ALASKAS I.T. PROVIDER

JP | TECHNICAL

CYBERSECURITY ESSENTIALS for BUSINESS OWNERS

OWN IT.
SECURE IT.
PROTECT IT.

TABLE OF CONTENTS

OWN IT.
SECURE IT.
PROTECT IT.

INTRODUCTION

Cybercrime and cyber-attacks are becoming **more prevalent** with each passing day.

Over half of small and medium businesses **(SMB)** have reported being the victims of cybercrimes. Every day, there are new headlines about **data breaches, hackings, cyber attacks,** and **various forms of crimes** against businesses.

In a survey, over two-thirds of the participating businesses had suffered at least one cyber attack, while one-third had experienced the same in the l**ast 12-months.**

66%

of **small businesses** are very concerned about **cyber security risk.**

56%	*Specific cybersecurity "experts" in the organization*
52%	*Incident response planning*
51%	*Cybersecurity insurance*
45%	*Document Management*
43%	*Endpoint protection*
40%	*Security awareness training*
37%	*Network protection*
31%	*Email security*

Cybercrime is a significant threat to businesses. It can lead to disruption of operations, breach of business and customer data, unauthorized access to networks, and more. The average cost of a data breach for a small-to-medium business is a staggering **$149,000.** On top of that, **80%** of SMBs worry about becoming the target of cybercrime in the **next six months.**

Additionally, cyber-attacks remain a worry whether we are talking about the **cloud** or through **emails**.

Many governments have moved to the cloud but are looking for **better ways to protect their data.** A part of that is to increase collaboration between intelligence and law enforcement agencies worldwide to tackle crime. The popularity of smartphones and the increased use of apps also pose a significant risk to **mobile security.** Consumers use apps to input sensitive information like personal, financial and banking information. These apps will need to evolve with new technologies to continually find new ways to resist **attacks** and **data leaks.**

Additionally, as more and more applications are moving to the cloud, malicious actors are getting better at **evading detection by standard security measures and protocols.**

The act of distributing ransomware and holding sensitive data is on the increase as organizational data is **going beyond the control of the company.**

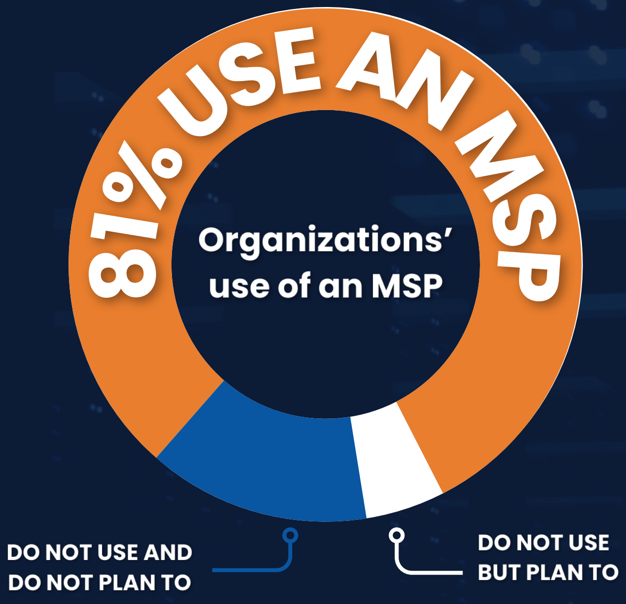
Evolving from simple malware, ransomware has become more **sophisticated** and **efficient.** Cybercriminals are now targeting the local backups, which foil the efforts of the security staff to **restore encrypted data.**

This threat is **no longer limited to local networks**: ransomware attacks remain a problem in cloud environments.

Email remains the most favored method of cybercriminals. Over **91%** of attacks are initiated by email. Traditional antivirus programs cannot identify the phishing attacks employed by hackers.

51% of small businesses say they are not allocating any budget to cybersecurity.

jptechnical.com



Malware can be delivered and initiated on a system **without the user's knowledge**, possibly for a long time. One example of such an attack was the one dealing with the **US Democratic National Party**, where cybercriminals took control of their system.

There is a need to increase the pace of development for holistic solutions to cybercrime. **75%** of businesses in the survey above feel they need to put more emphasis on cybercrime prevention. However, **there is a large gap between reality and expectation.** Most businesses are under educated when it comes to the nuances of cybercrime.

This creates an adverse situation as the organizations are **not able to protect themselves from cybercriminals.** Without a plan, organizations don't know how to react and what steps to take when their network and systems are **compromised.**

Here the role of managed IT service providers (MSPs) becomes **crucial.** MSPs can guide SMBs on the right path and help them stay protected from the increased incidents of cybercrime. They educate clients about the need for a **holistic security solution** and the evolving cybercrime landscape. MSPs should also provide SMBs with a complete collection of security solutions so that they can **stay protected** and **minimize risk.** MSPs can help bridge the gap between the current level of protection and the optimum level desired by businesses. **Enterprises** are recognizing this fact and joining hands with MSPs to eliminate and prevent cyber-attacks and threats. **Eight out of ten** surveyed SMBs are working with an MSP, and **four** of them want to keep working with their current security partners. **Three companies out of ten** plan to switch to a different MSP in the coming months. **12%** of SMBs that don't work with an MSP plan to partner up with one within the **next twelve months.**

9 in 10 employees say their organization would consider switching to a new MSP if they offered a solution that met their needs.

When asked what benefit they expected to see from using an MSP, **50%** of SMBs said increased security, even if they had **outsourced their cybersecurity**

MSPs can be the ideal partner of SMBs to fight cybercrime, as **62%** of companies don't have the required in-house skills. The managed IT teams can develop and implement security measures and even layout a **recovery plan** for probable attacks. The MSP helps the organization stay on top of cybersecurity trends and enables it to counter evolving cyber threats with **full confidence.** An MSP can be your partner in safety and protect you from threats or attacks.

PHISHING & SPEAR PHISHING

Phishing involves sending emails with **malicious attachments designed to steal personal information**. The phishing attack can also lead the victim to an illegitimate website that steals passwords, credit card details, business information, and other sensitive data. A phishing attack uses **technical trickery** and **social engineering** to achieve its goals. Attackers employing phishing choose their targets carefully and take on the guise of a **trusted source that victims are less likely to question.** The attackers also use personalized messages that make the emails look relevant and trustworthy. As a result, SMBs might find it challenging to protect themselves from spear phishing attacks. **Phishing is one of the most common forms of cyber threats.**

From **2022** to **2023**, there was an observed

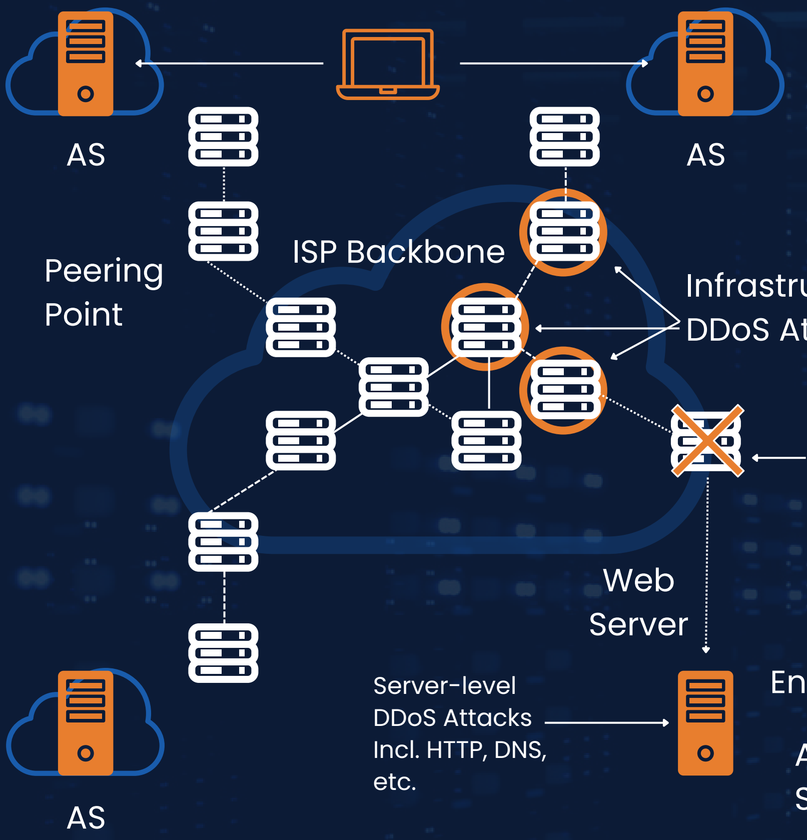
20%

increase in **data breaches.**

	PHISHING	SPEAR PHISHING
APPROACH	Spray & Pray	Targeted Attack
TARGETING	Broad & Automated	Specific employee and/or company
HACKING LEVEL	Not Very Sophisticated	Requires Advanced Techniques
THE ATTACK	Usually Obvious	Harder to Detect
WHAT THEY'RE AFTER	Usernames, Passwords, Credit Card Details, etc.	Confidential Information, Business Secrets, etc.

AVERAGE COST OF A DDOS ATTACK

$20K TO $40K



Hackers Activate Zombies on Innocent Computers

AS

AS

Peering Point

ISP Backbone

Infrastructure-Level DDoS Attacks

Bandwidth-Level DDoS Attacks

Web Server

Server-level DDoS Attacks Incl. HTTP, DNS, etc.

Enterprise

Attacked Server

AS

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Distributed Denial-of-service (DDoS) is an attack that targets the resources of a server, network, website, or computer to **take it down or disrupt services.** DDoS attacks generally have a host system that infects other computers or servers connected to the network. DDoS attacks **overload** a system with constant flooding of connection requests, notifications, traffic. As a result, the system denies service requests by legitimate users. DDoS attacks don't benefit the attacker directly as they don't steal any information: they compromise the systems so that they **can't function properly**. Nonetheless, DDoS attacks can be damaging for businesses as it can **halt operations** and **result in damages worth thousands of dollars.**

Shorter duration DDOS attacks were observed in 2022, with **89%** lasting less than one hour.

jptechnical.com

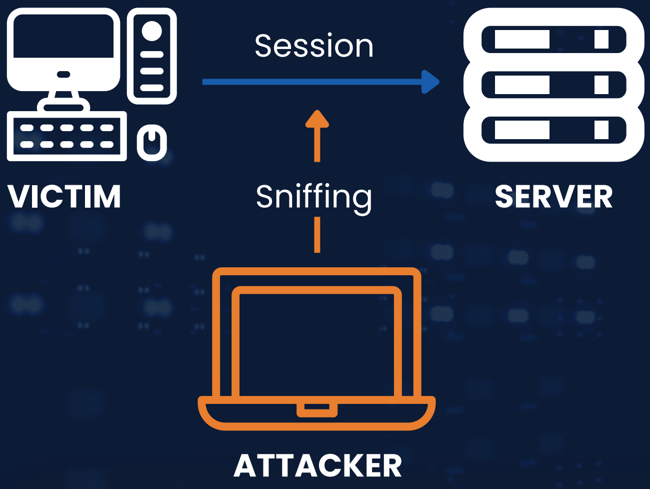
MAN-IN-THE MIDDLE (MitM) ATTACKS

A MitM attack occurs when a hacker inserts themselves between the communications of a **client** and a **server**. Cybercriminals use **session hijacking** to gain control of the victim's sessions and get access to resources or data. The most common method is **IP spoofing**, where the hijacker uses the IP of the trusted client to avail unauthorized services from a server or application.

More than one in four small businesses have no security plan at all.

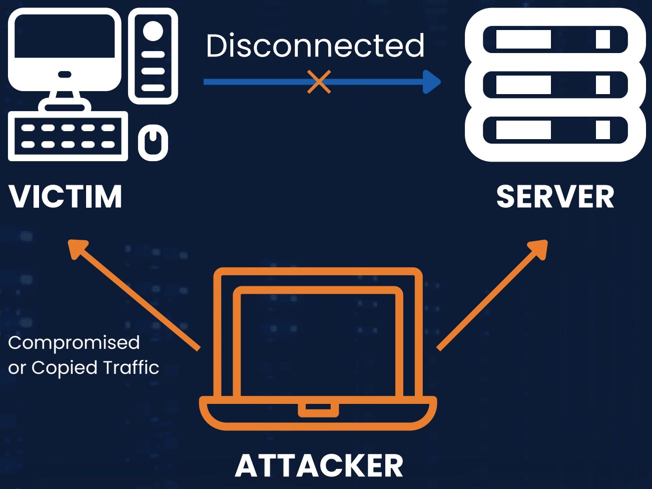
STEP 1

Hijacking the Session



STEP 2

Assuming the Victim's IP Address



95 PERCENT

OF HTTP SERVERS ARE **VULNERABLE**

TO MitM ATTACKS

MALWARE ATTACKS

Malware or malicious software is designed for **compromising a system for a purpose.** A user can unknowingly download malware that infects a system and replicates itself. Malware can be designed to act in many ways, **just like software.**

66 DAYS THE NUMBER OF DAYS TO DISCOVER A CYBERATTACK

600% Increase in Cyber Crime Due to **COVID-19 Pandemic**

Macro viruses

Macro viruses target the **initialization sequence** of an application to compromise programs such as **Microsoft Excel** or **Word**.

Trojans

Non-replicating viruses that gain **unauthorized access** to a system. Trojans often camouflage themselves in the form of **legitimate software.**

System or boot-record infectors

These infectors attach to **executable codes** residing in parts of a disc. Boot record infectors can connect to a hard disk's Master Boot Records and even boot sectors of USB flash drives. **The infectors are initialized when someone boots using the compromised disk or drive.**

Polymorphic viruses

Polymorphic viruses **replicate endlessly to sabotage systems.** They use dynamic encryption keys every time to **avoid detection.**

Stealth viruses

Stealth viruses hide under the **guise of system functions.** They also infect your computer's defenses to **stay undetected.**

File infectors

File infectors find their way in your system through executable codes like **.exe extensions.** The infector becomes active when you **access the .exe file** or the **executable code.**

Logic bombs

Logic bombs are pieces of malicious codes that get initialized when **predefined conditions are met.** Attackers can program logic bombs to serve a range of purposes.

Worms

Worms don't need a host file to propagate themselves on a network or system. **They are self- contained forms of viruses.**

Droppers

Droppers help viruses **find their way into your networks and systems.** Most often, your antivirus will not detect droppers as they don't contain the malicious code: **they just lead to it!**

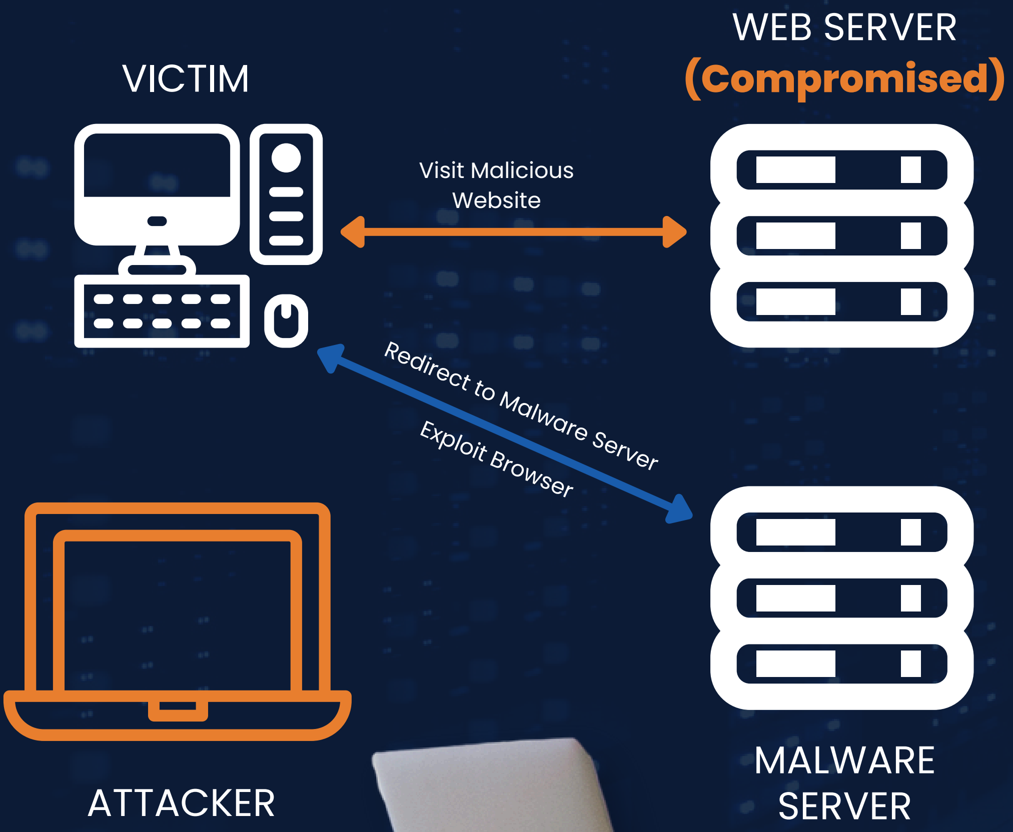
Ransomware

Ransomware can take the form of any virus that **holds a victim's data hostage for ransom.** Ransomware attacks often encrypt data or files and **demand money in exchange for decryption keys.**

DRIVE-BY ATTACKS

Drive-by attacks use **various online resources** to compromise a user's system. The malicious code can be inserted in internet ads, HTTP or PHP codes on websites, or even applications. Contrary to other forms of cyber-attacks, a user doesn't have to do anything to initialize the malicious software or virus. **A single click on a pop-up window or website link can do the job!** Drive-by attacks are increasingly used to spread viruses and malware. The attacks take advantage of **security vulnerabilities** in apps or websites to exploit victim systems. These include not updating the app, flaws in security patches, bugs, and more. The attacks also **run in the background** and are **not visible to the user.** As a result, you can't take any concrete steps to identify incorrect codes. Only being **proactive** can help businesses protect themselves from drive-by attacks.

HALF of all Cyber Attacks Specifically Target **Small Businesses**



WEB SERVER **(Compromised)**

VICTIM

Visit Malicious Website

Redirect to Malware Server

Exploit Browser

ATTACKER

MALWARE SERVER

92 PERCENT

of Malware is **Delivered by Email**

IN **2023,**

98 PERCENT

of organizations had a relationship with a vendor that experienced a data breach **within the last two years.**

PASSWORD ATTACKS

Password attacks enable cybercriminals to gain **unauthorized access** to user accounts and networks. Someone in your office can just guess or look around your desk to steal your password. That's why it's always recommended **not to write down your passwords.** Attackers may also spy on your network, use decryption tools, and use brute force to break your passwords.

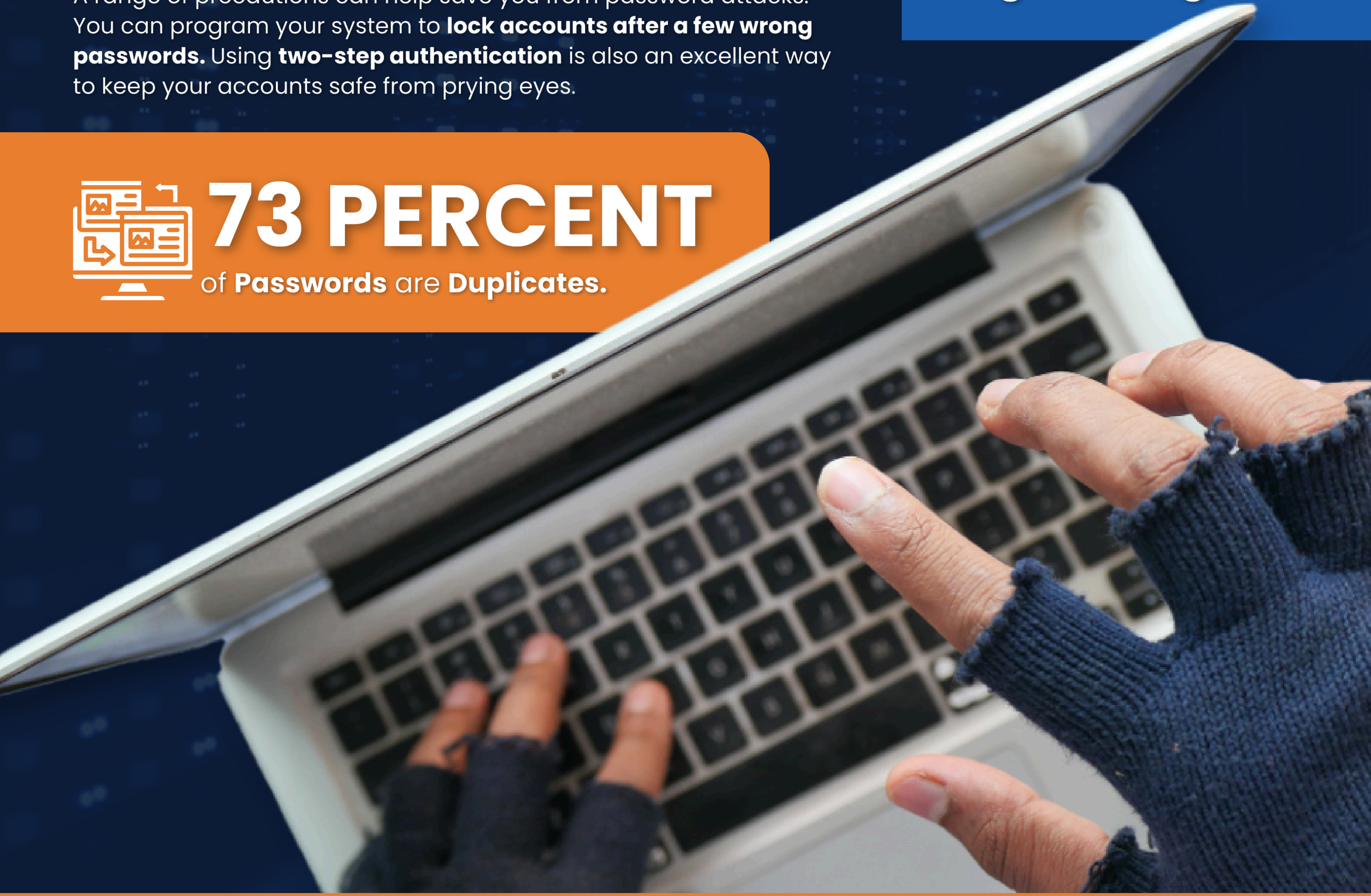
A range of precautions can help save you from password attacks. You can program your system to **lock accounts after a few wrong passwords.** Using **two-step authentication** is also an excellent way to keep your accounts safe from prying eyes.

98 PERCENT

of Cyber Attacks rely on **Social Engineering**

73 PERCENT

of **Passwords** are **Duplicates.**



jptechnical.com

ALASKAS I.T. PROVIDER

JP|TECHNICAL

WE CAN HELP!

We can help you navigate the complicated world of **IT** & **Cybersecurity** so you can better protect your **Data** and your **Business.**

🌐 **jptechnical.com/cybershield**

✉ **cybershield@jptechnical.com**

☎ **(907) 748 2200**

Colter Hobbs
JP Technical

Colter Hobbs

Sources & Attribution:

All statistics are from the following sources unless otherwise mentioned:

- **Harvard Business Review -** Why Data Breaches Spiked in 2023
- **Microsoft Security -** 2022 in review: DDoS attack trends and insights
- **PurpleSec 2021 Cybersecurity Statistics**
- **Verizon 2019 Data Breach Investigations Report**
- **Cyber Rescue Alliance**
- **Cyber Insights of 2021 Report**
- **FBI 2020 IC3 Annual Report**