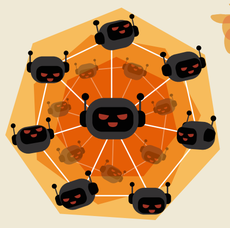
Cyber Literacy

The Internet of Things (IoT) has ushered in new conveniences, increased opportunities, and added means to share, connect, shop, and more. The integration of the Internet into almost every aspect of our lives has fundamentally redefined the way we as consumers operate. With this phenomenon, however, has also come a new array of risks and threats – and a new vocabulary to pair with it. Today's digital dangers affect almost every individual across the globe; and yet, for most, putting a name to these threats can often prove challenging. It's no secret that knowledge is power, and the best way to protect yourself starts with education.

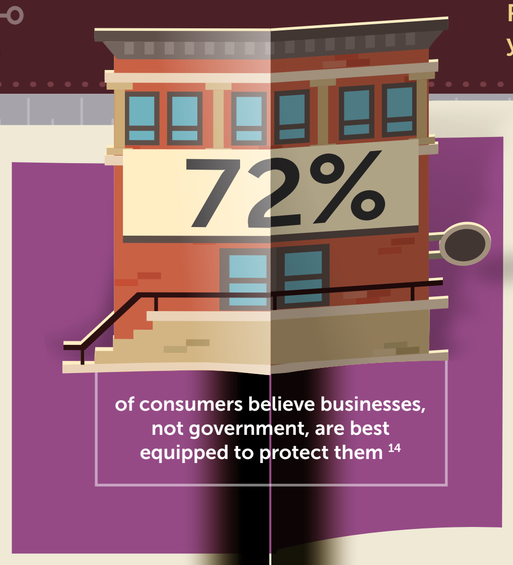
Read on to brush up on your cyber jargon so that you're better equipped to fend off today's hackers.



Botnet /bot-net/

A network of internet-connected devices infected with malware and controlled as a group without the owner's knowledge

Botnets are controlled by a "botmaster" who use them to commit crimes like identity theft/fraud or spreading malware or spam



of consumers believe businesses, not government, are best equipped to protect them [14]

Only **1 in 10** consumers feel they have complete control over their personal information [14]

Ransomware /ran-suh m-wair/

Malware that blocks access to important and/or sensitive data, whereby the victim is forced to pay a ransom to get it back

70% of ransomware payments were paid in Bitcoin in 2016 [8]

Examples include fake social media accounts of celebrities or even regular people

Brandjacking /brand-jak-ing/

When someone takes over the online identity of another person, business, or brand (usually for malicious purposes)

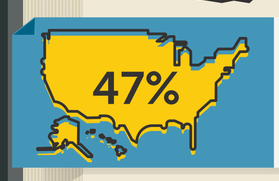
The word "spyware" didn't start getting used until early 2000 when it was included in a news release for a personal firewall product [9]

Spyware /spahy-wair/

Software that gathers personal data (i.e., credit card numbers or account credentials) unknowingly from a victim and then forwards it to a third party

Carding /kahr-d-ing/

Purchasing retail items with counterfeit credit cards or stolen credit card information



of the world's credit card fraud happens in the U.S. when Americans only account for **24%** of the world's total credit card volume

Social Engineering /soh-shuh l en-juh-neer-ing/

The psychological manipulation of people into performing specific actions or divulging personal information

95% of successful cyberattacks are the result of a phishing scam – a top social engineering technique [10]

Only a quarter of consumers believe most companies handle their sensitive personal data responsibly [14]

Catfishing /kat-fish-ing/

Setting up a fictitious online profile, most often to lure another person into a fraudulent romantic relationship

53% of people lie on their online dating profiles [1]

Trojan Horse /troh-juh n hawrs/

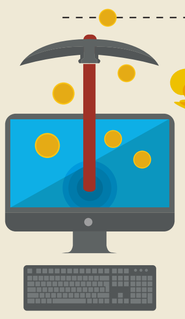
A type of malicious computer program that appears harmless and so is willingly installed on victims' computers – usually by a social engineering technique

The term comes from the Greek story of the Trojan War, whereby the Greeks gave a giant wooden horse to their enemies as a "peace offering" – only for Greek soldiers to emerge from it

Zombie /zom-bee/

A computer connected to the Internet that has been compromised by a hacker, computer virus, etc., often used to perform malicious tasks under remote direction

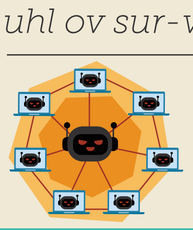
Botnets of zombie computers are often used to spread email spam and launch DoS attacks; unfortunately, most owners of zombie computers are unaware that their system is being used in this way



Cryptojacking /krip-toh-jak-ing/

The secret use of your computing device to mine cryptocurrency

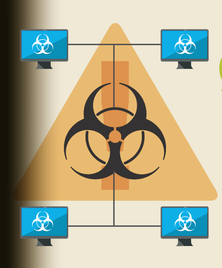
8,500% Attacks involving cryptojacking increased by 8,500% in 2017 [2]



Distributed Denial of Service (DDos) attack /dih-strib-yoo-tid dih-nahy-uhl ov sur-vis/

While a DoS attack typically uses one computer and one Internet connection to flood a targeted system, a DDoS attack uses multiple compromised systems (i.e., a botnet)

DDoS attacks are one of the hardest cyber threats to defend against because it's so difficult differentiating between legitimate access and a flood of botnets



Virus /vahy-ruh s/

Harmful "software" that attaches itself to active host programs (therefore replicating itself) so that the computer is unable to function normally

In 1992, only 1,300 viruses were in existence, an increase of 420% from December of 1990 [11]

Denial-of-service (DoS) Attack /dih-nahy-uhl ov sur-vis uh-tak/

A cyberattack in which a hacker makes a machine or network unavailable to legitimate users by flooding the target with traffic and making it crash

2000 The first documented DoS attack occurred in early 2000, when "mafiaboy," a 15-year-old Canadian hacker, successfully crashed sites like Amazon and eBay [3]

Keylogging /kee-law-ging/

When a malicious computer program unknowingly records every keystroke made by a computer user (usually to steal passwords or credit card numbers)

Keylogging predates the era of personal computers, with hardware-based keyloggers being used in typewriters as early as the 1970s [6]

Worm /wurm/

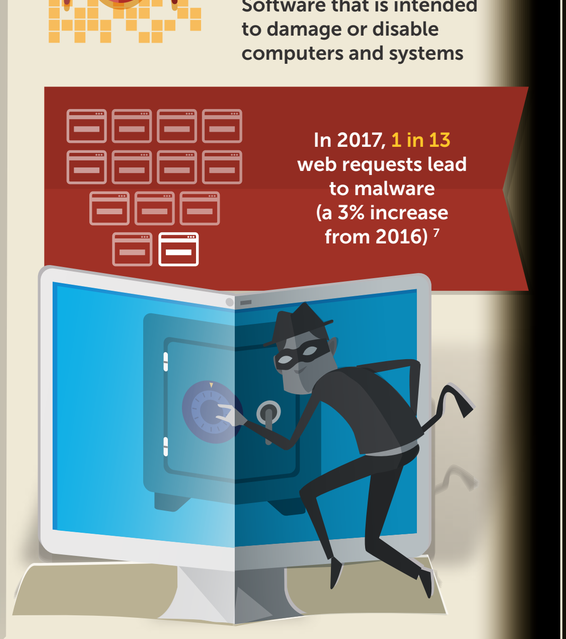
A stand-alone program that replicates from machine to machine across network connections, often clogging networks and information systems as it spreads

Unlike viruses, worms don't require any human intervention to spread and infect because they are able to self-replicate via computer networks

Malware /mal-wair/

Software that is intended to damage or disable computers and systems

In 2017, **1 in 13** web requests lead to malware (a 3% increase from 2016) [7]



Profile of a Cybercrime Victim [13]

Bad Password Habits

They're more likely to use the same online password across all accounts

20% victims 17% non-victims

They're more likely to share at least one device or account password with others

58% victims 37% non-victims

New Technology Adopters

37% of cybercrime victims own a gaming console and smart device versus 28% of non-victims

37% victims 28% non-victims

They're 2x more likely to own a connected home device than non-victims

victims non-victims

Cybersecurity Overconfidence

33% of cybercrime victims believe they're at a low risk of becoming one

While the majority of these terms were meaningless just a couple decades ago, their impact in today's cyber world is far from insignificant. With approximately one million new threats being released every day, it's no wonder that one in three people fall victim to some form of cyberattack each year [12].

SOURCES:

[1] psychologytoday.com/us/blog/the-mating-game/201609/the-ugly-truth-about-online-dating

[2] symantec.com/about/newsroom/press-releases/2018/symantec_0321_01

[3] britannica.com/technology/denial-of-service-attack

[4] venturebeat.com/2015/02/08/fullz-dumps-and-cvvs-heres-what-hackers-are-selling-on-the-black-market/

[5] venturebeat.com/2015/02/08/fullz-dumps-and-cvvs-heres-what-hackers-are-selling-on-the-black-market/

[6] community.spiceworks.com/topic/2003395-what-is-keylogging-definition-history-and-how-to-detect-word-of-the-week

[7] images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

[8] comparitech.com/antivirus/ransomware-statistics/#gref_

[9] adaware.com/faq/spyware-history

[10] infosecurity-magazine.com/news/phishing-remains-top-attack-vector/

[11] infoplease.com/science-health/computers/computer-virus-timeline

[12] cybintsolutions.com/cyber-security-facts-stats/

[13] https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[14] PwC US Protect.me Survey, 2017

The difference often lies in what you know. Now that you know what types of threats exist, it's time to put your new wisdom into action.