# **Unit 4** Lesson 8: Rapid Research - Cybercrime

**Objectives:**

**Students will be able to:**

* Explain the characteristics of a phishing attack
* Explain how a DDoS attack works
* Describe how one computer virus works
* Research and describe a cyber attack found in the news
* Reason about the threats posed by, and methods of recourse for, various types of cyber attacks

In this brief lesson you will learn about various types of cyber attacks and cyber crimes and do a small amount of research to learn more about one. The lesson should cap off learning about encryption by taking a moment to look at the kinds of attacks and threats encryption (among other things) is intended to thwart. The lesson is intended to be a transition as well, to kick off a Practice Peformance Task that begins in the next lesson about Big Data and Security more generally

We are trying to kill two birds with one stone here: 1. review terminology about cyber security and crime that is relevant for the AP CS Principles Exam and 2. practice research skills - both finding credible sources quickly, and backing up what you say with evidence. This lesson is intended to serve as a wrap-up to the work we’ve done with encryption by taking a look at cybercrime that happens in the real world (and in which encryption plays a huge role). This lesson should not go very long despite the potentially interesting issues and avenues you could go down. The intent is that this is a quick-hit percursor to a larger Practice Performance Task that follows this lesson about cyber security and big data in general. Students may want to take some of the research here and use it as a starting point for the Practice PT but it is not required to get into that level of depth here.

The widget in the lesson mimics the RSA encryption algorithm (with smaller numbers and slightly easier mathematics).

**Vocabulary**.

* **Implementing cybersecurity has software, hardware, and human components.**
  + This is a theme for the whole lesson
  + Vulnerabilities in hardware and software can be compromised as part of an attack.
  + But, as mentioned in the video, a large percentage of cybersecurity vulnerabilities are human-related, such as choosing bad passwords, (unintentionally) installing viruses, or giving personal information away.
* **Sockets layer/transport layer security (SSL/TLS)**
  + An encryption layer of HTTP. When you see the little lock icon and https it means that you are visiting a website over HTTP but the data going back and forth bewtween you and the server is encrypted.
  + SSL (secure sockets layer) and TLS (transport layer security) use public key cryptography to establish a secure connection.
* **Cyber warfare and cyber crime have widespread and potentially devastating effects.**
  + This is especially true in the case of warfare which (fortunately) we have not experienced much of on a global scale. But using cyber attacks to cripple basic infrastructure (power, water) and communication could be devastating.
* **Distributed denial of service attacks (DDoS)**
  + Typically a virus installed on many computers (thousands) activate at the same time and flood a target with traffic to the point the server becomes overwhelmed – doing this can render web services like DNS, or routers, or certain websites useless and unresponsive.
* **Phishing scams**
  + Typically a thief trying to trick you into sending them sensitive information. Typically these include emails about system updates asking you send your username and password, social security number or other things.
  + More sophisticated scams can make websites and email look very similar to the real thing.
* **Viruses / Antivirus software and firewalls**
  + A virus is program that runs on a computer to do something the owner of the computer does not intend. Viruses can be used as a Bot Net to trigger a DDoS-style attack, or they can spy on your computer activity, such as capturing all the keystrokes you make at the computer, or websites you visit, etc.
  + Antivirus software usually keeps big lists of known viruses and scans your computer looking for the virus programs in order to get rid of them.
  + A “firewall” is simply software that runs on servers (often routers) that only allows traffic through according to some set of security rules.

.

**Video Link** – [The Internet: Cybersecurity & Crime](https://youtu.be/AuYNXgO_f3Y)

**Worksheet** – Complete Video Guide for “Cybersecurity and Crimes” found on my website

**Reading: -** [How Not to Get Hacked](https://code.org/curriculum/csp/docs/hownottogethacked)

**Activity Guide** – Rapid Research – Cybersecurity & Crime found on my website

1. Choose - Choose a cybercrime topic to research (2 mins)
2. Rapid Research - Learn more (15 mins)

We will define “recent” for this activity as the AP Collegeboard does anything after June 2016. The intent is simply to find something that is modern, or well known

Wikipedia is likely to be a source that students find early on.

If you use Wikipedia find links within the wikipedia article to find related news stories. Also take a look at the sources cited at the end of a wikipedia article.

* Find a “recent” event in the news related to the cybercrime topic you have chosen.
* Find at least two articles (or other sources, e.g. video) about the event - presumably each partner finds one.

4. Prepare a brief explanation (5 mins)

* Partners discuss what they read and prepare to quickly present to another group the basics: who, what, where, why, when of the event they found.

**Presentation Tip**

This “presentation” may unfold more like a conversation which is fine. The goal is simply to have students exchange ideas and share interesting things they found but supported by facts they can cite in whatever sources they found.

5. Present to another group (10 mins)

* Put two partner groups together (i.e. small groups of 4) to explain what they found to each other.

6. Review cyber security terms from AP CSP (5 mins)

* The CSP Framework lists a number of terms related to cyber crime and cyber security that are covered in the video and potentially what students reserached here.
* Students need to have a passing knowledge of these terms to the degree that they they could explain each in a sentence, or give an example.
* We will review these terms in the wrap up.

**Assessments – Complete Assessments in Code.org**