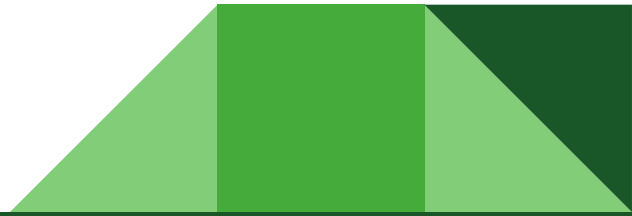
Cybersecurity

The Problem

Because of the way the Internet is built, *all* information is sent over **shared wires**.

Information like Credit Cards, Passwords, emails, Social Security Numbers…

If this information isn't protected somehow, it could be read by ***CYBERCRIMINALS***.



Cybercrime & Cyberwarfare

Cybercrime and Cyberwarfare are serious threats that have some devastating effects on the world around us.

Cybercrime has to do with attacks against **individuals**, where Cyberwarfare has to do with attacks as a military tactic, at a national level.

Cybercrime & Cyberwarfare

Cybercrime and Cyberwarfare are serious threats that have some devastating effects on the world around us.

Cybercrime:

- Identity theft
- Stealing money
- Stealing private information
- Controlling private computers

Cybercrime & Cyberwarfare

Cybercrime and Cyberwarfare are serious threats that have some devastating effects on the world around us.

Cyberwarfare:

- Hacking into government computer systems
  - Control things like communication, transportation, water, energy production
  - Interfere with elections

Cybercrime Example - DDoS Attack

DDoS stands for **D**istributed **D**enial **o**f **S**ervice, and it involves spamming a web server with so many requests so close together that it crashes.

Sometimes, servers might spit out some valuable information when they crash!

Other times, these attacks are performed just to spite an individual or company.

It's called a Denial of Service attack because the website being attacked is made unavailable, since its server has crashed. It's Distributed because the attack is coming from a large number of distinct devices, oftentimes computers that have been hijacked by a hacker.

Cybercrime Example - DNS Spoofing

If a ***cybercriminal*** pretends to be a DNS name resolver, they can feed computers incorrect IP Addresses for websites!

If they can get you to visit this false site, they can install malware, scrape your personal data, or any number of other bad things!

The Solution: Cybersecurity

There are several different things that go into Cybersecurity.

The Solution: Cybersecurity

There are several different things that go into Cybersecurity.

- Protocols for encrypting/decrypting data
  - Ensures that messages can't be read if they're intercepted

The Solution: Cybersecurity

There are several different things that go into Cybersecurity.

- Protocols for encrypting/decrypting data
  - Ensures that messages can't be read if they're intercepted
- Security Software
  - Programs designed to help your computer defend itself from cyberattacks

The Solution: Cybersecurity

There are several different things that go into Cybersecurity.

- Protocols for encrypting/decrypting data
  - Ensures that messages can't be read if they're intercepted
- Security Software
  - Programs designed to help your computer defend itself from cyberattacks
- Following Best Practices
  - Most cybersecurity breaches occur due to **human** error, rather than software bugs!

The Solution: Cybersecurity

One of the biggest contributors to this equation is **encryption**.

- Protocols for encrypting/decrypting data
  - Ensures that messages can't be read if they're intercepted
- Security Software
  - Programs designed to help your computer defend itself from cyberattacks
- Following Best Practices
  - Most cybersecurity breaches occur due to **human** error, rather than software bugs!

Encryption of Data

If our data is encrypted, it is much more difficult for hackers to learn what information was being sent if they intercept it!

To this end, there are open standards for encryption of information across the Internet, so that all computers understand how data should be encrypted/decrypted when sent!

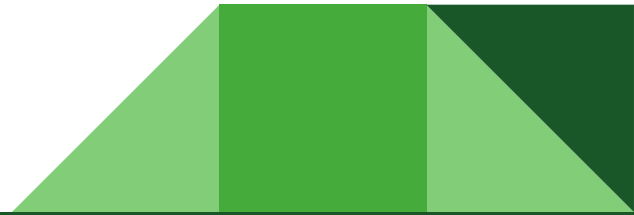
The protocol used across the Internet today is SSL/TLS - that stands for **S**ecure **S**ockets **L**ayer and **T**ransport **L**ayer **S**ecurity.

Encryption of Data

The protocol used across the Internet today is SSL/TLS - that stands for **S**ecure **S**ockets **L**ayer and **T**ransport **L**ayer **S**ecurity.

When we encrypt our data before it's sent, we're no longer sending simple HTTP requests over the Internet - we're scrambling them up beforehand, so that their contents are unreadable!

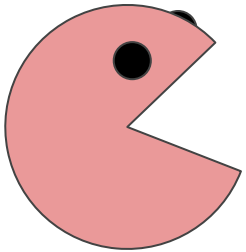
You can tell when you're using secure communication when you see an **s** after the http portion of your URL - **https**://www.example.com



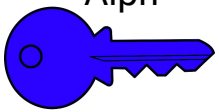
SSL/TLS - Public Key Encryption

SSL/TLS ensure that messages being sent across the Internet are following the Public Key Encryption method!

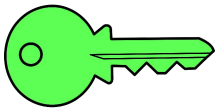
The **Public Key** *encrypts* information
The **Private Key** *decrypts* information



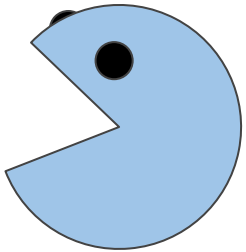
Alph



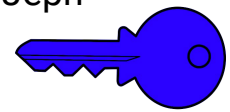
Alph's **Public** Key

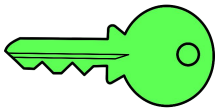


Alph's **Private** Key



Jeph

Jeph's **Public** Key 

Jeph's **Private** Key 

Certificate Authorities (CAs)

Certificate Authorities verify the public keys of the websites you use.

When we get the public key from a website, we'll check it against what a CA says, to confirm that we got the correct one! This way, if a hacker managed to intercept our transmission and send us a bad key, our computer won't send any messages using that key.

Security Software

Sometimes, we might accidentally download a program that someone malicious wrote to try and steal our information or do something else bad with our computer. These programs are called **viruses** or **malware**.

To combat this, we can install **anti-virus** software, which is designed to detect and delete these malicious programs.

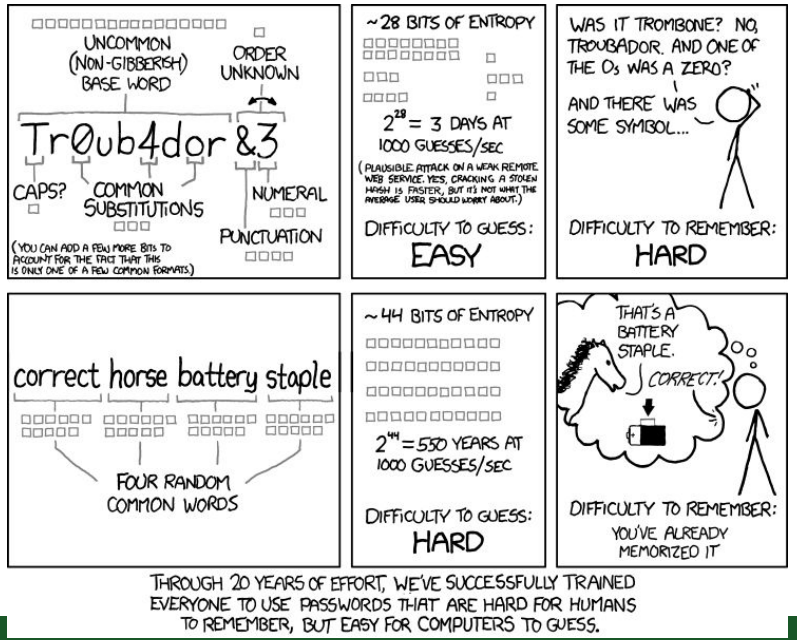
Following Good Practices

In addition to these other ways our information is protected on the Internet, there are all kinds of things that we can do to keep ourselves safe!

Following Good Practices

In addition to these other ways our information is protected on the Internet, there are all kinds of things that we can do to keep ourselves safe!

- Use strong passwords



Comic Credit: https://xkcd.com/936/

Following Good Practices

In addition to these other ways our information is protected on the Internet, there are all kinds of things that we can do to keep ourselves safe!

- Use strong passwords
- Don't use repeated passwords between websites
  - If a website gets hacked, your password could be leaked. If you use the same password in multiple locations, a hacker could gain access to any number of different accounts!
  - Password Managers are a great tool to solve both of these problems - you can have them generate a unique, strong password for each website that you visit, and you'll only need to remember **one** password to be able to access them all!

Following Good Practices

In addition to these other ways our information is protected on the Internet, there are all kinds of things that we can do to keep ourselves safe!

- Use strong passwords
- Don't use repeated passwords between websites
- Install security updates!
    - These often fix vital security breaches within your software - it's important that you don't keep clicking "Remind Later" over and over again!

Following Good Practices

In addition to these other ways our information is protected on the Internet, there are all kinds of things that we can do to keep ourselves safe!

- Use strong passwords
- Don't use repeated passwords between websites
- Install security updates!
- Think twice before clicking on suspicious links or downloading fishy programs
  - Don't click on links within emails from people you don't know
  - Don't visit websites when your browser warns you not to
  - Don't download files when your browser warns you not to

Phishing

One of the largest holes in our Internet security is often us!

Attacks against the user of the Internet are called Phishing, and there's all kinds of different attacks that can be carried out.

- People posing as someone you know in an email, asking you to click a link
- Websites posing as other websites, asking you to put in your email and password
- Voice calls asking you to call a number or visit a specific website