FACTS
A nelnet Company

K-12 School Cybersecurity Terms Glossary

Get familiar with these key IT and security terms and acronyms. They may help keep you and your school's data safe and secure!

DATA BREACH

A data breach is a security compromise that takes place without malicious intent. A data breach is unintentional and may happen due to a mistake or negligence. If a computer is left unattended while a spreadsheet filled with financial information is displayed, someone may be able to view or take pictures of the data displayed, resulting in a breach.

DATA HACK

Although the terms data breach and data hack are used interchangeably, they have distinct definitions. A data hack is the opposite of a data breach. It's an intentional, malicious attempt to access secure data without the authority to do so. The purpose of a hack varies depending on the goal of the hacker. It may result in data being unavailable to authorized users (ransomware or denial of service) or being stolen and sold for profit.

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS)

The purpose of a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack is to overload the target (usually a website) with extremely high levels of traffic. This amount of traffic causes the website to lose track of how to respond to all the requests – resulting in delayed service or, in some cases, a total website crash that lasts anywhere from hours to days.

The difference between DoS and DDoS is that a DoS attack only uses one system to flood the target with requests, while a DDoS uses multiple compromised computer systems to continually flood the target with requests. A DDoS attack is often more severe; since there are multiple computer systems in use, it can be more complicated to determine the origin of the attack.

DOMAIN SPOOFING

Like phishing, domain spoofing is a common type of scam where an attacker will register domains similar to legitimate websites in an attempt to attract individuals into visiting them or clicking on the URLs. Visitors will believe they are visiting or landing on a legitimate website, when they are actually visiting a site controlled by an attacker.

PHISHING

Phishing is a technique that uses electronic communication (email, instant messaging, or text messaging) to deceive users into providing personal information such as login credentials or credit card information to an attacker. One common example of phishing is communication from a trusted entity with correct formatting, logos, and signatures saying they've suffered a breach and need all customers to change their password by clicking on a link. The email address and web page from the link look like what could be expected from the trusted entity, so customers are tricked into submitting their username and password on a duplicitous page.

Since this malicious site isn't affiliated with the trusted entity in any way, the attacker collects the credentials necessary to create fraud against the individual. This can lead to unauthorized purchases, stealing of funds, or even identity theft. When phishing is used in a government, educational, or corporate environment, it can be even more devastating. Organizations can sustain financial losses, declining market share, loss of customer confidence, and loss of reputation after a phishing attack.

PIGGYBACKING OR TAILGATING

Piggybacking, also known as tailgating, is a physical social engineering attack. The term refers to when a person tags along behind another person who is authorized to enter a restricted area. This attack is extremely simple and can often be achieved without attracting suspicion. The attacker can visit with someone headed toward an authorized area and simply walk into the restricted area behind them. If the attacker is questioned, they can quickly make up a feasible excuse as to why they don't have their access key with them. The attacker can also look preoccupied or have their hands full when they are going through the door, causing the authorized person to lend a hand by keeping the door open. This is one case where good manners are not a good idea.

QUID PRO QUO

For those of us who haven't brushed up on our Latin in a few years, quid pro quo is Latin for "something for something." This social engineering tactic works well on students who may be offered a free t-shirt, access to an online game, or even a free pizza by simply filling out a form which may ask for personal information or school credentials. Once the attacker has the credentials, they can use them to gain unauthorized access to the school or student's information.

RANSOMWARE

As this method continues to grow by targeting governments, educational institutions, and other businesses, it's received more media attention than usual. Ransomware, as the name suggests, is used by attackers to hold data hostage by encrypting it. Before the attacker decrypts the data, they'll typically demand information or a ransom payment from their target.
Law enforcement, including the FBI, recommend not paying the attacker for the decryption key. Paying the ransom doesn't guarantee a decryption key will be provided or that the key is valid. Paying the ransom also provides incentive for more ransomware attacks and the payments could actually be funding other illicit activities associated with the attackers.

SCAREWARE

Scareware is a scam that frightens you into buying or downloading malicious software as security protection. Have you ever visited a website and a red banner warns you that your computer has a virus and that by clicking the banner you can remove it and protect your computer? Scareware works because the victim is scared or curious enough to click the link. However, by clicking the link malicious software is installed or the victim is directed to a website to purchase anti-virus solutions which contain the malicious software. The purpose of the malevolent software is to collect password credentials, financial information, or other confidential information that can lead to future identity theft.

VISHING

Vishing is the practice of eliciting information or attempting to influence action via telephone to gain personal information. For example, the attacker may impersonate a technical support analyst calling to discuss an issue. The attacker uses technical jargon and provides reasons why there's an urgent need for the person to provide their credentials so the "analyst" can ensure everything is working as expected. These attacks are easy to perform, take no technical knowledge, and only need to succeed once for the attacker to gain unauthorized access to the protected data.

For more information, explore a fact sheet and additional resources prepared by CISA in collaboration with the FBI: Cyber Threats to K-12 Remote Learning Education