CYBERSECURITY

THREATS

STG IT CONSULTING GROUP

TABLE OF CONTENTS

INTRODUCTION

It's no secret that our world lives, works, and plays on the internet. But while the internet increases our connectivity, productivity, and efficiency, it also brings numerous threats.

To help your business be prepared and secure for the coming year, STG IT Consulting Group has identified the Top 5 Cybersecurity Threats for businesses in 2021.

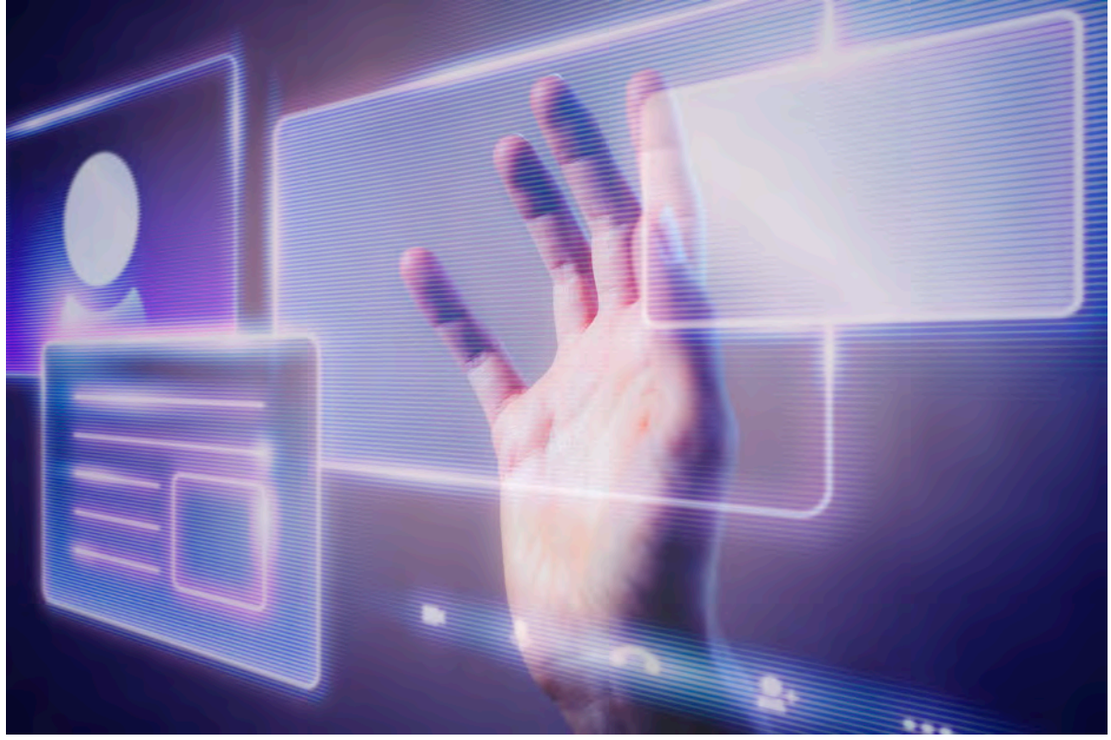
Keep reading to learn all about Phishing Attacks, Malware, Database Exposure, Credential Stuffing, and Accidental Sharing. In each section, we discuss the basics of each threat, as well as provide several practical ways your company can reduce your risk and exposure to these attacks.

Ready to feel confident with your company's cybersecurity?

Let's get started!

THREAT #1:
PHISHING

Phishing is one of the most common cyberattacks due to the high levels of interaction humans have on electronic communication.



In its most basic form, phishing occurs when a hacker uses a false identity to trick someone into providing sensitive information, downloading malware, or visiting a site containing malware.

Most commonly, phishing attacks target people through email.
The attacker's email is designed to look like it comes from your local bank or government, and it'll ask you to visit a website and enter your username and password. The goal is to trick you into logging into a fake online service so the hacker can capture your login details and use them to enter the genuine service later.

A typical phishing attack involves a hacker sending out a malicious email to hundreds of thousands, if not millions of users. Through this, attackers can guarantee that if only 1% of people fall for it, there is a lot of profit to be made by draining accounts.

Additionally, phishing has been around for so long that it's evolved into multiple forms, such as **Spear Phishing, PDF Phishing Scams,** and **Smishing (SMS-Based Phishing)**.

SPEAR PHISHING

Spear Phishing is a more modern and effective version of the traditional phishing attack. Rather than casting out a broad net with the hopes of capturing as many credentials as possible, spear phishing is targeted and precise. The goal is to convince a single business, department, or individual that a fraudulent email or website is genuine.

The attacker focuses on building a relationship and establishing trust with the target. By building trust and convincing the target that they are who they are pretending to be, the user is more likely to open attachments, follow links, or provide sensitive details.

Rather than receiving a suspiciously random email from your government, the malicious email can appear to come from a vendor you deal with regularly. It may even look like an invoice that you're expecting to receive. For example, attackers can simply substitute the vendors' banking details for their own, hoping the target will not notice the difference.

PDF PHISHING SCAMS

Rather than having you open a link to provide sensitive information, PDF Phishing Scams want you to open an attached, malicious PDF.

A typical PDF phishing scam involves an email being sent with a message, often stating a security policy has been updated or an account statement is attached. Although when you open the attached PDF, it exposes you to malware, such as a virus or ransomware.

Traditional phishing attacks have been around for so long; therefore, hackers are aware that people have become wary of emails asking them to click a link. PDF scammers bet on people being more likely to open an attachment as office workers tend to associate PDFs with work and business. If you're expecting to receive your monthly account statement, you might be less likely to confirm that the sender is legitimate.

SMISHING (SMS-BASED PHISHING)

Smishing has the same idea as traditional phishing, but instead of occurring online through emails or web browsing, it occurs through SMS text messaging on your phone.

Many email programs, such as Google or Microsoft Outlook, are smart enough to detect phishing emails and label them as spam. In response to increased email security, many hackers are turning to SMS-based phishing.

While opening the text message itself won't start the attack, the message will contain a link that will begin the attack once opened. Some common examples of smishing attacks are a message appearing to be from your bank asking you to enter your social security number, or your "delivery carrier" asking you to schedule a package delivery.

HOW CAN YOUR COMPANY PROTECT ITSELF FROM PHISHING ATTACKS?

The key to stopping phishing attacks is education. It's crucial to provide your employees with training so they can learn attack techniques, identify the red flags, and send phishing attacks straight to spam.

- Watch out for unusual emails that contain the common signs of phishing attacks:
    - Generic language, such as "Dear Customer" or "Sir/Madam," instead of using your name.
    - Incorrect grammar, language, or punctuation.
    - An odd sense of urgency or unusual request for sensitive information.

- Be cautious clicking links or inputting sensitive information. Always double check URLs: cybercriminals want their links to look legitimate and will often only change one character. When in doubt, contact the business directly to verify they sent the email.

- Same as with links, always double check the sender's email address. For example, if your verified vendor email is johndoe@gmail.com, a hacker might use john_doe@gmail.com.

- Make sure you have virus protection on your computers and network. Additionally, install anti-phishing toolbars for your internet browsers. These toolbars are automated to scan open webpages and alert you to sites containing phishing information.

- Never open a link in a text message. Most banks and businesses do not ask for information via SMS message, they'll call or email.

THREAT #2: MALWARE

Malware is one of the broadest terms when it comes to cyberattacks. It's any malicious form of software designed to harm a computer system.

When malware enters a computer, it performs a malicious function such as stealing, deleting, or encrypting data by hijacking core computer functions, or monitoring a user's activity without their knowledge.

Common malware includes **viruses**, **computer worms**, **adware**, **spyware**, and **ransomware.**

VIRUSES

A computer virus is a form of malware that is installed inadvertently, causing damage to the user. A typical virus may install a keylogger that captures passwords, logins, and bank information from the keyboard. It might steal data, interrupt programs, or cause the computer to crash.

A computer virus is often spread through phishing emails. As mentioned in the above section, always be careful clicking links or downloading attachments that look suspicious or raise a red flag.

COMPUTER WORMS

The computer worm is among the most common type of malware. Worms spread across computer networks by exploiting vulnerabilities within the operating system. Think of your computer as the host and the computer worm as a parasite. These programs cause harm to their host networks by consuming large amounts of network bandwidth, overloading computers, and using up all of the available resources.

One of the key differences between worms and a regular virus is its ability to make copies of itself and spread independently. A virus relies on human activity to run a program or open a malicious attachment; worms can simply spread over the network without human intervention.

ADWARE

Short for advertising-supported software, adware is a type of malware that delivers advertisements to your computer. These advertisements are intrusive, irritating, and designed to trick you into clicking something you don't want. A common example of adware is pop-up ads that appear on many websites and mobile applications.

Adware often comes bundled with "free" versions of software. The software uses the intrusive advertising to make up costs. Additionally, it is commonly installed without the user's knowledge and made excessively difficult to remove.

SPYWARE

Spyware is designed to spy on the user's activity without their knowledge or consent. Often installed in the background, spyware can collect keyboard input, harvest data from the computer, monitor web activity, and more.

Spyware typically requires installation to the computer. For example, users are tricked into installing spyware themselves instead of the software or application that they thought they were getting. Victims of spyware are often completely unaware of its presence until it's too late. They'll only realize it when the stolen data is acted on in the form of fraudulent bank transactions or stolen online accounts.

RANSOMWARE

Ransomware is a particularly malicious variety of malware. It prevents the user from accessing their own files until a ransom is paid. Files within the system are often encrypted with a password that won't be revealed to the user until payment is received.

Instead of accessing the computer as normal, the user is presented with a screen that details the contact and payment information required to access their data again.

Ransomware is typically spread through phishing emails, by downloading malicious file attachments, or a vulnerability in the computer system.

HOW CAN YOUR COMPANY PROTECT ITSELF FROM MALWARE ATTACKS?

- Make sure all of your computer software and hardware is updated. Outdated software, drivers, and other plugins are common security vulnerabilities.

- Enable click-to-play plugins to keep Flash or Java from running unless you click a link. This reduces the risk of running malware programs through Flash or Java.

- Removing old software, sometimes referred to as Legacy Apps, reduces risk. For example, if your computer has Windows 10 but you run programs designed for Windows 7, these are considered Legacy Apps and may be a security risk. In this case, your software company should be able to give you an updated program designed for Windows 10.

- Since malware attacks can spread through phishing emails, refer to the section above for ways your company can protect itself from phishing attacks.

THREAT #3: DATABASE EXPOSURE

A database exposure is exactly what it sounds like: when a security breach exposes database information to hacking or theft. To expose your data, cyber criminals need to hack into your server. They usually gain access through phishing attacks or malware.

Most company databases include customer contact information, financial records, or identity records such as Social Security numbers. Once this confidential information is exposed, it becomes fuel for future cyberattacks.

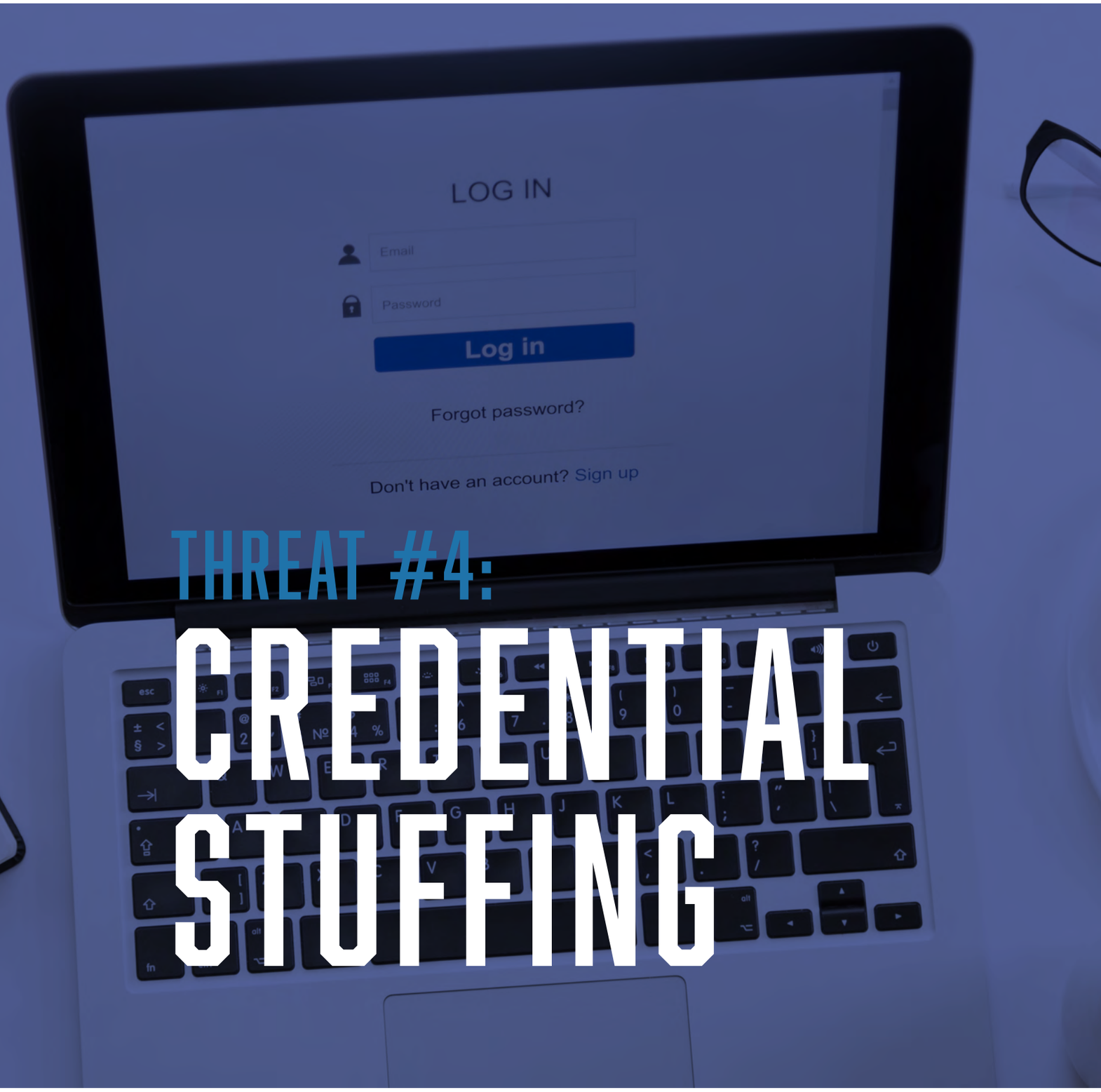
Hackers can send phishing attacks to all of your customers using the stolen contact information. Depending how much personal information is available, a database exposure is a goldmine for spear phishing. Cyber criminals are able to send specific, targeted emails if they have access to personal data.

HOW CAN YOUR COMPANY PROTECT ITSELF FROM DATABASE EXPOSURE?

- To protect your server, make sure you have a database firewall and web application firewall.

- Limit access to your server. Each person with a login to your server is a potential leak. Therefore, the fewer logins, the better.

- To further reduce your risk, encrypt the data on your server and keep a regular backup.



THREAT #4:
CREDENTIAL STUFFING

Credential stuffing is an attack focused on stealing user access through login credentials. This is only possible when the same login credentials are used for multiple websites.

Despite all the warnings, most people use the same password for multiple websites. According to a 2018 Cyclonis Password Security Report, 83.15% of users repeat passwords.

Credential stuffing attacks feed off of this. For example, say you use the same password for all of your social media accounts, as well as your banking accounts. If Facebook is hacked and your password is a part of the data leak, the hackers can use the password to log into your Chase account and steal money.

Additionally, hackers may target small businesses, assuming they don't have strong cybersecurity. They see them as an easy target to use as a stepping-stone to get to the big guys.

HOW CAN YOUR COMPANY PROTECT ITSELF FROM CREDENTIAL STUFFING?

- Implement Two-Factor Authentication for account logins. This requires an email or phone verification along with your standard username and password.

- Use different passwords for every account and program that your business uses. If one account is hacked, the hacker will not have access to more accounts with the same password. We recommend utilizing a password manager to not only securely keep track of all of your passwords, but also suggest complicated and unique passwords for each site or program.

- Never share passwords with others, at least not without the assistance of a password manager. We understand you might have shared accounts with only one log-in that multiple employees need to access, but it's not secure to type out credentials and share them over email or instant messaging. A password manager can securely share passwords across devices and users.

THREAT #5:

ACCIDENTAL SHARING

Accidental sharing is when personal or business data is accidentally shared or leaked through emails, unsecured forms, messaging, social media platforms, or a multitude of other ways.

Accidental sharing is usually a result of human error. Whether you're the one hitting send or on the receiving end; it's something we've all experienced. A classic example is the dreaded "Reply All." Best case scenario, too many people receive your greeting, and it ends up being a harmless mistake. Although, accidental sharing becomes a cybersecurity threat when confidential information, data, or credentials end up in the wrong hands.

HOW CAN YOUR COMPANY PROTECT ITSELF FROM ACCIDENTAL SHARING?

Ultimately, accidental sharing will always be a threat because humans will always make mistakes. With that being said, the following tips can reduce your risk:

- Limit the number of employees that have access to data. Only those who need to have access should. The more people who have access to information, the higher chance for human error in sharing the data.

- Consider implementing user activity monitoring software. This allows you to track and discover if your data is in danger.

CONCLUSION

In a world where the internet connects everything, cybersecurity has never been more critical.

Partner with a Managed IT Service Provider to ensure your business is at the least risk of a cyberattack. An MSP can assess your current cybersecurity efforts and give you proper recommendations to keep your business secure.

STG IT Consulting Group proudly serves Greater Los Angeles and surrounding areas. We invite you to take the next step and schedule a free, 15-minute Zoom or phone call with Stan Kats, Client Engagement Specialist and Senior Technologist.

There is absolutely no commitment and zero obligation; let's just chat and get to know you and your business.

During our meeting, we'll briefly discuss your current IT issues, what you want and need from your technology, and how we can help get you to where you want to be. Stan will assess your current IT infrastructure and answer any questions you may have.

Click here to schedule a time that works best for you.
We look forward to meeting you!