HEPLERBROOM LLC

PROVEN LAWYERS IN THE RIGHT PLACES

WE SPEAK THE LANGUAGE:
CYBERSECURITY GLOSSARY

As lawyers, we have a language unique to our profession, with terms and phrases that would be foreign to most. Many professions are like that, and the cybersecurity industry is no different. Fortunately, our lawyers also speak the language of the cybersecurity industry. Consider the following glossary a pocket dictionary of sorts. (And no, these definitions were not simply cribbed from Wikipedia.)

Bot: A computer that performs a repetitive task by way of software at a much faster pace than could be done with a human user. Bots can be used to buy up tickets, increase page views, and leave inflammatory comments on message boards. A bot is, in essence, a zombie computer. (*See also* **Botnet**.)

Botnet: A series of interconnected **Bots**, or a robot network, **that** work in coordination—and rarely for a noble cause. A botnet is often used to send large amounts of spam, distribute viruses and malware, and engage in DDoS attacks.

Cloud computing ("the Cloud"**):** The practice of using remote servers to store, manage, and process a user's data, rather than using a local server or personal computer. The advantage to cloud computing is that the user's data is accessible from any computer and that the data would not be lost if the local server or computer were damaged or stopped working.

Distributed Denial of Service (DDoS): A method of flooding the bandwidth or resources of a network or server until it crashes and cannot accept incoming traffic. A botnet is often the mechanism for crashing a website.

Drive-by Download: Software (which in this case is really malware) that downloads automatically to a user's computer or device, often stemming from a compromised or out-of-date website, browser, or operating system. It is a "drive-by download" because the user does not need to actively download the software to infect their device.

Firewall: Part of a computer network that is designed to prevent unauthorized access based on predetermined security protocols.

The Internet of Things (IoT): Everyday devices (such as pacemakers, fitness devices, thermostats, automobiles, and other consumer products) that are now networked and connected to the Internet, which, in turn, allows these devices to receive and provide feedback. There are estimates that the IoT could consist of 50 billion objects by 2020.

Malware: The general term for malicious software or code, which broadly includes viruses, Trojan horses, spyware, and other methods for compromising or infecting a computer.

Penetration Testing (Pen Test): The practice of testing a computer system or network to find security flaws or weaknesses before an attacker could exploit these same vulnerabilities. (*See also* **White Hat.)**

Periscope Skimming: A process that involves using a skimming probe that connects directly to an ATM's internal circuit board as a means of stealing credit card data.

Personal Identifying Information (PII): Information that would permit someone, either directly or indirectly, to discover an individual's identity. PII can include an individual's name, address, Social Security number, telephone number, email address, birth date, and mother's maiden name. If not properly safeguarded, an individual's PII can be misused and lead to identity theft.

Phishing: The process where criminals send out legitimate-looking emails, en masse, hoping that at least one recipient will be tricked into disclosing their personal or financial information. The email often appears to come from a large, well-known company, such as a bank or pharmacy, and asks the user to update their credit card information or supply identifying information to receive a product. (*See also* **Spear Phishing**.)

Ransomware: Software that encrypts the files on a user's network, making the files impossible to access. Once the ransom is paid (usually in untraceable Bitcoin), the criminal then unencrypts the files. Because ransomware offers the potential for a quick payout, it is becoming a well-worn arrow in the digital criminal's quiver.

Scareware: Programs that trick a user into believing he or she has a virus or has inadvertently downloaded illegal content. The user is then prompted with a bogus solution, which can involve downloading malware or paying for a useless anti-virus system.

Social Engineering: Any form of cyberattack that relies on human interaction and involves convincing that individual to breach security, often unwittingly. **Phishing, Spear Phishing**, and **Scareware** are examples of social engineering.

Spear Phishing (or "whaling" for larger targets): The process where h, criminals use personal-looking emails that purport to be from a company executive, co-worker, or client in order to access protected information or to perpetuate a fraud. Because the messages looking genuine, they are far more successful than previous, widely-cast phishing efforts.

Trojan horse: A malicious program, such as an innocent-looking email attachment, designed to breach the security of a computer network by misleading the user about the program's true function.

White Hat: Someone who specializes in breaking into networks for the purpose of identifying vulnerabilities before they can be exploited by a black-hat hacker. (Also known as a so-called "ethical hacker.")

Zero-Day Vulnerability: A security flaw in software that is unknown to the vendor until that flaw is exploited by hackers, giving the vendor essentially "zero days" or "zero hours" to develop a patch.

Please note that these definitions, while being drawn from sources we consider reliable, do not constitute legal advice. These definitions are not intended as a substitute for reviewing the relevant statutes, regulations, and case law.