March 2023

TechSage Tech Talk

TechSage Solutions

Insider Tips to Make Your Business Run Faster, Easier and More Profitable

INSIDE THIS ISSUE:

We love technology and We love helping people.

Give me a call to find out whether we can help you better secure your data and get more out of technology.

-John Hill
Founder CEO

Keep Your Business Protected By Becoming Aware Of The Most Common Types Of Cyber-Attacks

The rate of cyber-attacks has significantly increased over the past few years. Businesses of all sizes are at risk of becoming victims of them, which is why it's crucial that every business owner and leader is aware of the most common cyberthreats impacting the business world today. Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals.

These criminals' tactics will improve as technology continues advancing, but cyber security defenses will as well. Knowing exactly what you're up against with cyber-attacks and creating the proper safeguards will protect your business. If you're new to the idea of cyber security or need an update on the common threats that could impact your business, we've got you covered. Below, you will find the most common types of cyber-attacks out there and how to protect your business from them.

Malware

Malware has been around since the dawn of the Internet and has remained a consistent problem. It is any intrusive software developed to steal data and damage or destroy computers and computer systems. Malware is an extensive type of cyber-attack, and many subcategories belong to it, including viruses, spyware, adware and Trojan viruses. One type of malware that has lately been used more frequently is ransomware. Ransomware threatens to publish sensitive information or blocks access to necessary data unless a sum of money is paid to the cybercriminal who developed it.

Unfortunately, malware can be detrimental to nearly every operation of your business, so you should do two essential things to prevent it from affecting your company. First, you should install the latest anti-malware programs. If you hire a services provider, they will take care of this for you. If not, you'll need to find anti-malware that works best for your system. You should also train your team about these risks and ensure they are aware not to click on any suspicious links, websites or files that could be dangerous.

Continued on pg.2

Continued from pg.1

Phishing

Have you ever received an e-mail asking for sensitive information that looked official, but something just wasn't quite right? Chances are it was probably a phishing scam. Phishing occurs when cybercriminals send official-looking messages to individuals, posing as another organization, in an attempt to receive personal information. Falling for a phishing scam can quickly result in you becoming a victim of identity fraud. The results can be substantially worse if a business falls for the scam.

So, how do you best prepare for and protect your team against phishing scams? Utilize employee cyber security trainings so they can spot the warning signs. The actual e-mail will usually line up differently from whom the cybercriminal is trying to represent. Also, most organizations will not request private information over e-mail. Common sense will prevail over phishing scams.

Distributed Denial Of Service

DDoS attacks can bring your business to a standstill. These attacks occur when malicious parties overload servers with user traffic, causing them to lag or shut down since they are unable to handle incoming requests. If your business falls victim to this kind of attack, your employees might not be able to access key functions required to do their jobs, and customers may not be able to use your website or purchase items from you.

> **"Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals."**

DDoS attacks are very difficult to thwart, and a determined cybercriminal can lock up your websites and networks for days on end. You'll have to identify malicious traffic and prevent access before it can cause damage. Hiring an MSP is your best bet to prevent DDoS attacks. If a DDoS attack is successful, you'll probably have to take your servers offline to fix the issue.

Password Attacks

If a cybercriminal gets your password or another employee's password, this is the easiest way for them to access your valuable information. They may attempt to guess the passwords themselves or use a phishing scam to gain access. It is vital that you enable multi-factor authentication for your employees and require complex passwords so you can defend your company against password attacks.

Now that you know the most common forms of cyber-attacks currently happening, you can take the necessary precautions to protect your business, employees and customers.

IT Security is Like an Onion

Cybercrime can cause significant downtime and financial loss for your business. That's why it's essential to have a robust security plan in place. However, it could be a heavy lift on your own.

Partnering with an IT service provider can take a significant load off your shoulders and help you focus on running your business.

To learn how to strengthen your IT environment with layers of protection, **download** our eBook "7 Elements of an Effective Defense in Depth Security Strategy."

www.techsagesolutions.com/7-elements-effective-defense-in-depth-strategy-ebook/

Cartoon Of The Month

Don't you dare open that attachment!
Open it! You know you want to. It's probably a legitimate email.

Shiny New Gadget Of The Month:

PREMIUM TRAVEL POUCH

Tired of digging through your bags to find all the right chargers and cables when you get to your hotel? This high-quality travel pack by SIDE BY SIDE will help you keep your spaghetti jungle under control.

Easily store all your power cables, USB chargers, extension cords, adapters, plugs, hard disks, flash drives etc organized in one place when you are on the move! Search "Side by Side Pouch" on Amazon to see all the models.

COOL WINDOWS 11 FEATURES YOU MIGHT LOVE

Every time Microsoft releases a new Operating System, some people love it and some people hate it.

(although I think we can all agree that everyone hated Windows Vista)

Here are some areas in Microsoft's latest Operation System, Windows 11, that Microsoft has focused on to help you work easier and faster:

- Snap Layouts
- Master Search
- Clipchamp Video Editor
- MS Teams Video, Audio & Text Messaging
- Accessibility Features
- Collections in Microsoft Edge
- Microsoft Defender SmartScreen

You'll also notice they have re-designed and centered the Start Menu / Task Bar, perhaps taking inspiration from Apple's Mac.
Call us today if you want help planning your businesses Windows 11 Roll-out.

The Most Important Word In Business?

It's Not What You Think

A video podcaster recently asked me, "What's the most important mindset for success in business?" For a moment, I doubted I could identify just one key mindset for success. As trusted advisors to CEOs and investors of large companies, our consultants at ghSMART typically emphasize the importance of context. For example, there is no "perfect candidate" to hire for a job. Success depends mostly on a leader fitting a given context, which has many variables – the customer landscape, strategic challenges, operating challenges, financial or legal factors and culture (among other things).

But then it dawned on me. There is one mindset that I have observed in successful versus unsuccessful ventures. The most important word in business, which you rarely hear, is *generosity*.

Leaders who succeed are generous and treat everyone with a fundamental mindset of generosity. In contrast, people who lack a spirit of generosity fail in the long run. Over the years, I've witnessed many examples of both selfishness and generosity. Here are a few lessons you can learn from my own experiences.

(Don't) Trick The Customer: Once, while talking with the CEO of a mortgage company, I instantly got a bad feeling about his character. His mindset was selfish. He implied that his business succeeded by "tricking" low-income homeowners into signing up for mortgages with hidden terms that were unfavorable to them. Well, that mindset backfired. When the housing crisis happened in 2008 and 2009 (caused partly by bad actors like this guy), a pile of lawsuits snuffed out his company and career.

(Do) Create Unexpected Experiences: At ghSMART, one of our colleagues, Alan Foster, expressed an interest in improving his "storytelling" skills. Alan is a charming Brit who leads our UK office. For anybody who knows him, they understand that he's already a fantastic storyteller, but he just wanted to take his game up a notch – to dazzle audiences when he gave talks about leading talented teams. Some other colleagues took the initiative to research opportunities and found an upcoming two-day seminar hosted by a star Hollywood movie screenwriter and master storyteller. They got Alan admission to this exclusive seminar, comped the cost and gave the experience to him as a present. How cool is that? Can you imagine working at a firm where people look for ways to give you what you need or want? As the chairman and founder, I am very happy to see our culture of generosity and gratitude continue to blossom as we grow.

Wall Street's Gordon Gekko may have said, "Greed is good," but a mindset of generosity is better, especially if you want to succeed in your career and live a fulfilling life.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

Happy St. Patrick's Day!

IS THAT A REAL TEXT FROM YOUR CEO? OR A SCAM?

Imagine you're going about your day when suddenly you receive a text from the CEO.

The head of the company is asking for your help. They're out doing customer visits and someone else dropped the ball in providing gift cards.

The CEO needs you to buy six $200 gift cards and text the information right away.

The CEO promises to reimburse you before the end of the day. Oh, and by the way, you won't be able to reach them by phone for the next two hours because they'll be in meetings. One last thing, this is a high priority. They need those gift cards urgently.

Would this kind of request make you pause and wonder? Or would you quickly pull out your credit card to do as the message asked?

A surprising number of employees fall for this gift card scam. There are also many variations. Such as your boss being stuck without gas or some other dire situation that only you can help with.

Without proper training, 32.4% of employees are prone to fall for a phishing scam[1].

Variations of this scam are prevalent and can lead to significant financial losses, both personally and in the business.

In one example[2], a woman from Palos Hills, Illinois lost over $6,000 after getting an email request from who she thought was her company's CEO about purchasing gift cards for the staff.

Need Help with Employee Phishing Awareness Training?

Give us a call today to schedule a training session to shore up your team's defenses.

TIPS FOR AVOIDING COSTLY PHISHING SCAMS

1. Always Double Check Unusual Requests

Despite what a message might say about being unreachable, check in person or by phone anyhow.

If you receive any unusual requests, especially relating to money, verify them.

Contact the sender through other means to make sure it's legitimate.

2. Don't React Emotionally

Scammers often try to get victims to act before they have time to think.

Just a few minutes of sitting back and looking at a message objectively is often all that's needed to realize it's a scam.

Don't react emotionally, instead ask if this seems real or is it out of the ordinary.

3. Get a Second Opinion

Ask a colleague, or better yet, your company's IT Service Provider, to take look at the message.

Getting a second opinion keeps you from reacting right away.

It can save you from making a very costly judgment error and only takes a few extra minutes.

Sources

1. https://itsupplychain.com/ 1-in-3-employees-fall-for- phishing-attacks-without- training/
2. https://abc7chicago.com/ scam-email-fake-boss-from/ 5901884/