| Security Term | Definition |
| --- | --- |
| Advanced Persistent Threat (APT) | A targeted and sophisticated cyberattack, usually executed by a group, such as a foreign government or a hacker organization. These attacks focus on systems rather than individual users, and often target businesses or political organizations. The goal of these types of attacks is to access specific sensitive information by infiltrating a network and mining information over an extended period of time until they’re eventually discovered.  *See also: Cyberattack* |
| Business Associate | Derived from HIPAA, a person or an organization doing business with or performing services on behalf of a health care covered entity, such as a hospital or health insurer. Business Associates are subject to HIPAA guidelines with regard to how they handle protected health information (PHI), and are subject to penalties for disclosure of that information. Many law firms are considered Business Associates.  *See also: Business Associate , Business Associate Agreement, Covered Entity, HIPAA, Protected Healthcare Information* |
| Business Associate Agreement (BAA) | An agreement between a Covered Entity and a Business Associate, or between two Business Associates, that the Business Associate will comply with the appropriate guidelines and regulations related to handling, using, and securing PHI. Business Associate Agreements typically include requirements for reporting a breach or disclosure of protected information.  *See also: Business Associate, Covered Entity, PHI* |
| BYOD (Bring Your Own Device) | The practice of allowing employees to use their own mobile devices, rather than devices owned by the firm, to access firm email, software, and other systems. |
| Clickjacking | A method of tricking someone to click on a web link to reveal confidential information or take control of their computer or device using malicious code or script.  *See also: Malware* |
| Confidential Information | A broad term applied to client data for which unauthorized access or disclosure could result in an adverse effect.  *See also: Protected Information* |
| Covered Entity | Derived from HIPAA, this is an organization or corporation that directly handles Personal Health Information, or PHI. Common examples include hospitals, doctors’ offices, health insurance providers, and assisted living facilities. Under HIPAA and HITECH, covered entities are required to comply with specific guidelines for collecting, maintaining and securing PHI.  *See also: HIPAA, HITECH, PHI* |
| Cyberattack | An attempt to damage, disrupt, or gain unauthorized access to a computer, network, or electronic information. Cyberattacks range from relatively simple social engineering attacks to sophisticated Advanced Persistent Threats.  *See also: Advanced Persistent Threat, Social Engineering* |
| Dual-factor Authentication | Sometimes referred to as two-factor or multi-factor authentication, it is the process of requiring two of the three factors of identifying and validating a person’s identity before granting access.  *See also: Multi-factor Authentication* |
| Electronic Protected Health Information (ePHI) | Protected Health Information that is transmitted or maintained electronically.  *See also: Protected Health Information* |
| Encryption | The process of converting data into a code. To read encrypted data, a secret key is needed to "unlock," or convert, the data into readable form. Encrypted data is referred to as *ciphertext*, and unencrypted data is called *plaintext*. |
| Espionage | A form of intelligence gathering by which secret, confidential or protected information is obtained without the permission of the information’s owner. |
| Hacking | Bypassing security measures to gain access to a computer system or network. Individuals who perform this action are referred to as Hackers. |
| Health Insurance Portability and Accountability Act (HIPAA) | The Act includes regulations protecting the privacy of individuals’ health information by governing the way in which Covered Entities and their Business Associates collect, maintain, use, and disclose Protected Health Information (PHI).  *See also: Business Associate, Covered Entity, Protected Health Information* |
| Health Information Technology for Economic and Clinical Health Act (HITECH) | Signed into law in 2009, the primary goal of the HITECH Act was to encourage the adoption of electronic health records, or EHRs, by healthcare organizations. The Act also establishes requirements for professionals who serve the healthcare industry, including law firms, around how they maintain, use, and disclose PHI.  *See also: Protected Health Information* |
| Juice Jacking | A name applied to the action of interrupting or redirecting the data flow from a mobile phone when connected to an unsecure power supply such as those in an airport kiosk. |
| Malware | A broad term describing malicious software intentionally designed to disrupt computer operations, gather sensitive information, or gain access to private computer systems.  *See also: Trojan Horse* |
| Metadata | Often called “data about data,” metadata is information embedded in an electronic document that contains properties such as the software used to create it, the date and time of its creation, or the name of the author. Metadata profiles are sometimes likened to cards in a card catalog in a library. |
| Multi-factor Authentication | The process of requiring more than one method of identifying and validating a person’s identity before granting access. It requires using two of three categories of verification factors: what you know, what you have, and who you are. |
| Personally Identifiable Information (PII) | Information about an individual that could reasonably be used to identify them, such as their name, fingerprints, email address, or social security number. PHI and PIFI are subtypes of PII.  *See also: Protected Healthcare Information, Personally Identifiable Financial Information* |
| Personally Identifiable Financial Information (PIFI) | A type of Personally Identifiable Information (PII) linked to an individual’s finances, such as a credit card number, or a bank account number.  *See also: Personally Identifiable Information* |
| Phishing | The practice of sending spoofed email messages with the intention of collecting information for malicious purposes. Often, phishing messages include a link which the recipient clicks and then enters confidential information, which is captured for later use. This is the most common type of social engineering attack.  *See also: Social Engineering, Smishing, Spoofing* |
| Protected Health Information (PHI) | Individually identifiable information relating to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; past, present or future payment for the provision of health care to an individual. |
| Protected Information | Highly sensitive information that is safeguarded by law or regulation.  *See also: Confidential Information* |
| Ransomware | Malicious software designed to block access to a computer system until a sum of money is paid. Most attacks are the result of clicking on a link in an infected email message or visiting a website that has been hacked. |
| Scraping | The process of taking information posted on a social media or web site and using it to breach the owner’s account(s) or commit fraud involving identity theft. Also known as screen scraping.  *See also: Social media, Social Engineering* |
| Shoulder Surfing | The use of direct observation, such as looking over someone's shoulder or using video surveillance, to obtain information. |
| Smishing | A text-based, or SMS (Short Message Service)-based, phishing scam.  *See also: Phishing, Spoofing, Social Engineering* |
| Social Engineering | A method of hacking that relies on human interaction and deception to circumvent security procedures and obtain confidential information. Social engineering is like a con game, with the hacker relying on the target to volunteer information that can be used for malicious purposes.  *See also: Phishing, Smishing, Spoofing* |
| Social Media | An online publication or website designed to facilitate social interaction, often in real-time. Examples include Facebook, Twitter, LinkedIn, and YouTube. Social media sites have become an increasingly common tool for social engineering attacks.  *See also: Scraping, Social Engineering* |
| Spear Phishing | A targeted approach of sending spoofed messages that is distinguished by three elements: the message appears to come from someone who is known and trusted by the recipient, contains specific information that gives it credibility, and the request in the message appears to be reasonable, based on the alleged sender of the message.  *See also: Phishing* |
| Spoofing | A process by which technological data is altered so the actual information is disguised. For example, phishing messages are often spoofed to change the sender information so the email appears to have come from someone other than the actual sender. IP spoofing is a method of falsifying a computer’s IP address so it is difficult to track online.  *See also: Phishing, Social Engineering* |
| Spyware | A broad term for applications that send information from their computer to a third party without the user's knowledge or permission. Spyware is often installed online by clicking links in pop-up windows, advertisements, or games. |
| The Cloud | Computing resources that are delivered as a service over a network, including the Internet. Cloud services might allow a user to store files or use software that is not installed on their computer. A cloud can be private or public; public clouds provide services via the Internet to anyone, while private clouds utilize a proprietary network or limited access environment. Popular cloud solutions include Dropbox, Flickr, iCloud, and Gmail. |
| Trojan or Trojan Horse | A type of malware in which malicious code intended to damage computer systems or steal information is hidden in a seemingly legitimate computer program or document. The name comes from Greek mythology, when the Greeks presented Troy with a “gift” of a huge wooden horse, with an army hidden inside. The Greek Trojan Horse serves as a perfect example of a social engineering attack.  *See also: Malware, Social Engineering* |
| URL (Uniform Resource Locator) | The letters, numbers, and symbols that are the address for a resource on the Internet. For example, http://www.travelingcoaches.com. |
| Virus | A computer program that replicates itself by executing code that copies the malicious code to other programs or files, allowing it to spread from one computer to another. |
| VPN (Virtual Private Network) | Technology that creates a secure network connection over a public network such as the Internet. VPN allows employees who have Internet access a secure method to connect to their organization’s network while outside the office. |
| Wi-Fi | Short for “wireless fidelity,” it is a type of wireless network, most commonly associated with internet access. Wireless networks can utilize varying degrees of security, ranging from no security to sophisticated encryption protections. The level of security associated with a wireless network is important to understand as lesser security protocols can be susceptible to access by unauthorized users. |