CANNABIS CONTROL DIVISION
MONTANA

Cyberattacks Are Requiring Businesses to Implement Effective Cybersecurity

What is a cyberattack?

A **cyberattack**[1] is an intentional action conducted by an individual or organization (a.k.a. an attacker, hacker, or cybercriminal) to gain unauthorized access to computer systems. These attackers are often attempting to steal sensitive information as it pertains to companies, and the personally identifiable information (PII) of their customers.

These cyberattacks can disrupt business operations, and they can even annihilate a business, forcing it to close. In fact, approximately 6 out of 10 small businesses in the United States that have been victimized by a cyberattack ceased their operations in less than a year.[2]

The marijuana industry is not immune to cyberattacks but can help reduce the likelihood of becoming a victim by understanding and identifying what cyberattacks are and by implementing effective cybersecurity practices.

What are the common types of cyberattacks employed by hackers?

- **Phishing**[3]
  In this type of attack, the hacker impersonates a person or a company and then sends a deceitful email to the recipient. This email is sent as an attempt to have the recipient disclose confidential information (credit card information, trade secrets, etc.) or download malware (a.k.a. malicious software). Phishing is the most common type of cyberattack.

- **Malware**[4]
  Malware is a file or code that is sent by the hacker in attempt to breach a computer network by having the recipient click on a link or email attachment that

[1] https://www.ibm.com/topics/cyber-attack
[2] https://blog.rsisecurity.com/5-cyber-security-threats-in-the-cannabis-industry/
[3] https://blog.rsisecurity.com/5-cyber-security-threats-in-the-cannabis-industry/
[4] https://www.paloaltonetworks.com/cyberpedia/what-is-malware

was sent in order to gain access to the computer's network. Malware can deliver viruses, spyware and even ransomware.

- **Man-in-the Middle Attacks (MitM)**[5]
  This occurs when communications between 2 or more parties is intercepted. The hacker is often eavesdropping on their potential victims to then steal log-in credentials and other sensitive information. It is one of the oldest forms of a cyberattack.

This is not a comprehensive list of the types of cyberattacks utilized by hackers to attempt to gain unauthorized access into a computer network.

What is cybersecurity and why is it important?

Cybersecurity is the practice of protecting computer systems, networks, and programs from digital attacks[6]. If a business can successfully implement effective cybersecurity measures, it can reduce its likelihood of being attacked. These attacks are costly to a business and are also costly to society.

The global losses incurred by cyberattacks were estimated to $945 billion dollars (USD) in 2020. There are over 71 million people that fall victim to cybercrimes yearly, and individuals lost an average of $4,476 (USD). Additionally, personally identifiable information (PII) like a Social Security Number or a passport number can fetch a hacker up to $200 per record[7].

What can businesses do to effectively implement useful cybersecurity practices?

- Educate employees about cyberattacks as they are often a company's first line of defense, and hold regular sessions to continue their education
- Create a strong password policy: longer & more complex passwords mixed with characters, and frequently change passwords
- Be sure to create data backups and regularly perform backups
- Maintain the physical security of company devices (computers, cell phones, store keys, etc.)

---

[5] https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html
[6] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[7] https://purplesec.us/resources/cyber-security-statistics/#:~:text=71.1%20million%20people%20fall%20victim,scams%20lost%20%24225%20on%20average.

- Have dedicated IT support, when possible

Are there educational resources available for businesses and their employees?

The Department of Homeland Security offers training and related resources and materials with their "Stop. Think. Connect" campaign at no cost.