Cyber Security Awareness

A presentation by Steven Christopher Wong

Purpose of Presentation

The objective of this presentation is to show various cybersecurity threats and resources in order to mitigate or reduce its occurrence in society.

The purpose of this presentation is to show you resources on how to train in order defend yourself in cyberspace.

Resources will be presented on how to pursue a career in cyberspace and access to free software that will protect you from these attacks.

Purpose of Presentation

The objective of this presentation is to show various cybersecurity threats and resources in order to mitigate or reduce its occurrence in society.

The purpose of this presentation is to show you resources on how to train in order defend yourself in cyberspace.

Resources will be presented on how to pursue a career in cyberspace and access to free software that will protect you from these attacks.

Ideas

It is a good idea to incorporate the young in the fight for cyber security.
Cyber-security is security it means defending yourself in cyberspace and educating others about the topic.
Eliminating ignorance about illegal activity online will help reduce these types of attacks by establishing an awareness.
An ounce of avoidance is a pound of cure.

Cybersecurity mOtivational speech For HIgh School students (Click image to access video)

HONEY POT

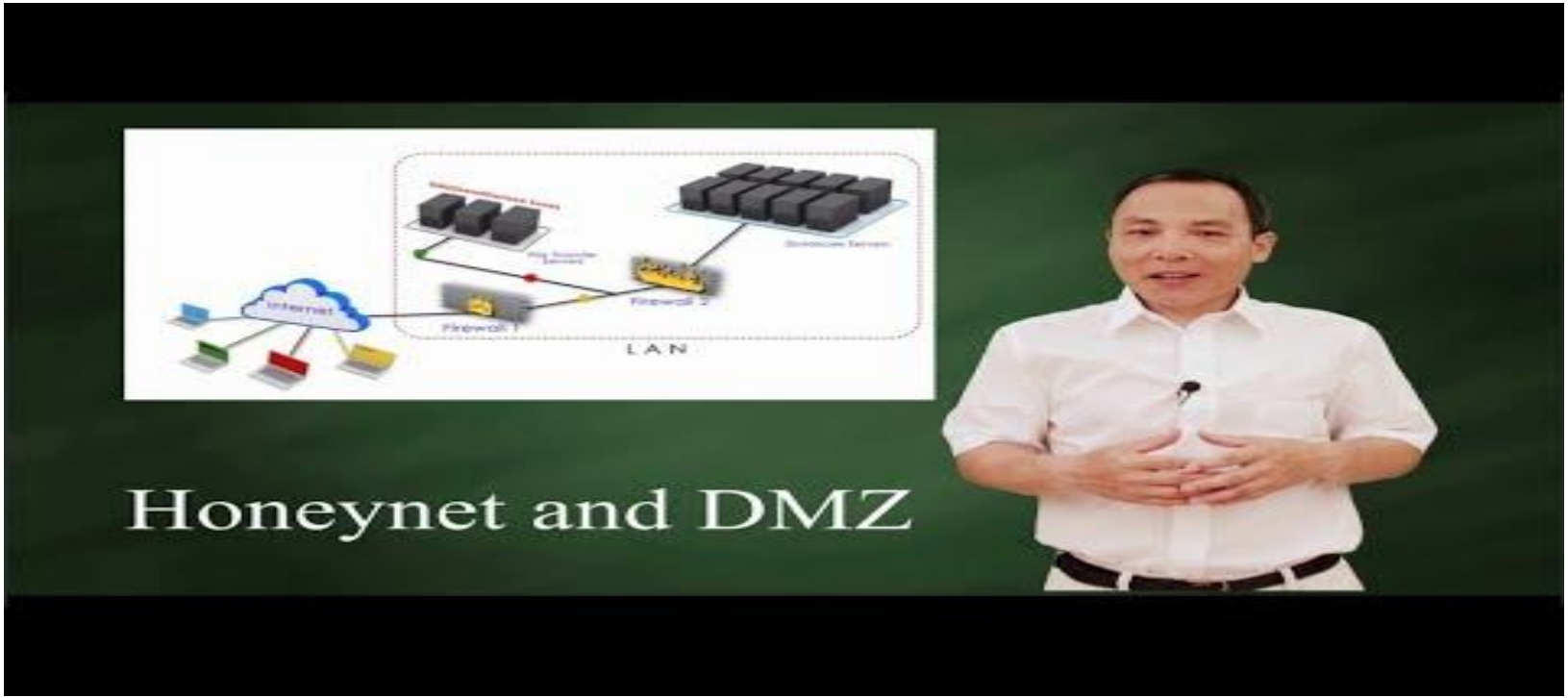
- A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate.

How do honeypots work?

If you, for instance, were in charge of IT security for a bank, you might set up a honeypot system that, to outsiders, looks like the bank's network. The same goes for those in charge of — or researching — other types of secure, internet-connected systems.

By monitoring traffic to such systems, you can better understand where cybercriminals are coming from, how they operate, and what they want. More importantly, you can determine which security measures you have in place are working — and which ones may need improvement. Please click the image for a honey pot video

HoneyNet



Security Operations Center

It is important to create a security operations center for local businesses to communicate network attacks to government and to be compliant with laws rules and international regulations when handling government, business, and patient information.

SIEM

Their must be another department that deals with anomalous activities online.

Please watch video it deals with ethics.

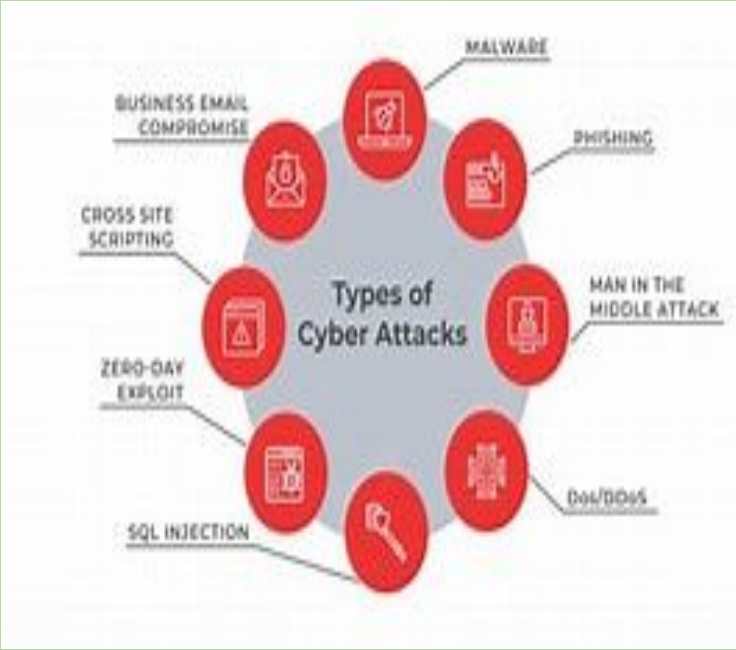
What is cybersecurity and why should we be aware of threats in cyberspace?

Cyber security definition

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Types of Cyber attacks

- Business email compromise
- Malware
- Phishing
- Man in the Middle Attack
- Denial of Service/ Distributed Denial of Service
- SQL Injection
- Zero-Day Exploit
- Cross Site Scripting



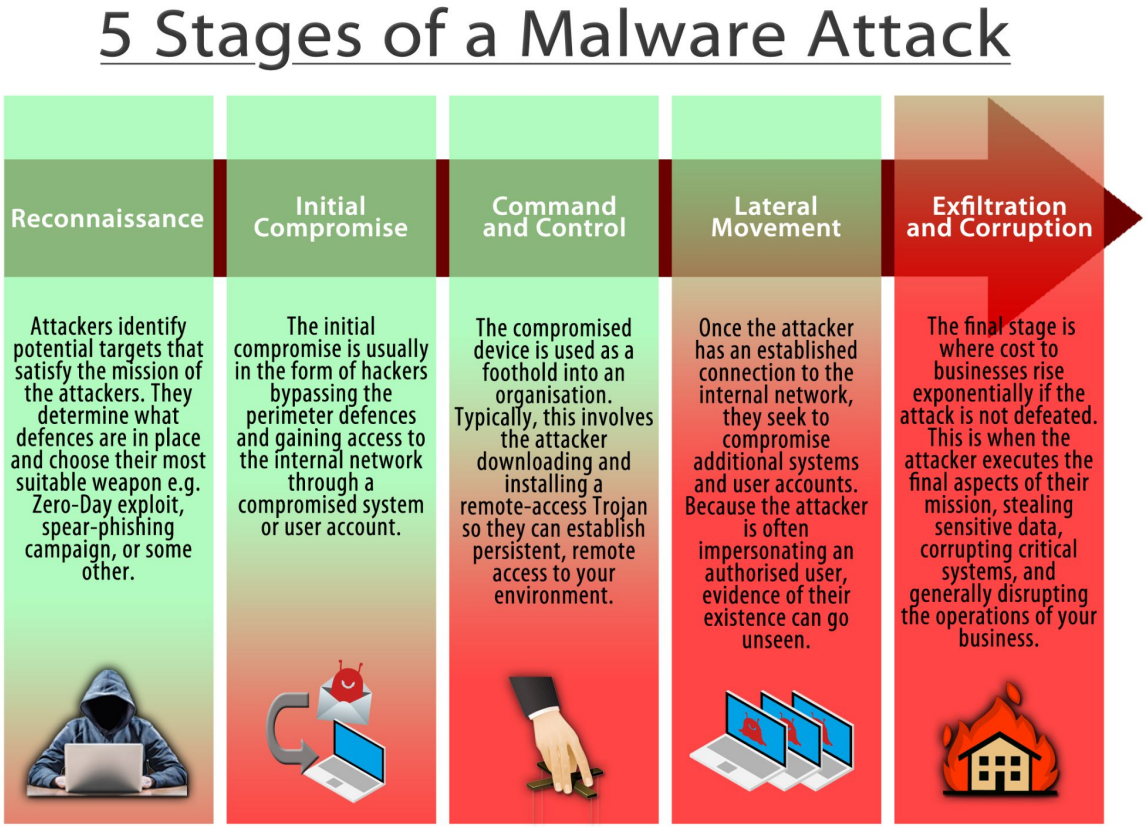
Business Email Compromise

Business Email Compromise (BEC) is a cyberattack involving the hacking, spoofing, or impersonation of a business email address. The victim of a BEC attack receives an email that appears to come from a trusted business. The email looks and feels genuine. But it typically contains a phishing link, a malicious attachment, or a request to transfer money to the attacker.


BUSINESS EMAIL
COMPROMISE
A New Age of Deepfake Crime

Malware Attack

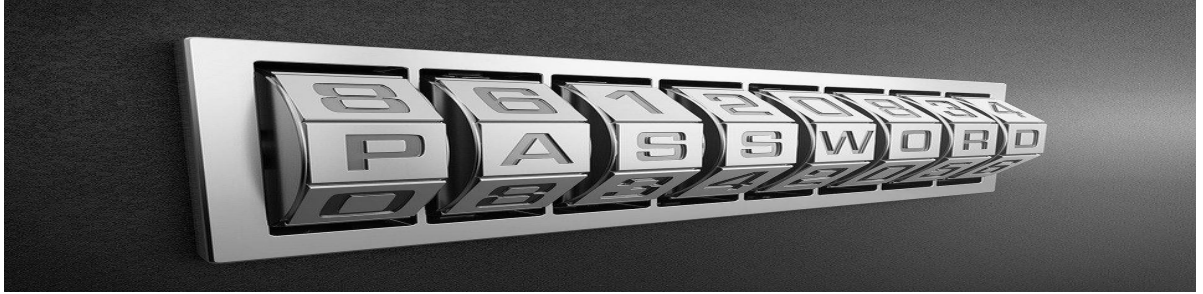
A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software (a.k.a. virus) encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.



Malware Bytes: a free software that finds and deletes Malware

www.malwarebytes.com

Password Protection



Passwords are the keys to your advanced life. Ensure they are no less than 10 characters in length - including letters, numbers and images to make them harder to break.

Try not to record passwords. Think about utilizing a solid secret phrase director. Additionally utilize two-factor validation - either an actual security key or an application conveying time sensitive one-time passwords, as Authy or Google Authenticator.

Try not to impart passwords to companions. It's equivalent to giving them the keys to your home or your vehicle - in addition to the ability to see all that you've done and even imitate you on the web. For similar reasons, don't save usernames and passwords on shared PCs, and consistently log out when you're done utilizing another person's gadget.

One more key method for ensuring your information is to back it up consistently to an outside hard drive or a distributed storage framework.

Mobile Safety

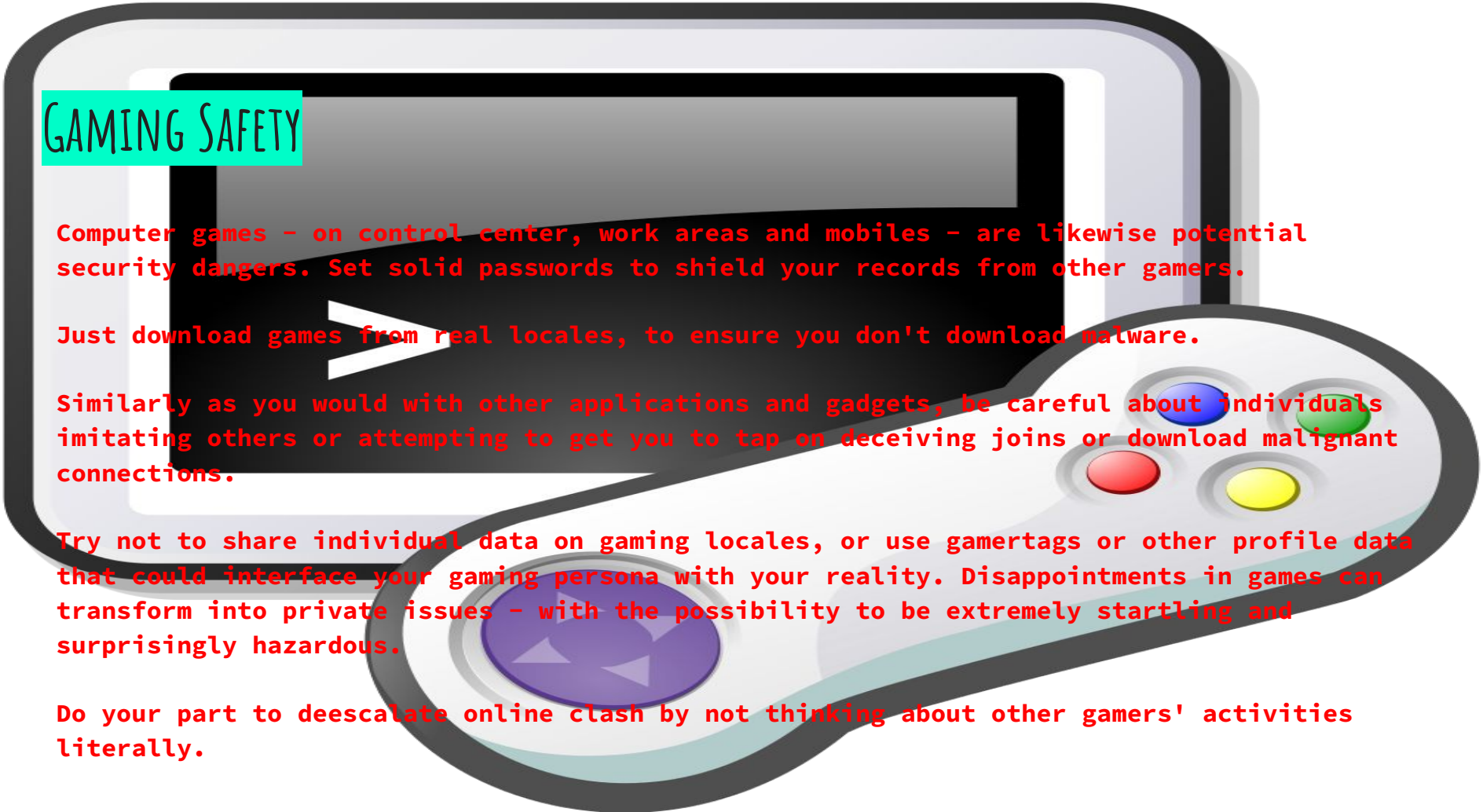
The most ideal way to secure your cell phone is to know where it is consistently. Additionally, set a secret phrase on it and be certain it's set up so you can remotely wipe it in the event that you truly do lose it.

Be extremely cautious while downloading applications. Regularly programmers will make applications that look a ton like a certifiable famous application however are rather malware that will take your own data.

Incapacitate Bluetooth on your gadgets except if you're effectively utilizing a Bluetooth association. Particularly out in the open spots, it frees your telephone up to being captured and having your information taken.

Keep away from open public Wi-Fi organizations. They can without much of a stretch be entered by programmers - or even set up and worked by information criminals - who can watch the traffic and see what you do on the web. Consider utilizing a virtual private organization, which encodes all that your gadget sends.

Gaming Safety



Computer games - on control center, work areas and mobiles - are likewise potential security dangers. Set solid passwords to shield your records from other gamers.

Just download games from real locales, to ensure you don't download malware.

Similarly as you would with other applications and gadgets, be careful about individuals imitating others or attempting to get you to tap on deceiving joins or download malignant connections.

Try not to share individual data on gaming locales, or use gamertags or other profile data that could interface your gaming persona with your reality. Disappointments in games can transform into private issues - with the possibility to be extremely startling and surprisingly hazardous.

Do your part to deescalate online clash by not thinking about other gamers' activities literally.

Social Media Safety

At the point when you're via web-based media, don't become friends with individuals you don't really know, all things considered.

To ensure your protection and to limit the advanced impressions future schools and bosses may find, don't post - or let companions post - humiliating pictures of yourself or some other sketchy material.

Know about cyberbullies and online stalkers. Limit the amount you uncover about your day by day schedules, propensities or ventures. Furthermore assuming you at any point feel awkward or undermined by somebody on the web, promptly quit speaking with that individual and alarm a capable grown-up, similar to a parent, instructor or school administrator.

How to start a career in cyber-Security

1. Don’t specialize just in security

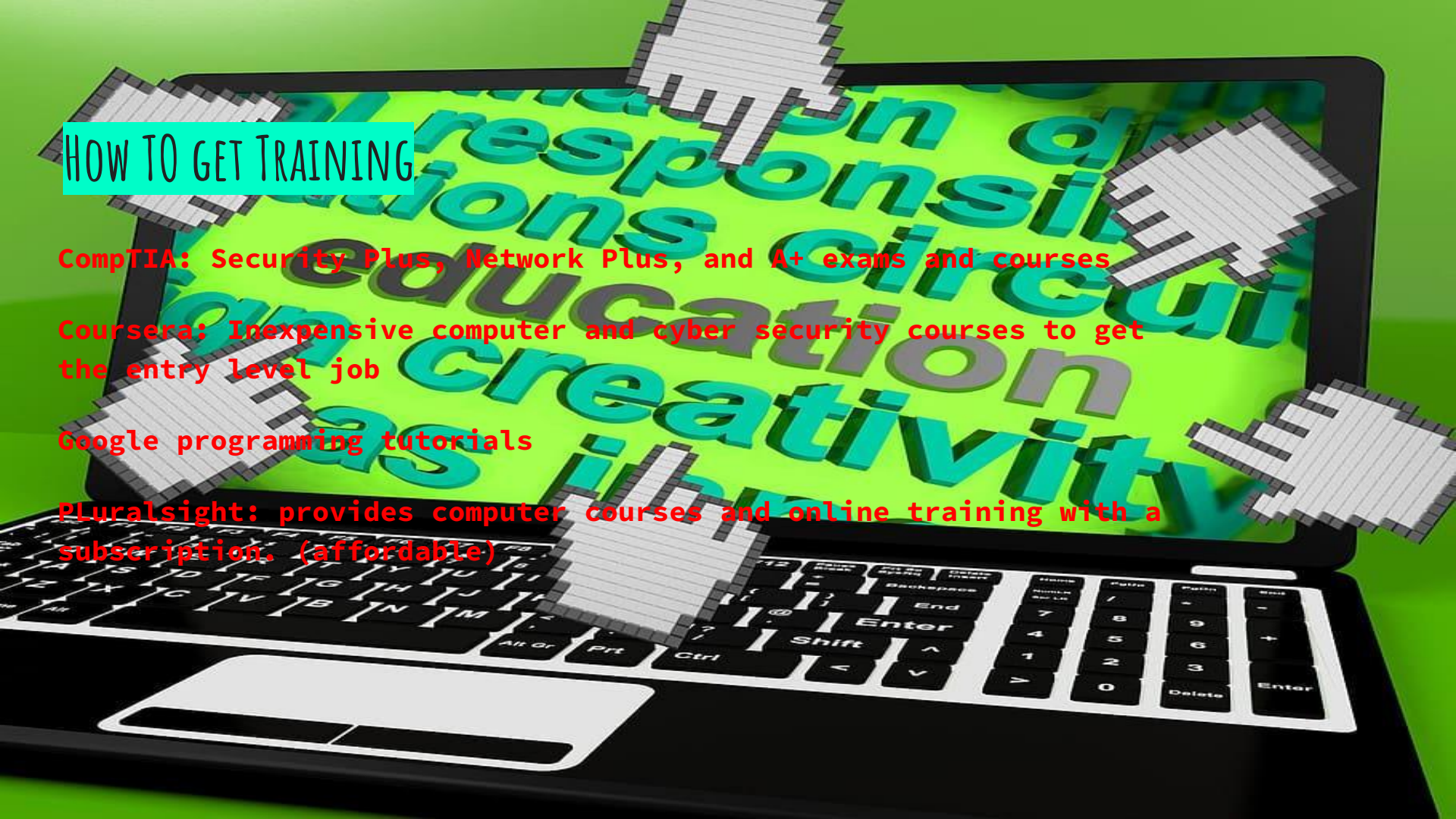
2. Sometimes it’s who you know--so network

3. Not in tech yet? Start by studying up on IT basics

4. Legitimize your skills by earning certifications

5. Show initiative in your own time

6. Hone your data analysis skills


How TO get Training
CompTIA: Security Plus, Network Plus, and A+ exams and courses
Coursera: Inexpensive computer and cyber security courses to get the entry level job
Google programming tutorials
Pluralsight: provides computer courses and online training with a subscription. (affordable)

Conclusion

The World is short staffed and desperately in need of smart people like you from Cottonwood High School.

Countless cyber-attacks happen everyday.

Start with internships at Department of Homeland Security and IBM or local credit card companies in the area like American express.

Cyber security analysts which is a beginner role starts off at $63,000 a year and can advance and make up to or over 100,000 a year.