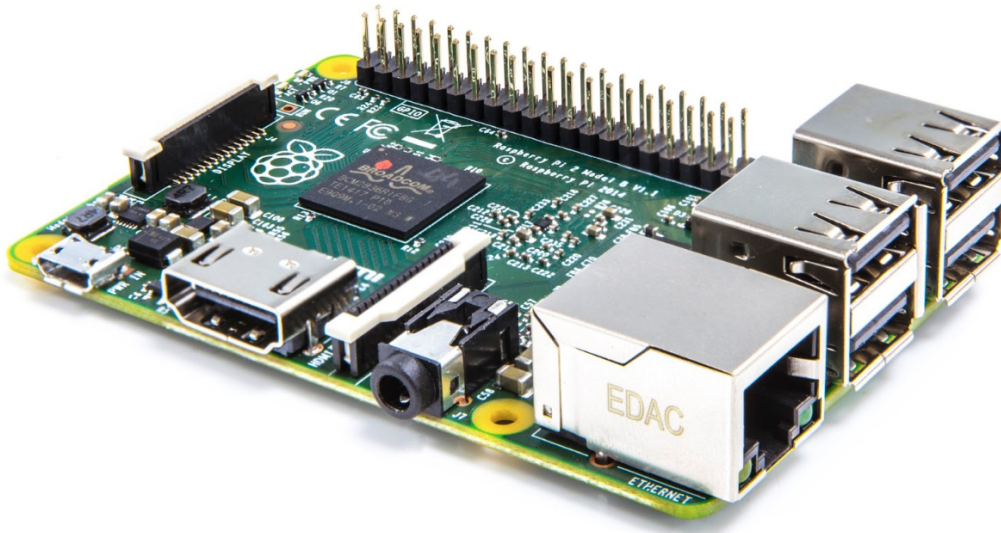


The top blueberry layer is the **Application** layer. When you use a phone or a computer, you would likely see small icons on the screen. What are the icons? Those icons are shortcuts to the Applications that you can run. You may have used applications or apps such as the phone app, the browser app, the chat app, and many others.



Raspberry Pi 3 Computer

Ask the students to work on Day 1 Computer Lab.



Review Vocabulary

- Cyber
- Cyberspace
- Internet
- Computer Network
- Cybersecurity
- Operating System

Activities:

- Charades: Guess the vocabularies
- Vocabularies Practice
 - Worksheet
 - Crossword

Design Challenge Stage One

Play the CyberAttack! game to learn the about CyberSecurity.

Day 2 Attacks and Defense



Be Smart online, Be Cybersmart



Cyberspace is like a foreign country you are visiting for the first time. When you are there, it's not enough that you are Book Smart (and you should be), but you must also be Street Smart. To be Street Smart in Cyberspace is to learn the following:

- Danger or threats
- Attacks
- Defense
 - Before Attack: prevention
 - During Attack: battle strategy
 - After Attack: recovery

We are going to learn several very important concepts in security today. It's the concept of threats, attacks, and defense. Let's demonstrate to help you understand.

Exercise: T.A.D. (Threat, Attack, and Defense) Smart

Let's look at another example. Micah is pretty hungry as he gets ready to eat his sandwich at the picnic table. But he needs to use the restroom. What are the possible threats to his sandwich while he is gone?



- A bird ready to make a dropping
- Joe, Micah's little brother, who is known for tripping over anything and everything, holding a giant bucket of iced water and walking wobbly toward the table
- Stacie, Micah's cousin, who is always hungry and loves to help herself with others' food, looking at the sandwich with intense interest

If Stacie does take Micah's sandwich while he is gone, then her taking the sandwich is called an attack.

What do you think is a good defense against Stacie's attack? (Ask someone to watch your sandwich, take your sandwich with you, etc.)

Exercise: Protect your cell phone from a “Shoulder-Surfer” Attack



THREAT: Someone wants to use your cell phone without your permission.

ATTACK: They watch you enter your password over your shoulder (meaning you don't know they are watching) and wait for you to be careless with your phone.

DEFENSE: What are some good defenses?

(A: Cover your phone when you enter your passcode. Use your biometric signature such as a thumbprint so that no one can steal your password - just make sure no one steals your thumb or your thumbprint. Demonstrate biometrics using thumbprint or photo if someone has a phone with the biometric interface.)

Targets, Threats, Attacks, Vulnerabilities, and Defense

Vocabularies

- A **TARGET** is something or someone that can be attacked, and should be protected.
- A **THREAT** is a person, thing, or condition that can potentially cause damage or danger to a target.
- An **ATTACK** is an action taken against a target.
- An **INTERFACE** of a computer is an opening to access the data on that computer
- A **VULNERABILITY** is a weakness that makes a target easy to be attacked
- **DEFENSE** is an action taking against an attack.

Imagine you are traveling in a city for the first time, and you are carrying a lot of cash. Don't ask me why. You are just rich like that. Since you are a tourist who are carrying valuables, you are a target. How can you protect yourself and your valuables?



You have to be street smart. You have to be aware of your surroundings, know how you may be attacked, and keep your valuable in a safe place. You also should have a **plan** if your valuable is taken. For example, what would you do if your passport or your wallet is stolen?

[Mentor Demonstration] I need to buy something from the convenience store, but I put the money in my back pocket (put fake money in your backpocket, easily visible). What do you think it will happen? The wind may blow it away. A pickpocket can steal it. Or I could just buy toys I don't really need. These potential dangers are called threats.

[End Mentor Demonstration]

If someone does steal my money, then that's an attack. That person can take my money, the target, because I leave it out in the open, making it vulnerable. The location of the money becomes a vulnerability.



What if you put the money in a house?



A house has many openings, such as a window, a door, or even chimney. Every opening can be broken into therefore needs to be protected. Just like a house, a computer has many “openings” as well. These openings are called interfaces, which allow you to get data from and write to your computer. These interfaces are vulnerabilities and need to be protected against hackers and malicious programs.

Targets, Threats, Attacks, and Defense in Cyberspace

In Cyberspace, a computer is a target that has vulnerabilities and can be attacked at all three layers. Just like a house or a human body which both has openings, a computer has openings as well. Its openings are called interfaces. Examples include WiFi, Bluetooth, and USB port.

Common Threats to a Computer

The most common Cyberspace threats include:

- Malware
- Cyber Attacks
- Human errors
- Hardware failures
- Power outage
- Natural disaster

Common Cyber Attacks

The most common Cyberspace attacks include:

- Keylogger Attack
- Phishing Attack
- Social Engineering Attack
- Brute Force Attack
- Dictionary Attack
- Credential Reuse

Attack Types

KEYLOGGER ATTACK



Another type of ATTACK is called a KEYLOGGER ATTACK. In this attack, the cybercriminal sneaks a program onto your computer that copies all of your keystrokes. The attacker reviews all of your keystrokes to find the usernames and passwords.

Defense: Protect Your Computer.

PHISHING ATTACK



Another common attack is called PHISHING. You say it the same as you would say fishing. In the PHISHING attack, the cybercriminal puts out bait in the form of an email. Guess what the cybercriminal is phishing for? It's phishing for you.

The email may say something like: "Mr. Click-A-Lot, you need to update your password now and please click this link." When you click on the link to change your password, it will ask for your username and old password to prove your IDENTITY. What is it doing? Stealing your password so it can get to your ACCOUNT.

SOCIAL ENGINEERING ATTACK



SOCIAL MEDIA is fun. But learn to be cyber smart. If you share your DATA unwisely, you make yourself a target for an ATTACK. What are some common ways users can be unwise about sharing their DATA on SOCIAL MEDIA. One is to OVERSHARE or to share without careful consideration.

BRUTE FORCE ATTACK



One attack pattern is called BRUTE FORCE ATTACK. In a BRUTE FORCE ATTACK, a cybercriminal tries every possible combination of passwords. Your best defense is a long password.

DICTIONARY ATTACK



Another type of ATTACK is called a DICTIONARY ATTACK. The hacker guesses your password by using a computer program to run through all the words in a dictionary. Do you think it is a good idea to use a word out of the dictionary for a password? (Defense against dictionary attack: pick good password, don't use common words)

EAVESDROP ATTACKS



Eavesdrop Attack is when hackers listen on the unsecured network connection and steal sensitive information.

For example, someone can extract passcodes sent from the car key or garage opener, then use it to unlock car or a garage door.

DENIAL OF SERVICE ATTACK (DoS)



The Denial of Service Attack is when hackers send a lot of fake requests to a Computer System that it is unable to process the real request. Have you heard of prank calls? Prank calls are people who make so many fake calls to the police station or fire station so the first responders are swamped with fake incidences and cannot help the people who truly need help. This is a form of Denial of Service Attack.

Common Defense

- Be cybersmart
 - Being vigilant and careful when online, just as if you are in a unfamiliar place
- Don't overshare
- Use better and more secure password
 - Follow the better password guideline and select more secure password
 - Don't share your password with anyone
 - Don't reuse your password for different sites.
- Protect your machines
 - Use Anti-Virus software to scan and block virus
 - Install software patches regularly to fix security vulnerabilities
 - Think twice before installing freewares.
- Visit safe sites and check the browser warnings.

Group Activities:

Charades

Guess the vocabularies by acting out the word

Review Vocabulary

- Attack
- Threat
- Vulnerabilities
- Defense
- Target
- Brute Force Attack
- Dictionary Attack
- KeyLogger Attack
- Denial of Service Attack
- Eavesdrop Attack
- Social Engineering Attack
- Keylogger Attack
- Shoulder-Surfer Attack
- Ransomware Attack

Day 3 Online Activities



(

Trust is the belief in the reliability, truth, ability, or strength of someone or something.

You can trust someone or in something. You can trust your friend. You can trust that your environment is safe
You can trust in information. There is different level of trust.

You may trust somebody, but how can you be certain they are who they say they are? How would you prove that you are you?

Identity is the fact of being who or what a person or thing is.

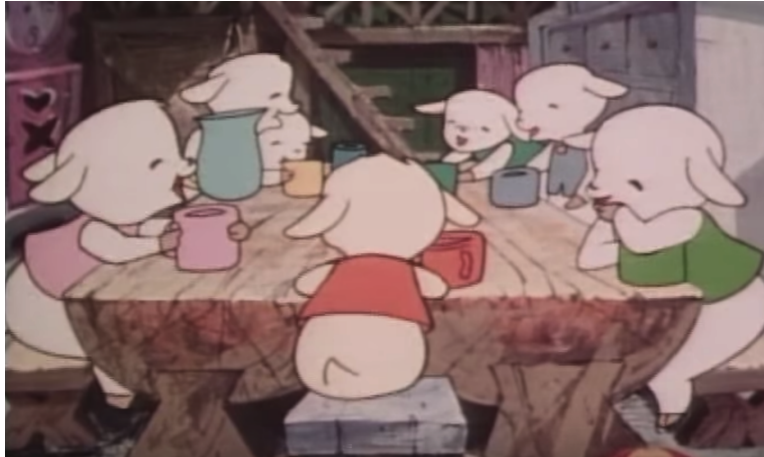
Let's start with your cell phone. Later, we will talk about the rest of Cyberspace. How does a cell phone know your IDENTITY? What is a PASSWORD? (A: a secret word or number that identifies the person as the individual). When a PASSWORD is only numbers, it is sometimes called a passcode or a PIN.

Is your PASSWORD your IDENTITY? (A: you do not share your phone with anyone, your phone is part of your IDENTITY, the PASSWORD is used to prove it).

Your phone, and as we will see later, other computers, need a way to prove that you are who you say you are. Proving to a computer that you are who you say you are is called AUTHENTICATION. Authentic means real or genuine. The computer needs to know if you are the real owner of the phone.

Let's watch a video of a story that tells what bad things could happen if someone pretends to be someone else, even in a fairytale. This story is called The Wolf and Seven Little Kids

(<https://www.youtube.com/watch?v=GswJyEh7jgA>), and the animation was created by a Japanese Anime company in 1976.



[Discuss]

What is the THREAT and what is the ATTACK? Talk about TRUST, IDENTITY, and AUTHENTICATION. What could better DEFENSEs the sheep have used to prevent Wolf's trickery?

THREAT: the hungry wolf wanting to eat the kids,

ATTACK: the Wolf tried to break in pretending to be the mom, to breach the security (door)

DEFENSE: A door only to be opened for the mom.

TRUST: the kids thought the Wolf was mom,

IDENTITY: mom,

AUTHENTICATION: mom's hands, feet, and voice

[Explain]

You prove your IDENTITY through AUTHENTICATION.

Authentication is the process in which you prove to a computer, that you are who you say you are.

There are these main categories of AUTHENTICATION used to prove your identity.

- What you know
- What you have
- What you are (the kids in the story use to determine whether someone is mom)

Can you guess what authentication the Wolf uses to (falsely) authenticate itself?(Answer: the "What You Are" authentication method)

[Challenge]

Can you teach the kids in the Wolf and Seven Kids a better to AUTHENTICATE, to prove ?

Identity Theft

Have you ever checked out books from the Library? What do you use to prove your identity? You usually use a library card. What if your library card is stolen and then someone else checks out loads of books and do not return them. If someone uses your card and pretend to be you, then you have become a victim of identity theft.

Accounts - Your Online Identities

When we talk about going into CYBERSPACE to use a computer server, you may have to set up an ACCOUNT, so that the server knows who you are, so it can keep track of your DATA or maybe even charge you or your parent's money to use it.

To set up an ACCOUNT on the server, you will have to create a username and a PASSWORD. The username is your unique IDENTITY on that server computer that must be different from all the other users of that server. The username tells the server who you are. You create a PASSWORD so you can AUTHENTICATE (prove that you are who you say you are) to the server. The SERVER will also ask for other personal information like your email address and answers to questions that you should know the answer to, in case you forget what your PASSWORD is.

Once you have an ACCOUNT set up, you can use the services of the SERVER. Every server provides services that you may want to use such as Instagram, Netflix, or PlayStation (other sites kids tend to use). Services are why people use the Internet in the first place. The Internet is convenient, but it can be an also be too open and dangerous if you are not careful. Many people store their pictures and personal information online, but how safe are those data?

Data passed through the Internet Convenience is the good part of the Internet. But what is the THREAT? (stolen account information, including username and password)

Protect Your Accounts

To protect your IDENTITY, you should protect your AUTHENTICATION methods. If you use a student ID to prove that you can check out books at the library or get on the bus, you should make sure you keep your student ID safe. You may also have several online ACCOUNTs, and use PASSWORD to log in. Then it's important that you have a good password.

Account Authentication

Authentication is to prove that someone is the owner of this account.

“What You Are” Authentication (Biometrics)

In the cartoon, the sheep are using the “What You Are” AUTHENTICATION methods to determine if the Wolf is their mom. But the Wolf is shrewd and manages to fool them. For the kids today, he would have to be smarter to trick them successfully. Today’s little sheep have several ways to authenticate including fingerprint, facial recognition, voice recognition, iris reading, and possibly even DNA shortly! When the computer authenticates us using something unique about our bodies, we call this BIOMETRIC AUTHENTICATION.

Fingerprint



Face



Voice



Eye



Although the Biometric Authentications are convenient-no password needed, they can be forged. Someone close to you can steal your fingerprint, record your voice, or take a close-up picture of you. Iris scanning is harder to crack but it’s also possible.

[Exercise]:

Have students create authenticate card that identifies themselves. Shuffle all the cards, and have a student of different group matches the cards to students. Suggest using fingerprint and picture they draw of themselves, and a smiley face signature.

“What You Know” Authentication

The “What You Know” categories include password or passphrase. The password works like the “Open Sesame” phrase in the story of Ali Baba and the Forty Thieves. A secure password needs to be complex enough, else it can be guessed. A secure password should also be changed frequently in case someone cracks or steals the password.

[Exercise]

Use a knock as the password. What is an example of a bad knock to use as a password? (Example: Shave and a haircut, two bits).

What is a simple ATTACK of a knock? (Example: listen and replay)

“What You Have” Authentication

The “What You Have” categories include physical keys or tokens. Whoever owns these things are also trusted.



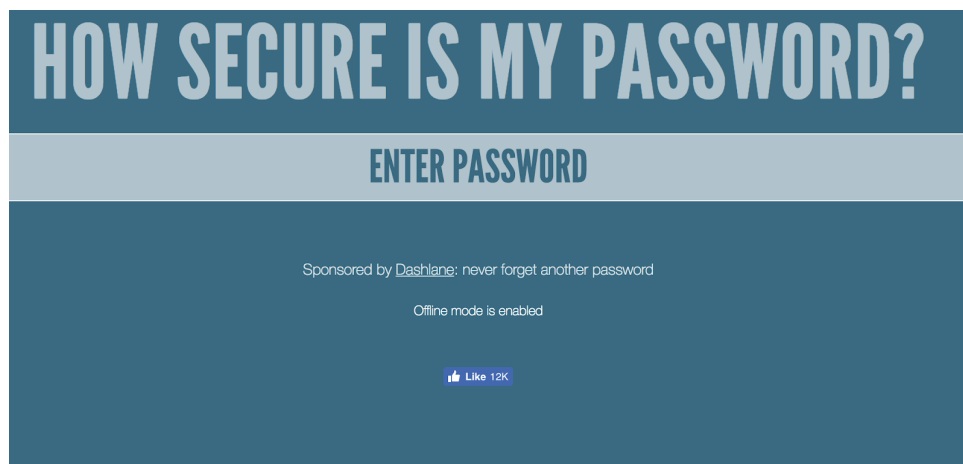
- Key
- Smartcard or badge
- Token (an electronic key)

How to Protect Your Account

The most important way to protect your account is to protect the account authentication, to make it hard for someone to steal your account. The most common way is to have better passwords.

[Exercise]

Visit <https://howsecureismypassword.net/>.



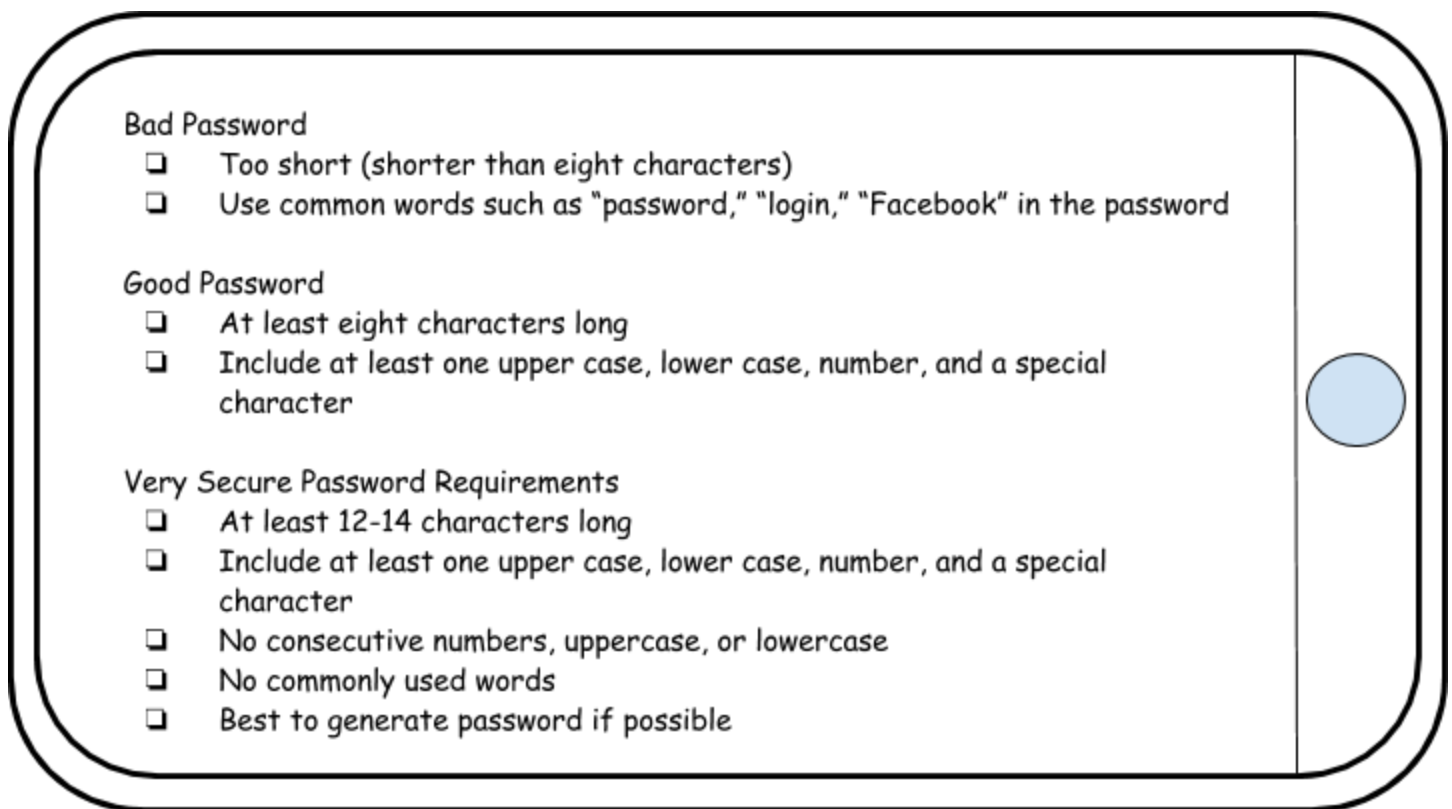
Try the password “password.” How long would it take for a hacker to steal your password?

Try the password \$someRandom\$phraseWithNumber9.

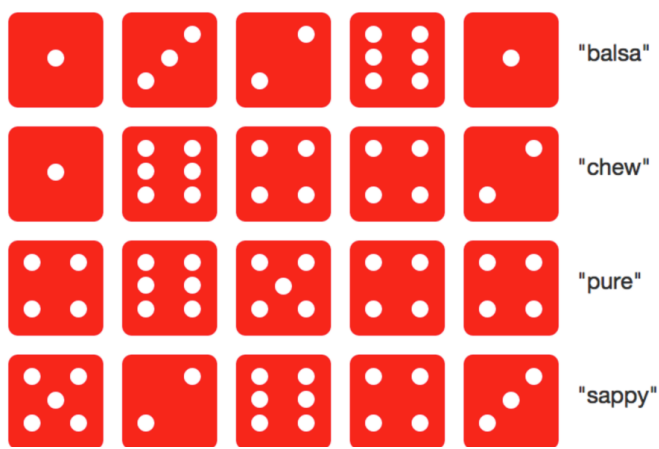
Think of 5 passwords and let’s test how strong each of your password

How did you do? How long would it take to crack your password? What score did you get?

Here is a chart that will remind you what are bad and good passwords. Some very important accounts should be protected with very secure passwords.



Diceware



Diceware is a creative method that uses randomness to generate secure passwords.

How it works:

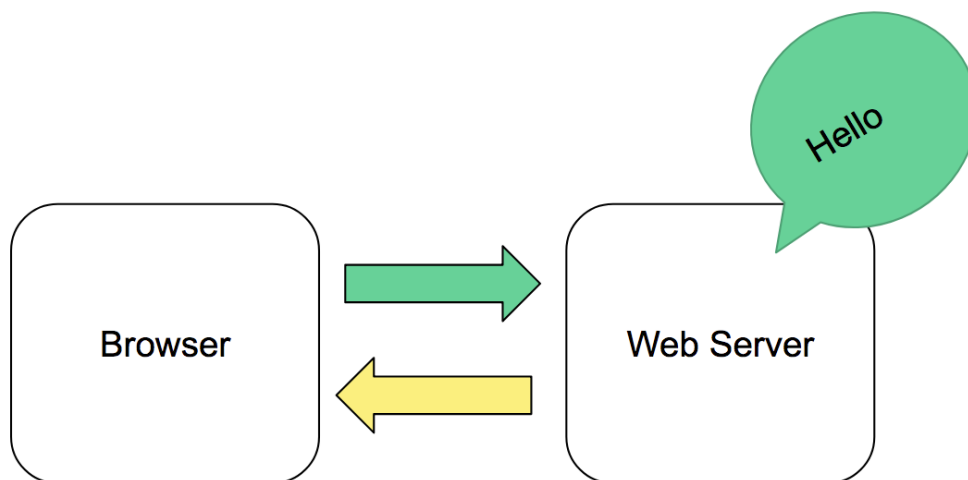
- Roll a dice several times to form a number
- Use the number to find a word in a dictionary

How does Website Work

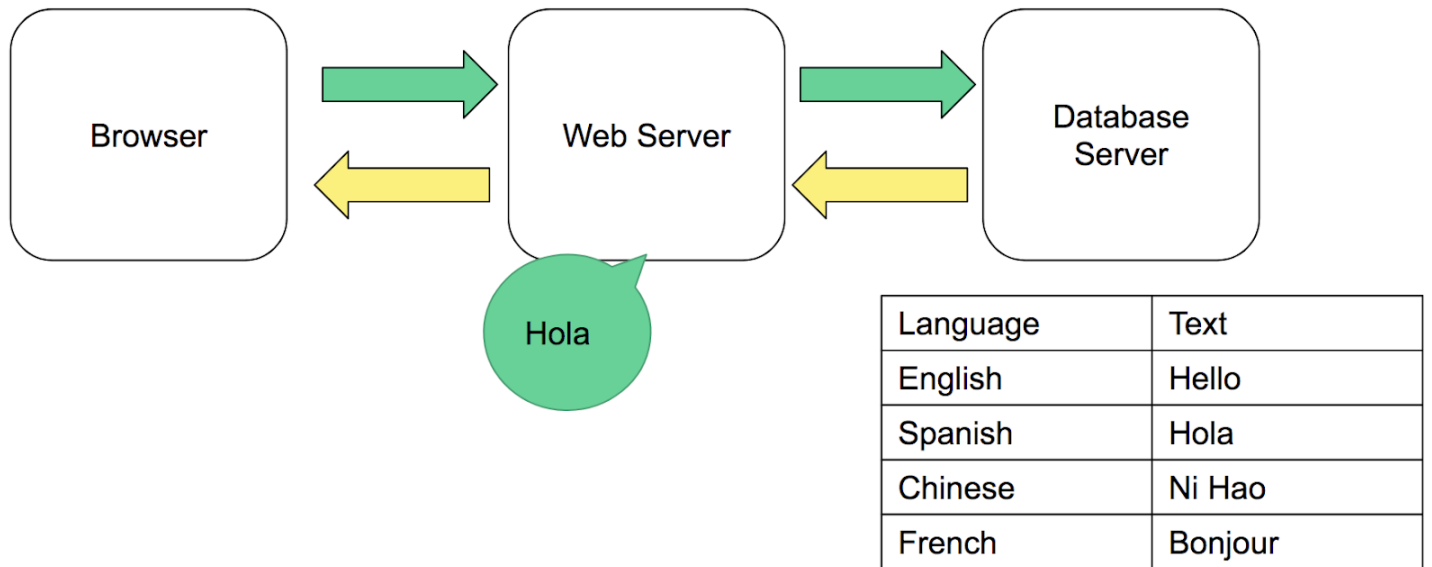
When you visit a website, there is a chain of actions that take place. The parties that are involved include Client machine, Router, and Server machine. We will just focus on the computers.

The Client machine is where the Client Application runs on. A web browser is a type of Client Application. A web browser talks to a web server, which then perform some actions.

Say there is a super simple website that says “Hello” when you visit the site. You visit that site in a web browser, which sends a request to a web server, which then return some data. The web browser then displays the “Hello” message on the web page.



For a little fancier website that says hello in different language, then it could look like the following. The web server then talks to a database server, which manages language data.



How Does Subscribed Music Streaming Work?

Review Vocabulary

- Account
- Authentication
- Online Identity
- What You Are Authentication
- What You Know Authentication
- What You Have Authentication
- Client Machine
- Server Machine
- Web Server
- Database Server

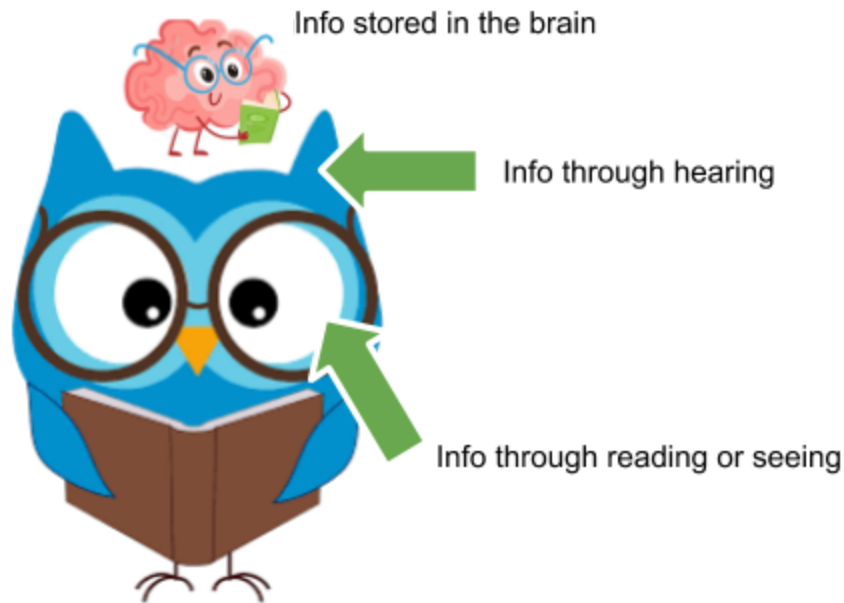
Day 4 Data Security

Has someone ever shared a secret with you and ask you “Not to tell”? What do you do with that information? Do you tell someone else? Do you add extra information to make it more interesting?



Online Data

A computer is like the human body, and it is a target for cyber attacks. To keep a computer healthy, one must protect its data. What is data? **Data is information** that can flow in and out of, or be stored at the computer. Think of data like a piece of information you learn. You can learn a piece of information through hearing, reading, or seeing. This information is then stored in your brain.



For a computer, the data could come in from the other computers, over the connection.

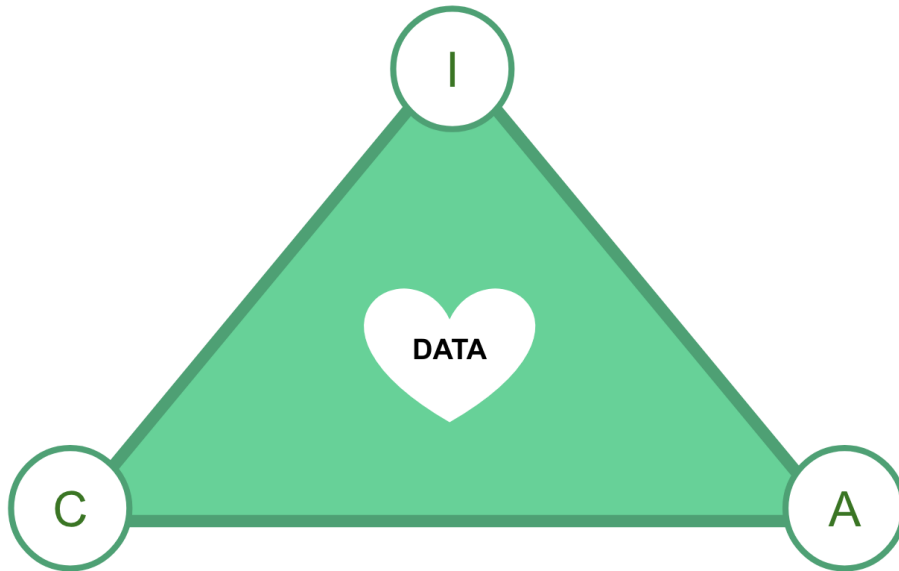
What does Data Security Mean?

Cybersecurity is about using technology to protect data in computer networks. What are the data in Cyberspace? They include information, identities (who you are), and assets (money, credits, or bitcoins). Some data is sensitive and needs to remain secret, and some data is not sensitive, and can be shared with the public.

Protecting the Data in Cyberspace is to protect three things about the DATA: Secrecy, Correctness, and Availability.

- Secrecy is the guarantee that my DATA is private and secret. It's also called **Confidentiality**
- Correctness is that my DATA is correct and not corrupted. It's also called **Integrity**.
- **Availability** is that I can access data when I want to.

Data is secured when all three areas of data are protected. It's like a triangle, and if any point breaks, then the triangle (data security) is broken.



How Data Security can be broken

Say you are sending an email or a chat message from your phone to your best friend's phone. You have something you want to share but you don't want anyone else to know. Your message is only SECURED when all legs are secured.

How can someone break the CONFIDENTIALITY point? It breaks when your private data is no longer private. Someone can break it by eavesdrop on the message exchange. Or take a sneak peek at the email or message stored on your phone or her phone.

How about INTEGRITY? INTEGRITY is the correctness of the DATA and it breaks when someone or some program corrupts the DATA. A corrupted email may contain incorrect information or worse, virus that could crash your friend's phone or computer.

The AVAILABILITY point breaks when you email is not available to your friend. This could happen if someone attacks the company that handles the email or chat message, such as SnapChat. Some hackers can bring down a company's computer network, so you are unable to use its service.

To protect the Cyber Security is to protect these three legs: CONFIDENTIALITY, INTEGRITY, and AVAILABILITY.

To Protect Data Security

Defense Against Secrecy:

What a user can do?

Pick a better password. More secure authentication method. HTTPS.

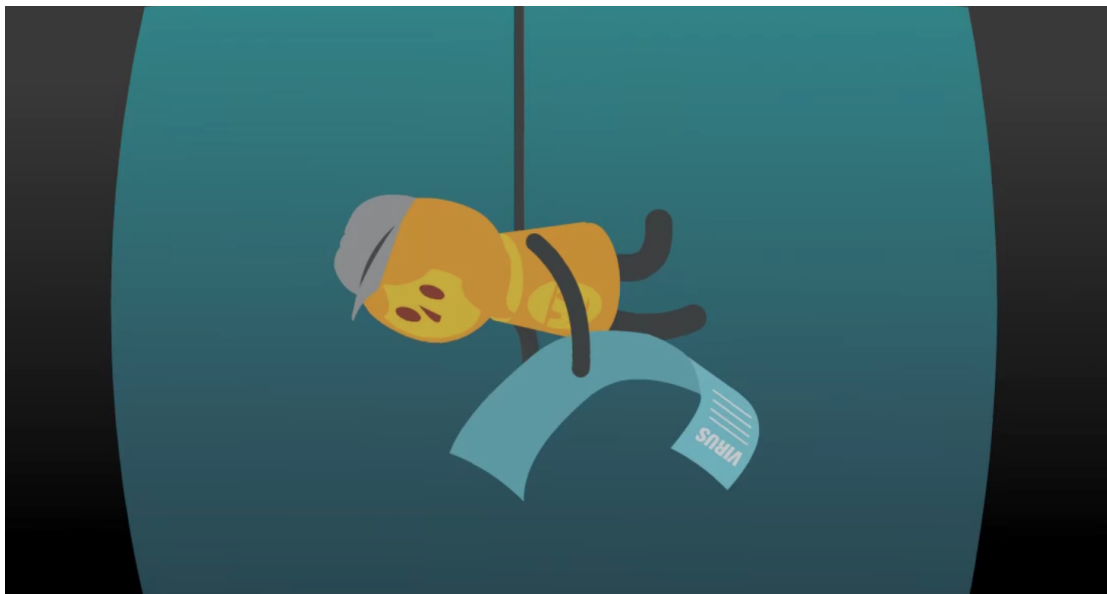
Correctness: Use checksum. Talk about message digest.

Defense Against Availability:

- The security measure is done at the server side.

Watch this video learn about hackers:

(<https://www.youtube.com/watch?v=DKzi5CYNFAg>)



Hackers are people who, with their technical knowledge, break into the computer system. Not all hackers are bad; some are White Hats, who help find vulnerabilities such as backdoors in the system. On the other hands, there are hackers with evil and selfish intentions, and they are called Black Hats.

Some hackers hack for amusement and curiosity, while Black Hats or cyber criminals hack most often for monetary gain. There are also **hacktivists**, who use their skills to promote a social or political goal.

We won't talk about how to become a hacker but we have learned attacks how hackers use to steal your accounts or break into a computer network. Today we will look at more advanced attacks called Network Attacks and the defense to each of them.

Computer Network Model

Build a Computer Network model with empty water bottles.

Idea:

Packets/Request

Marbles

Water

Perla beads

Connection

Use Large Boba Straw as pipe.
water pipe

Build a Computer Network

EAVESDROP ATTACKS - Unsecured Interfaces

The INTERFACES of a machine are where it sends out and receives message, like the slot of a mailbox. You can send and receive mails from the opening of a mailbox, but a thief can also steal your mails through the same opening. Such opening is called an INTERFACE.



Do you know that each device that you use to connect to the Internet is potentially a security hole where virus or malware can come in? Moreover, a device can also be used to hack into a home or a system. For example, some hackers could eavesdrop on the INTERFACE of a device, steal its username and password of ACCOUNTs, and fake the IDENTITY of an user.



Another way that a cybercriminal can get your personal information is by eavesdropping. That means they listen in to our devices through the INTERFACES. One example is your Wifi network interface. When using Wifi, pay attention to what Wifi network you connect. If it's an unsecure network, then someone could eavesdrop on your chat or even steal your password.

Defense Against Eavesdrop Attack: Encryption

To defend against the eavesdrop attack, connect only to secure Wifi networks that ask for password before connecting and also encrypt the connection.

To encrypt the connection means to change the original message before sending, and then change the altered message back to the original version at the receiver.

To illustrate how encryption works, let's use an example of you sending a secret message to your friend sitting across the room from you. You need to pass this letter across the room to her, and you don't want anyone reading it guessing what you wrote. But you want her to read your message. To do that, you and your friend can decide on an encoding/decoding mechanism.

Each character, such as "H" in "Hello", can be represented in a unique number, as shown in the table below.

Character	Value	Character	Value
A	65	N	78
B	66	O	79
C	67	P	80
D	68	Q	81
E	69	R	82
F	70	S	83
G	71	T	84
H	72	U	85
I	73	V	86
J	74	W	87
K	75	X	88
L	76	Y	89
M	77	Z	90

One simple way to encode is to add something to that number. Let's look at an example.

To send a secret message that says A-T-T-A-C-K, which each character is represented as a number:

Character	Number
A	65
T	84
T	84
A	65
C	67
K	75

To encode, let's add 3 to each character:

Character	Number	Encoded Number
A	65	$65 + 3 = \mathbf{68}$
T	84	$84 + 3 = \mathbf{91}$
T	84	$84 + 3 = \mathbf{91}$
A	65	$65 + 3 = \mathbf{68}$
C	67	$67 + 3 = \mathbf{70}$
K	75	$75 + 3 = \mathbf{78}$

If to encode is to add 3, how do you decode a message?

Encoded Number	Decoded Number	Character
75	$75 - 3 = \mathbf{72}$	H
72	$72 - 3 = \mathbf{69}$	E
79	$79 - 3 = \mathbf{76}$	L
79	$79 - 3 = \mathbf{76}$	L
78	$78 - 3 = \mathbf{75}$	O

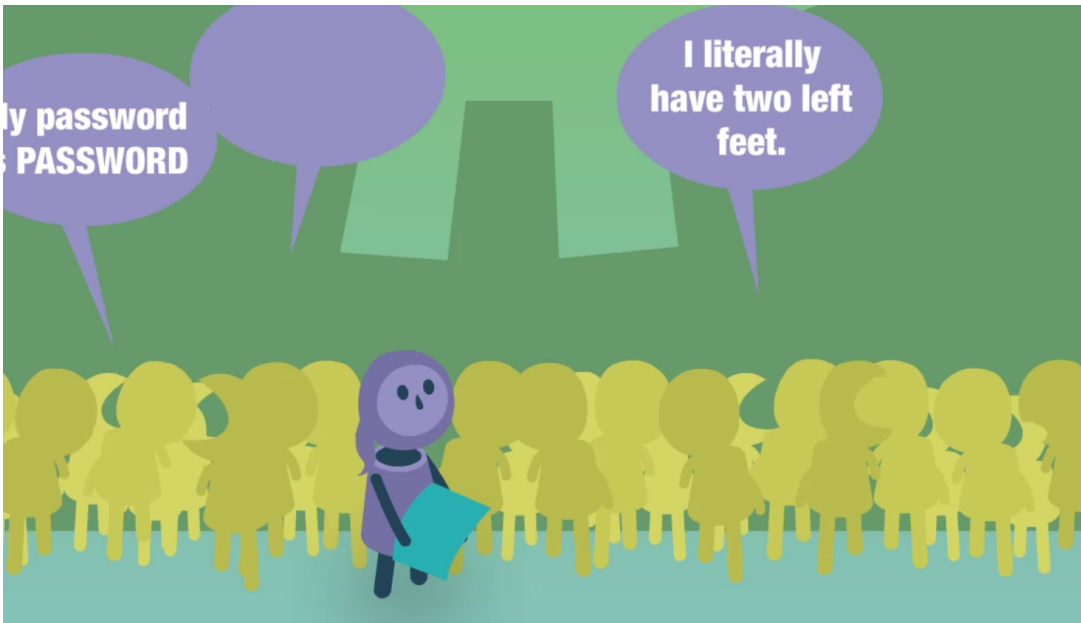
[Advanced]

WPA stands for Wi-Fi Protected Access and it keeps Wi-Fi connection safe. The most popular WPA version is WPA2. The latest and more secure WPA3 just came out this year.

Cyber Codes

[Video]

Watch this video to learn how to defend against EAVESDROPPING ATTACK by using Codes



(https://www.youtube.com/watch?v=q6FanLhvsEs&index=2&list=PLz1_3ursPgRR3kimKo-mA6obx75i4obGj)


When you send a message to someone else, you use an **INTERFACE** to connect your device so that it can connect to other devices that connect you to someone else or to a **SERVER** where your **DATA** is stored.

ENCRYPTION uses secret codes to keep the messages that you send and receive secret. **ENCRYPTION** is a **DEFENSE** against the **EAVESDROPPING ATTACK**.

CRYPTOGRAPHY is the art and science of secret codes. Cryptographers use math to create secret codes so that eavesdroppers can't read your message.

[Exercise]

Look at URL and look at the browser. Show https. Some browser has a lock. Look for https and lock before you send DATA. If the address bar shows a lock, as the image below, that means that site provides SECURE CONNECTION.

 Secure | <https://www.youtube.com/watch?v=q6FanLhvsEs&index=2&>

[Exercise]

Create your secret code. (Example: Advancing all the letters by 3).

[Discussion]

What is a good code. What is bad code? (Answers: Good codes are hard to crack, and bad codes are)

DENIAL OF SERVICE ATTACK (DoS)

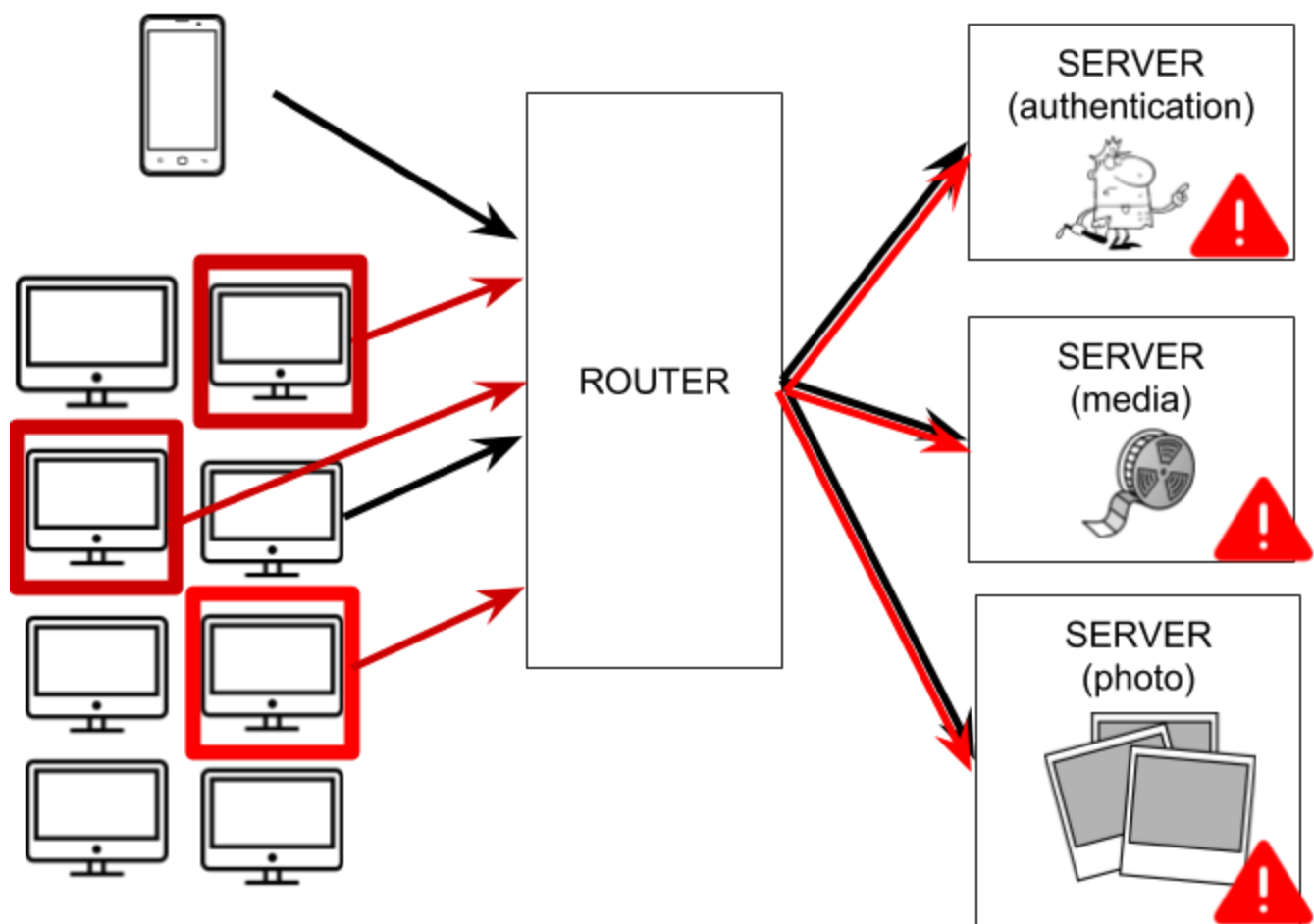
The Denial of Service Attack is when hackers send a lot of fake requests to a Computer System that it is unable to process the real request.



Have you heard of prank calls? Prank calls are people who make so many fake calls to the police station or fire station so the first responders are swamped with fake incidences and cannot help the people who truly need help. This is a form of Denial of Service Attack.

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.



An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS)

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

The Distributed DoS or DDoS is a large-scale and coordinated attack that the fake requests are generated from multiple locations. It's much harder to fight.

BotNet and Distributed Denial of Service Attack

How do hackers manage to perform DDoS attack from many locations and not get caught? They do it often through a Botnet or Zombie Net. A Botnet is a large number of computers infected and used together to send malicious emails, mine bitcoins, or perform DDoS attack. A Zombienet is a type of Botnet, that its infected hosts are working normally until the attack start.

When attacking, all the computers in the botnet send a flood of dummy message. Such DDoS can knock services offline and bring down the network of a large company or many companies.

What CAN we do to prevent DDoS? The computer owner often do not know that their devices have been infected, participating in crimes and sometimes even in crimes that involve random. We can help by protect our own computers and prevent them from being infected by virus and turned into an accomplice in crime against Cyberspace!

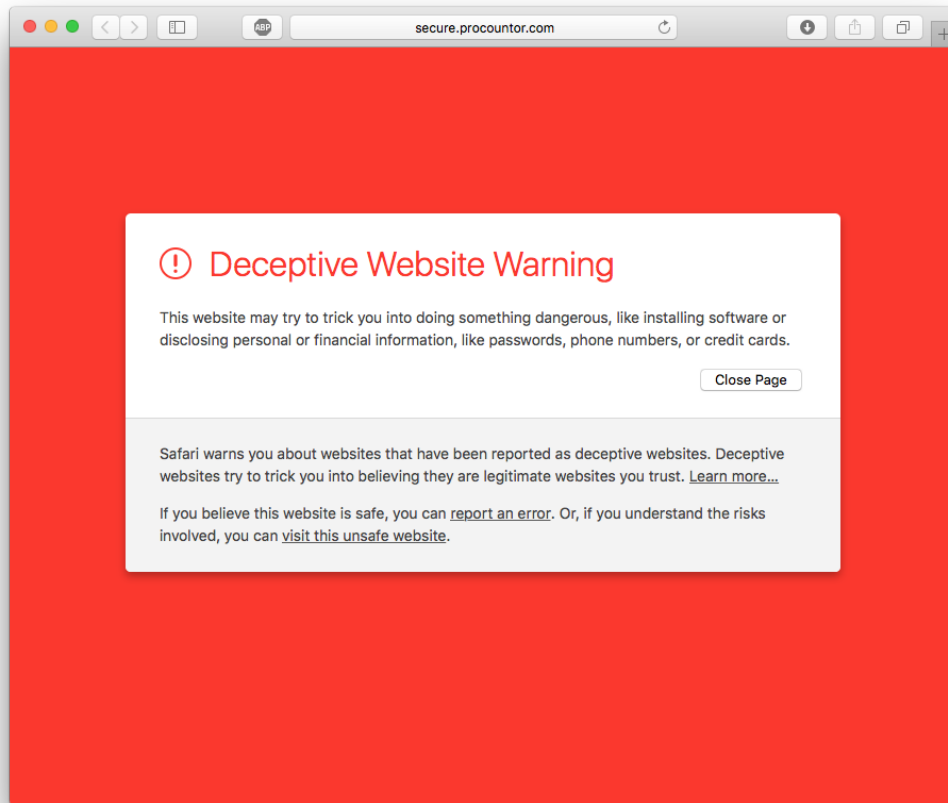
DEFENSE Against Denial-of-Service Attacks from Individual User

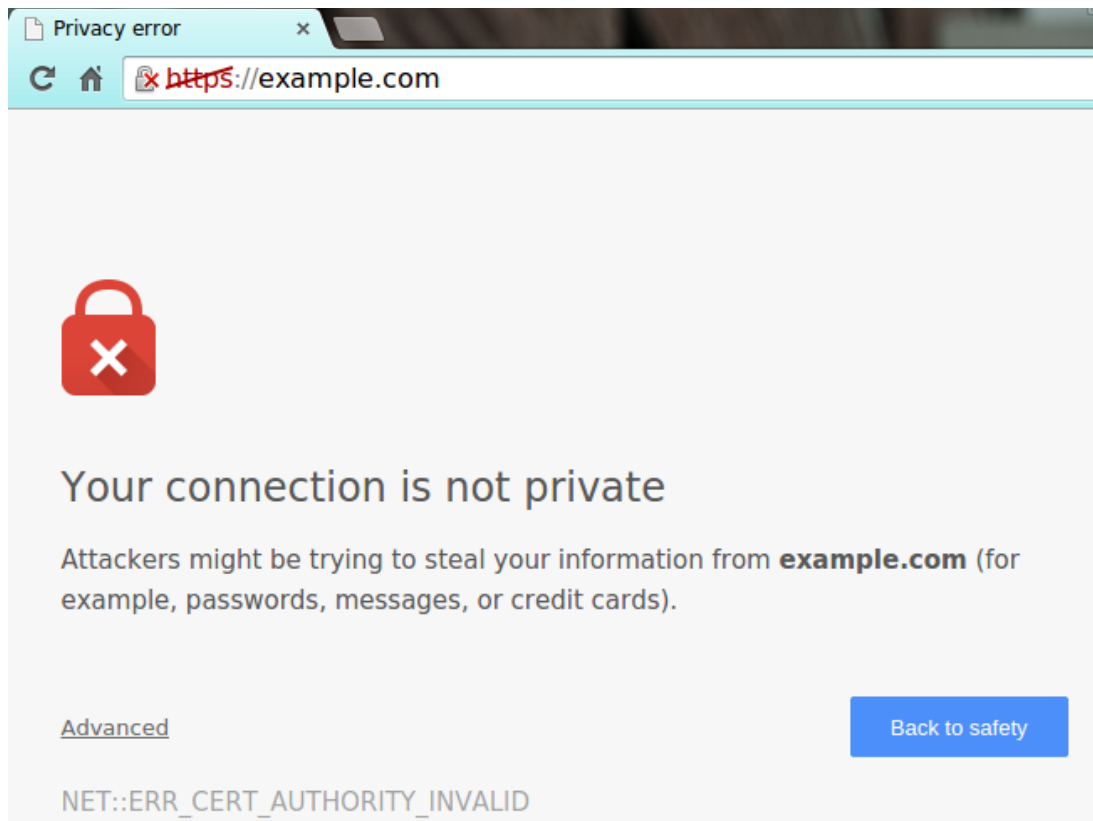
What CAN we do to prevent DDoS? We can help by protect our own computers and prevent them from being infected by virus and turned into a bot in the botnet.

These are some steps YOU can take to prevent entering the dark side:

Install and maintain anti-virus software

Don't visit suspicious sites





- Turn off your machine when not using.

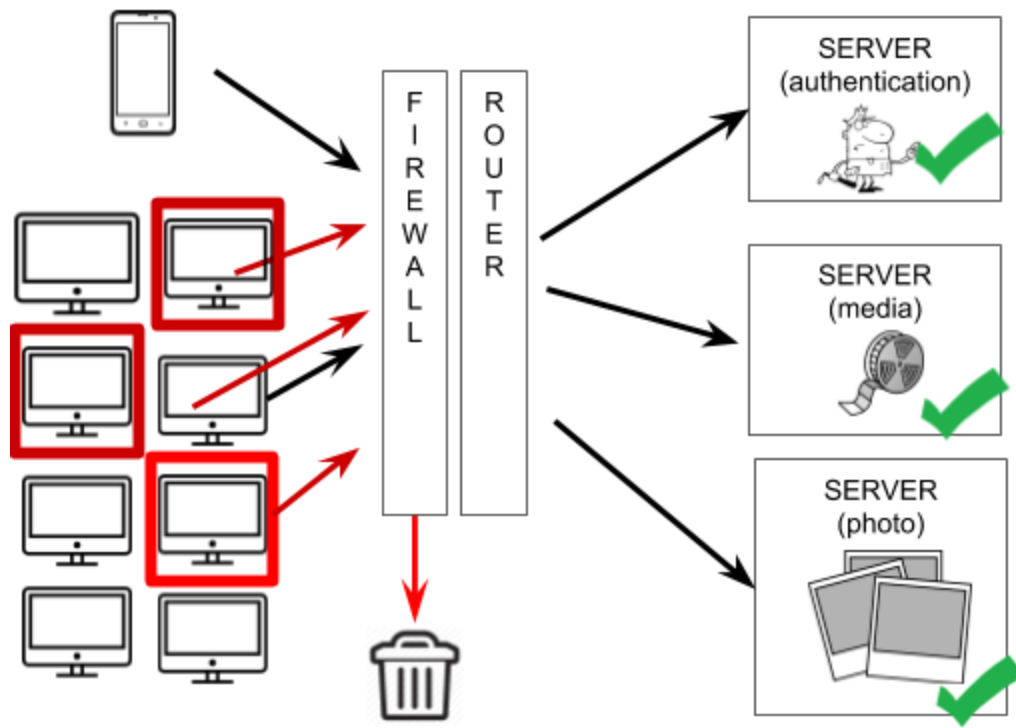
[Advanced]

- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address (see Reducing Spam for more information). Applying email filters may help you manage unwanted traffic.

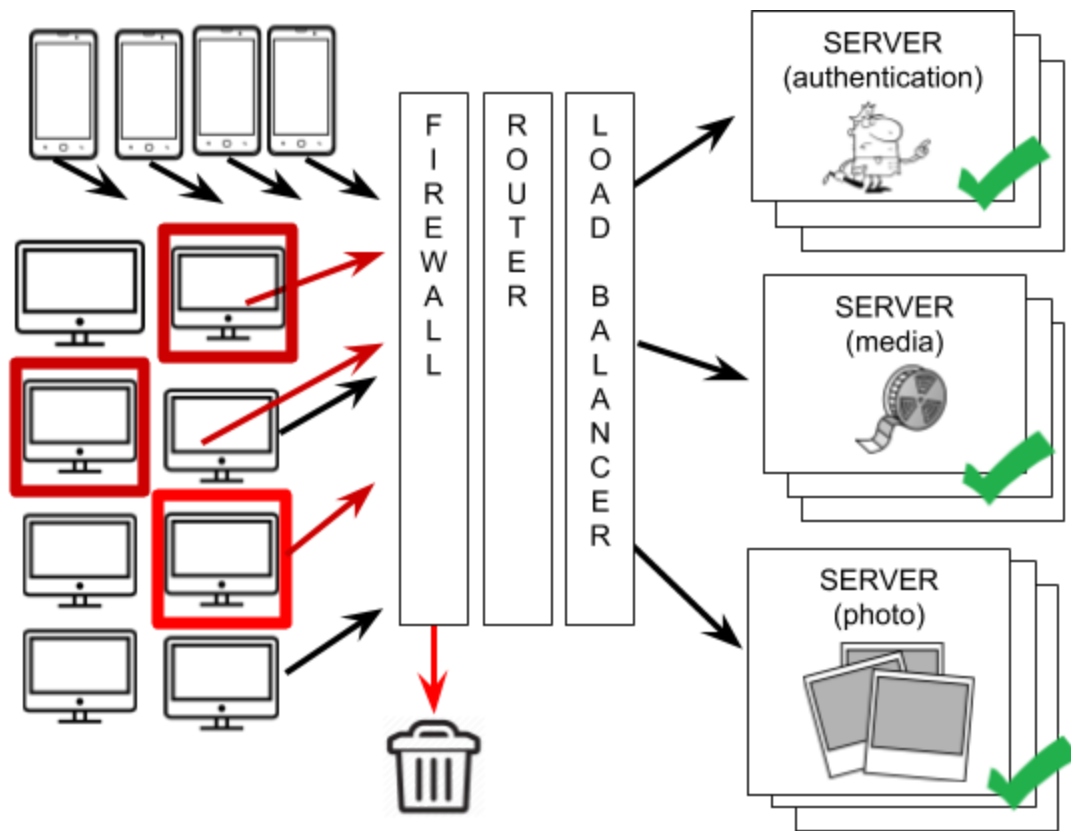
DEFENSE Against Denial-of-Service Attacks from a Company - Advanced

Use Firewall to filter out bad traffic:

If you are a company owner or an engineer who needs to protect your Computer Network against DDoS,



DEFENSE Against Denial-of-Service Attacks and Gate Rush



Internet-of-Things Devices

[Video]

Watch a 13-year old security expert shows that he can hack into people's computer using a mini machine hidden inside a teddy bear.

Example of hacking a teddy bear (YouTube video)

https://www.youtube.com/watch?v=8z3XuRQ3-bl&index=30&list=PLz1_3ursPgRR3kimKo-mA6obx75i4obGj



Exercise: Identify the THREAT and the ATTACK. What interface on the Teddy bear did 13-year old security expert use to demonstrate an EAVESDROPPING attack?

References:

For Parents:

<https://staysafeonline.org/>

For Future Cybersecurity Experts

https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7dint.html

<https://www.dhs.gov/topic/cybersecurity>

<https://csrc.nist.gov/>

https://www.youtube.com/watch?v=bPVaOIJ6ln0&list=PLz1_3ursPgRR3kimKo-mA6obx75i4obGj&index=7

Understanding Denial-of-Service Attacks

<https://www.us-cert.gov/ncas/tips/ST04-015>

Understanding Anti-Virus Software

<https://www.us-cert.gov/ncas/tips/ST04-005>

Understanding Firewall

<https://www.us-cert.gov/ncas/tips/ST04-004>

Understand Rootkit and Botnet

<https://www.us-cert.gov/ncas/tips/ST06-001>

Avoid Social Engineering Attacks

<https://www.us-cert.gov/ncas/tips/ST04-014>

Protecting Your Privacy

<https://www.us-cert.gov/ncas/tips/ST04-013>

Staying Safe on Social Network

<https://www.us-cert.gov/ncas/tips/ST06-003>

Choosing and Protecting Password

<https://www.us-cert.gov/ncas/tips/ST04-002>

Botnet

<https://www.technologyreview.com/s/610056/a-fast-evolving-new-botnet-could-take-gadgets-in-your-home-to-the-dark-side/>

Hacker News

<https://thehackernews.com/>

Mirai (Future) Botnet

<https://thehackernews.com/2017/12/hacker-ddos-mirai-botnet.html>

Carnegie Mellon's Data Classification Guideline

<https://www.cmu.edu/iso/governance/guidelines/data-classification.html>

Common Cyber Attacks

<https://www.rapid7.com/fundamentals/types-of-attacks/>

[Extra] How can someone guess your password?

If you use the face of a coin to be your password, then there are two possible passwords:

Head

Tail

There is $\frac{1}{2}$ chance you can guess it right the first time.

What about two coins.

There are four possible ways the coin toss could turn out.

Head Head

Head Tail

Tail Tail

Tail Head

So there is $\frac{1}{4}$ chance you can guess it right the first time.

Let's use the face of a dice to be your password. There are six possible passwords:

One

Two

Three

Four

Five

Six

If you use the combination of two dices to be your password

If your password can only be one of the numbers 0,1,2,3,4,5,6,7,8,9, how many guesses would it take, at most, to guess your password? (Answer: 10) How many guesses would it take, in the least, to guess your password? (Answer: 1) What are the odds of guessing your password on the first try? (Answer: 1 in 10).

Now your password must have four numbers instead of one. How many guesses would it take, at most, to guess your password? (A: 10000) How many guesses would it take, in the least, to guess your password? (Answer: 1) What are the odds of guessing your password on the first try? (Answer: 1 in 10000)

Which password is harder to guess? Many DEFENSES work like this. A cybercriminal may still have a chance to guess your password. When you are cybersmart, you make it very hard for the cybercriminal to get lucky. Cybersmart people make their luck.

[Extra] A Computer Network Under Attack

A Computer Network is

Client ==> Connecting Parts =====> Server

Client <==== Connecting Parts <===== Server

A Client computer is used by an user. It includes a phone, a tablet, a laptop, or anything connected to the Internet and can send request to the Server.

A Server computer is a powerful computer that provide one or more services. A server can also work with the other servers to provide a service.

What does it mean when a computer is under attack? A computer can be infected with virus or malware. Someone can log into a computer via backdoor, meaning not from the normal login, but by sending an Operating System command, fooling it into thinking that it is an legitimate user.

A computer's data can also be stolen either by someone physically removes the hard disk or hacks into a computer and transfer the data out of it.

A computer's camera can also be hacked so that it turns on and start filming. A computer's microphone can be hacked into as well.

To keep a computer safe, think about securing these interfaces

- WiFi
- Bluetooth
- Camera
- Microphone
- Operating System
- Disk