UNHAND MY DATA!

A comprehensive yet user-friendly guide to cybersecurity.
Welcome to the Information Age

- The most valuable tool in the modern era is information.
- Data is more than simply that; it opens access to virtually everything one can think of.
- It’s also easily stolen. An attacker needs only one vulnerability; defending requires fixing all vulnerabilities. This is near impossible.
Reasons for Cyberattacks

There are many reasons someone would perform a cyberattack:

- Cybercrime (ex. : Identity theft)
- Espionage (State/Corporate/Personal)
- “Hacktivism” (ex. : Sabotaging someone’s website in protest)
- Intellectual Property
- Messing around

Virtually any system is under attack all the time.
Base Pattern for an Attack:

1. Reconnaissance
2. Find Targets
3. Probe
4. Find Vulnerability
5. Exploit
6. Take Advantage of Vulnerability
Base Pattern for an Attack:

Reconnaissance:
- Automated Scans
- Directory Browses
- Scraping Websites
- Acquire list of Targets

Probe:
- Bad Security
- Missing System Patches
- Easy Password
- “Social Engineering”

Exploit:
- Compromise
- Deny Access
- Hijack
A (very) Common Attack Type: Malware

This irritating cyberweapon comes in many forms:

- **Virus** (Spreads to other executables when run)
- **Worm** (Spreads to other computers in the local network)
- **Trojan** (Disguised as harmless software)
- **Rootkit** (Persistent little bugger that modifies the operating system itself, AND possibly any security software)
- **Backdoor** (Allows unauthorized access)
- **Keylogger** (Records keystrokes. Don’t type anything you wouldn’t want your grandma to know about.)
A (very) Common Attack Type: Malware

It can infect computers in 3 ways:

- Software errors (Exploits bugs in the code)
- Configuration errors (Exploits unconfigured/badly configured software)
- User errors (Exploits the foolishness of users who think .exe files they received from “XXX Real Estate Prescription Credit Corp.” are safe)
Noteworthy Examples

- **Rootkits** can provide “registry keys” which can keep malware multiplying.
- Malware from other countries can check region – if a computer only has the English language installed...
- Some disguise themselves as security software popups – don’t push any button, INCLUDING the “X”.
- Spyware that haunts your internet history,,, that you thought you cleared a day ago.
A Certain Example: Attack on Sendori

- On Windows, an exploitation of a vulnerability in this software called Sendori installed a PUP consisting of adware that just wouldn’t die.

- The adware installed two registry keys, meaning it would keep appearing every minute or so. Multiple instances of this malware could appear.

- Not one, but two security systems were required to remove it.
Attack on Sendori

- The first security software actually detected and, at a button press, removed the existing instances. A scan run on the second software also removed a (possibly different) instance.

- Running a scan on the first revealed the registry keys themselves, and removed them. This did not stop the malware from generating on its own, however...

- ... The second software allowed active processes on the computer to be viewed and controlled. Blocking one of Sendori’s processes and “trustedinstaller.exe” and then restarting the computer seemed to solve the problem.

- The first software still detected some instances upon reboot, but only managed to remove the first instances because the others “didn’t exist”. The malware did not at any time afterwards, and is most likely removed.
Part 2: Protection

Again, defence is so complex that the only way to be completely secure is to prevent your computer from connecting to the internet entirely (airlocking). But you probably want to use the internet, right? Here are a few steps you should take.

- The first line of defence is to NOT ASSUME YOUR COMPUTER ISN’T UNDER ATTACK. Every connected computer is targeted at any time, though with proper security, most attacks fail.

- Update your system and plugins, no matter how lazy you are. Many updates are security patches designed to address known vulnerabilities.

- Switch IP addresses occasionally.

- Change all passwords frequently. And please, don’t make your password something obvious such as “kitty1”.

- Set “routing rules” on your router to route untrusted packets away from the server.
Protection, Continued

- Disk encryption encrypts the entire hard disk.
- Obtain powerful security software, even if your computer is a mac. Multiple security software can provide additional defence, as demonstrated in the Sendori case.
- Intrusion Detection software is an antivirus for your entire network, not just your computer. “Integrity Monitoring” searches for unauthorised changes to the system.
- Encrypt your emails. Numerous resources exist that can help you with this.
- Don’t trust websites without an https:// (the “s” means it’s secured) and be wary of websites without a lock specifying the site is certified. (Have you ever noticed a warning symbol occasionally appears instead of a lock when logging in to the KUA website?)
Protection, Continued

- Secure your network with a WPA complex password.

- Look at the active processes running on your computer (many antivirus programs can help you with this) and monitor the ones you find glaringly suspicious. A process such as “trustedinstaller.exe” is most likely not a legitimate trusted installer (and, in this case, isn’t).

- For privacy, Firefox is the best browser. You can further improve privacy by installing add-ons for Firefox and configuring it not to accept cookies. Also, clear your cache.

- And please, use common sense when downloading files, especially .zip and .exe files. Some security programs have sandboxes where you can safely run the file and check for malware first.