TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON CONSULTING & SOLUTIONS

Inside This Issue

March 2023

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

Keep Your Business Protected By Becoming Aware Of The Most Common Types Of Cyberattacks

The rate of cyberattacks 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 cyber threats impacting the business world today. Being aware of common cyber threats 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 to advance, but cyber security defenses will as well. Knowing exactly what you're up against with cyberattacks 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 cyberattacks 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 an 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 service provider, they will take care of this for you. If not, you'll need to find anti

Continued on pg.2

Continued from pg.1

-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.

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 training 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.

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

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.

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 multifactor 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 cyberattacks currently happening, you can take the necessary precautions to protect your business, employees, and customers.

Do's And Don'ts Of Mobile Devices

In the past, mobile phones were just a means of communication via calls. Today, mobile phones have become an inevitable part of everyday life. It is difficult to imagine a world without mobile phones, due to how they have evolved with advanced technology and applications. It's no longer just used for making phone calls; it also serves as a modem, GPS navigator, music player, camera, and lots more. It's been designed to multitask.

With all these advantages, we forget that even mobile phones are just electronic devices that contain data and that we need to be cautious while using them. These overwhelming features and applications even increase the likelihood of freezing of phones, crashes, and so on. Here are a few precautionary measures to keep your mobile phone data safe.

Let's have a look at the mobile phone do's and don'ts listed below:

DO'S:

✓ Keep your phone and apps up to date.

When it comes to the operating system on your mobile phone, you should update your mobile platforms, whether it is iOS, Android, or Windows, to their latest versions. It is not only important that the platform is continuously updated, but also the apps you are using on the phone. This would avoid the compatibility issues that lead to constant crashes, timeouts, outdated interfaces, etc. Therefore, it's essential to have updated platforms and applications.

✓ Defend your phone against malware.

Phones are most susceptible to getting infected with malicious software like malware, virus infections, etc. These programs hide in a seemingly harmless app, such as a ringtone or game, but contain hidden code designed to exploit or damage your mobile device; running the app unleashes the malware on your phone. Know exactly what you are installing on your phone and avoid downloading apps from sources you are unfamiliar with.

✓ Turn off your Bluetooth.

If your phone works with Bluetooth technology or NFC standards that support mobile wallets, turn them off when you are not using them. This will block the unwanted downloads and prevent the intruders from accessing the data stored on your phone.

✓ Encrypt all your sensitive information.

If your phone includes data encryption features, do not neglect them; just use them. If your phone is stolen, offenders will not be able to access any personal information that's stored on your phone if your data is encrypted.

✓ Secure your device with a pin or password.

When it comes to security, ensure your mobile device is enabled with a password, screen lock, or pin to ensure protection from unwanted access to your device and support the encryption of sensitive data. Use of a pattern lock is available on some phone models, but security experts recommend a pin or password as the securest method for mobile phone security.

✓ Enable Remote Wipe feature.

Many phone vendors support a remote wipe feature that allows the device to be remotely wiped or erased in the event the phone is lost or stolen. Review the information provided by your phone vendor to register your device and enable the remote wipe or erase capabilities of your device. This will assist in being able to securely erase information on your phone, including all personal information, applications, and financial information, while still having the device registered in your name. Should the device be found or returned, restore from a backup to gain functionality back to the device.

DON'TS:

✗ Don't go overboard with animations.

While the animations can be entertaining and add a flair of simplicity to your mobile phones, they delay the access time. This is because the animations technically can't begin until the mobile device is loaded. For example, think of any website that is fancy and professional-looking, but it requires you to wait a few seconds to load all animations and to access the website you're visiting.

That's what happens when you have too many animations on your mobile device; it makes it run slow. Keep it as simple as possible.

✗ Don't download too many addictive apps.

Regardless of the plethora of apps available, it doesn't mean that you should download them all. Most of the apps will be useless and just eat up your mobile memory. In some instances, you might download some malicious tools by thinking of them as apps. As a result, be cautious when downloading apps and only install those that you really need.

✗ Don't run your mobile when battery is low.

Keep checking your mobile battery's power. Don't allow your mobile phone battery to go below 30%. Using the phone to take pictures or transfer data while your battery is low will just lead to the loss or corruption of your data on the phone. Just make sure your phone is fully charged before you use it. It's advisable to switch off your phone when not in use; that saves battery power.

✗ Don't jailbreak your mobile phone.

Most phones only run software recognized by their operating systems. Jailbreaking or unlocking your mobile phone will enable it to execute untrusted software, which might carry a harmful virus. Always try downloading apps only from major app stores like the Windows Phone Store, Apple App Store, and Google Play Store.

With the help of the above-explained tips, one can easily operate and secure their mobile phones from unexpected disasters such as freezing, virus infections, or data loss. Your negligence while using the phone might cause a blunder, and you may lose all your important information.

2 Selling Strategies Your Business Should Avoid

In the world of business, there are good and bad selling strategies. Strong selling strategies bring your customers back for more and encourage them to refer their friends and family. In contrast, poor strategies will send your customers running for the hills.

They'll never look back at your business and will tell everyone about their negative experiences. If you or your sales team are utilizing any of the following strategies when selling to customers, you should put a stop to it immediately, or your sales will begin to decline.

Not Addressing The Customer's Main Problem

When customers approach you for a specific product or service, they most likely have a reason for coming. Listen to your customers' concerns rather than overexplaining your product or service. If you provide a solution to their problem, you'll likely earn a sale.

Arguing With Customers

Has a customer ever said something unreasonable or completely wrong about your product? You might have been quickly defensive, but starting an argument with a customer will never lead to a sale, even if you're right. Listen to them and figure out where they're coming from before responding.

Become A Better Business Leader By Ditching These Habits

You want to be the best leader possible if you own or operate a business, but you may have developed habits over the years that are preventing you from being your best. As you grow in your role, you must overcome habits and certain ways of thinking that might impede your progress. If you're utilizing any of the following habits, it's time to change the way you're approaching things.

Black-And-White Thinking

There is plenty of gray in the world of business. You can't look at things as being one way or another. There are many different ways to approach each problem.

Your Opinion Matters More

You must listen to your team if you hope to be a great leader. You won't be right with every decision. Hear suggestions from your team and make an informed choice in order to determine the best path for your business.

Want To Improve Your Business?

Track These 2 Key Performance Indicators

Many businesses determine their level of success by looking at specific key performance indicators. Some popular KPIs include tracking revenue, customer satisfaction, lead generation, and client retention rate. But not everyone knows there are several other KPIs worth checking out for their businesses. Below are two KPIs your business should track if you aren't already.

Contact To Customer Conversion Rate: How many times does your team have to reach out to a potential customer before making a sale? The fewer touches your team has before a sale, the better their approach may be.

Churn: How many customers do you lose each month? By tracking this KPI, you'll recognize when customers are dropping off so you can make the necessary adjustments to keep them.