HACKING

People ask me: Why do we learn about “Hacking” and “Internet Security” in an English class. Well, when you are doing online research, it’s important to protect yourself from potential hacks while you are searching for material online.

HOW DOES THE INTERNET WORK?
The internet is composed of individual computers (cellular phones, tablets, laptops, and desktops) talking through their Internet Service Providers to different servers. Honestly, servers running web-based code (html, php, java, etc.) comprise the bulk of the material on the web.

In accessing material on a website, your computer voluntarily makes an exchange.
The server asks: Do you want to access my page?
Your computer says: Yes!
The server then offers permission to enter its directories of information.
However, sometimes the server asks to install certain files (or temporary files) in order for you to have access.

These files, oftentimes called Cookies, are stored in your browser in order to permit regular access to the server (and its corresponding website).

Now, here’s the “kicker”:
These cookies sometimes help the server to track you after you leave, oftentimes for marketing purposes, although sometimes these cookies track many different functions.

In addition, servers receive different information from your computer. For example, in order to “access” a server, your computer will relinquish the following information:
Your IP Address
Your Location
Your Browser Type (e.g., Chrome, Firefox, etc.)
Your Browsing History
Your Operating System
And more….

When your computer accesses a dubious system (a server that seems relatively benign, but operated by a hacker), the common files that are instantly uploaded (such as images, coded pages, media, etc), and common files that you choose to download (documents, etc.) may be corrupted and may contain a plethora of different malware and spyware.

WEBPAGES
The front side of a webpage is what you see when you bring up the webpage on a browser.

The back side of a webpage is only the information seen by the person who owns the server.

The owners of websites see many different things as discussed above (your location, your browsing history, etc.). Oftentimes, owners of websites are able to obtain reports about individual users who browse their sites. Some of the tracking software is so insidious that it can track your movement and/or even send the keystrokes you make on your computer or phone.

MAINTAINING PRIVACY
The best thing to do is to use a “private” browsing function which deletes and/or hides your information.

The very best thing to do is to use a Virtual Private Network (or VPN) service which helps to hide your information from the website.

WHO ARE HACKERS?
Various definitions exist:
"A person who uses technology access unauthorized data"
"A person who finds shortcuts"
"A person who innovates"

Hackers represent a culture, a subculture, groups, factions, etc.

White Hat (good)
-Computer Engineers and Developers (playing to make the world a better place)
-Hackivists
-State-Sponsored Hackers (FBI, CIA, NSA, etc.)

Black Hat (evil)
-Script Kiddies (deface websites, overload systems, or cause other mayhem)
-State-Sponsored Hackers (from external countries)
-Corporate Espionage Hackers (spying to gain information on competitors)
-Cyber Terrorist

The first computer engineers were scholars at universities and colleges.
They were the first hackers. In addition, many of our commercially successful business icons are hackers:
Bill Gates was a hacker.
Steve Jobs was a hacker.
Mark Zuckerberg was a hacker. In fact, Facebook started as a "Hack."

And, hackers with in the group, Anonymous, help or hurt computer systems all over the world for the benefit of society.

What are the Primary Targets of Hackers:

+The Internet (via computer, phones, tablets, etc.)
+Internet of Things (everyday things, like refrigerators, cars, appliances, are connected to the web and inherit the same security issues as computers and mobile devices).

COMMON INFORMATION COLLECTION HACKS
Keystroke Logger
-installs into a computer via software application, USB, or via hidden program files in images, emails, and website downloads.
-logs all of the keystrokes by recording them/transcribing them, and sends them to the hacker.

Packet Analyzer (Wireshark) & Encryption Decoder
-the analyzer captures or records traffic within a wired or wireless network by capturing "packets of information" between computers.
-logs all the movement by listing individual IP addresses.
-packets can be decoded and read by hackers (packets include usernames, passwords, comments, messages, etc.)

Infrared Scope/Frequency Intercept Scope
-reads the main screen of a computer or television by intercepting the signal of the screen.

COMMON DISRUPTIVE HACKS
Trojans/Viruses
-installs into a computer via software file
-uploaded by the hacker via website or downloaded by the user via website, email, email attachment, even phone calls/texts
-the applications can do everything from overload your browser (causing it to shutdown) to over working your cooling fans, which prompt your computer to meltdown.

Collaborative Attack/DOS (Denial of Service) Attack
-the hacker attacks multiple computers with a program. These computers attempt to connect to a server or group of servers. The number of connections is too much for the servers to handle, which shuts down access to the server.

TIPS
Social Networking:
ALL PUBLIC INFORMATION is BAD!
[Keep all information private]

Passwords/Phrases:
Upper Case and Lower Case and Numbers don't really matter...
[Sniffers, Remote Screen Readers, etc. can detect passwords, even encrypted passwords]

Password Managers are NOT ALWAYS SECURE! Rather, write them down (on paper) and keep these in a safe place.

DO NOT USE iMessaging or Other Mobile-to-Computer Applications which allow your computer to read your phone's communication.

USE DOUBLE AUTHENTICATION!