yardstick technologies inc.

4 Common Types of Cyber Attacks

Social Engineering

Uses psychological manipulation to trick users into making security mistakes or giving away confidential information. This includes attacks like phishing, scareware & baiting.
By March 2020, phishing attempts increased by **667%** and **43% of workers** admit making mistakes that compromised cybersecurity.

Ransomware

A form of malware that encrypts a victim's files. The attacker demands a ransom from the victim to restore access to the data after receiving payment. The average amount to restore the damage is **$1.45 million**.

Third-Party Breach

Occurs when sensitive data is stolen from a third-party vendor or when their systems are used to access sensitive information stored on your systems. As much as **80% of organizations** experienced a cybersecurity breach from a vulnerability from their third-party vendor.

Cloud Computing Vulnerabilities

Cybercriminals scan for cloud servers with no password, exploit unpatched systems, and perform brute-force attacks to access the user accounts. Cyber-attacks on cloud systems spiked **250%** from 2019 to 2020.

The Best Protection

Protecting against cyberattacks starts with implementing a strong cybersecurity strategy and effectively communicating it to the entire workforce and training employees on how to respond.

Looking for a solution?

Yardstick has built a comprehensive security program using a multilayered approach that takes into account both technology and human factors.

Contact us to learn more!
780-701-1838
www.yardsticktechnologies.com

INFORMATION SOURCE

SECURITY MAGAZINE
HTTPS://WWW.SECURITYMAGAZINE.COM/ARTICLES/94506-5-BIGGEST-CYBERSECURITY-THREATS