

Security Update

Should You Allow Guests To Access Your WiFi Network?

Do you have guest access on your company WiFi network? Or do you simply give out the same password that your employees use? If you give out your password, you're practically opening the door for anyone to come in and steal private information, infect your private computers and even steal customer credit card data if you are processing them over the same Internet connection.

The key to providing free guest WiFi access is in segregation and security. Your WiFi guests need to be completely isolated and segregated from your private network (something we can do for you). Your guests should not be able to reach your internal computer network, credit card terminals or other network-connected devices.

Don't know how to enable guest WiFi access? Give us a call and we'll help you out.

March 2023



This monthly publication provided courtesy of Tom Crossley President of Fairoaks IT

"As a business owner, you don't have time to waste on technical and security issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Tom Crossley



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 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.

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.

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

Continued on pg.2

Continued from pg.1

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 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.

“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 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 cyber-attacks currently happening, you can take the necessary precautions to protect your business, employees and customers.

Free Report Download: I.T. Buyers Guide What You Should Expect To Pay For IT Support For Your Business



You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.FairoaksIT.com/ITbuyersguide

**Get More Free Tips, Tools and Services at:
www.FairoaksIT.com (774) 222-5500**

Be Sure To Visit The Fairoaks IT Team At Booth 508



The Westin Boston Seaport District 425 Summer Street Boston MA 02210
 Event Link <https://www.thesmallbusinessexpo.com/city/boston/>

News Corp Cyberattack

News Corporation (News Corp) has disclosed more information about the 2022 cyberattack against the major publishing conglomerate. News Corp revealed that the cybercriminals had access to its systems two years ago, starting in Feb. 2020.

News Corp recently sent notification letters to affected employees. These laid out the most recent information on the data breach. The breach affected workers at the company's publications, The New York Post and The Wall Street Journal, and its UK news operations.

The Dates of the Breach and Affected Information

Hackers accessed News Corp data from Feb. 2020 to Jan. 2022. News Corp discovered the breach on Jan. 20, 2022, and took immediate action.

The breach allowed attackers access to emails and business documents from limited personnel. Although the attackers accessed personal details, this doesn't seem to be their goal. There are no reports of identity fraud from the breach.

The attackers may have accessed the following employee information:

- Names
- Birthdates
- Driver's license number
- Social security number
- Passport number
- Medical information
- Health insurance information
- Financial account information



How News Corp Reacted

News Corp immediately hired cybersecurity firm Mandiant to investigate the breach. The company also contained the activity.

News Corp has also arranged 24 months of Experian credit monitoring and identity protection. This comes at no cost to the employees. It covers identity theft insurance, credit monitoring, and identity restoration.

Final Thoughts

This type of data breach is becoming common. If it can affect a company as large as News Corp, then business owners should take it seriously. Be proactive with prevention and monitoring to catch potential breaches or malware early. This is essential to protecting you and your customers. It will also help maintain the reputation of your business. Even small business owners should take steps to protect themselves and their clients from data breaches.

Fairoaks IT Tech Heroes



We Love Feedback From Our Clients!

Steve always fixes the problem
quickly and efficiently!
March 8, 2023

"Very speedy
response."
March 10, 2023

"Paul intercepted spyware, cleansed and
flushed the intruder down the drain. A well
done and ultra fast response."
March 9, 2023

TJ is always great at communicating and letting
me know what she was doing and if there was
anything that was taking a bit longer than
expected. Great experience overall!
March 7, 2023

"As always this was a wonderful experience with
a knowledgeable and experienced technician.
We love working with you guys!"
March 7, 2023



Tom Recommends: Digital Spring Cleaning

Overview

We often hear of the term "spring cleaning," the time of year when we go through our belongings and organize our house and lives in preparation for the upcoming summer. This is also the perfect time to take an annual review of your digital life. The following seven simple steps, taken once a year, will go a long way toward ensuring you can make the most of technology, safely and securely.

ACCOUNTS:

Review each of your accounts. Using a long, unique password for each account ensures that if one account is compromised, your other accounts are still safe. Can't remember all those different passwords? Don't worry, neither can we. We recommend you use a password manager to securely store all your passwords and make your life far simpler and more secure. Enable multi-factor authentication (MFA) when possible, especially for your personal email or financial accounts. This is the single most important step you can take to secure any online account. If you have any online accounts, you have not accessed in over a year, it could be time to simply delete them.

PROGRAMS:

Keeping your devices and software updated and current ensures you have the latest security features installed and known vulnerabilities are fixed. The simplest way to do this is to make sure you have automatic updating enabled on all your computers, mobile devices, and even smart home devices. Also, delete any unused programs or apps on your mobile devices and computers. Some apps require large amounts of storage, can introduce new vulnerabilities, and may even slow things down. The fewer apps you have, the more secure your system and your information remains. Many devices show you how long it has been since you've used an app. If it has been a year since you last used the app, chances are you don't need it anymore.

FINANCES:

Verify that your bank accounts, credit card accounts, investments, and retirement accounts are configured to alert you whenever a transaction is made, especially for unusual signs, large purchases, or money transfers. This will make it so you

can spot any fraud or unauthorized activity right away. The sooner you identify fraudulent activity, the sooner you can stop it and the more likely you can recover your money. Depending on which country you live in, an additional step you can take is to implement a credit freeze, which can be one of the most effective ways to protect your identity.

DISPOSING OF DEVICES:

Over time you may find yourself collecting old devices you no longer need - perhaps an old smartphone or smart home device. If you dispose of any of these devices, first wipe any personal information from them. Most devices have a simple wiping function that securely purges all personal information (or reset to factory default) before disposing of the device.

BACKUPS:

No matter how safe or secure you are, at some point you will most likely need backups to recover your important information or migrate your information to a new device. Set your devices to automatically back up to the cloud. Creating and scheduling automatic backups allows you to recover your most important information.

PARENTING:

If you are a parent or guardian, this is a good time to review any parental controls settings you have in place for children. As children get older, you will most likely need to update these controls settings.

SOCIAL MEDIA: Review privacy settings on your social media accounts - these are a goldmine of personal information. Review your accounts to check that you are not sharing sensitive information such as your birthday, phone number, home address, banking information, or geo-location in personal photos.

Spending just a couple hours a year taking these steps will go a long way toward protecting you, your devices, and information.

Subscribe to OUCH! And receive the latest security tips in your email every month - www.sans.org/ouch.

Shiny New Gadget Of The Month:



Valve's Steam Deck

Nintendo, Microsoft and Sony are some of the most prominent players in the video game console industry, but there's another name making headlines in these console wars: Valve's Steam Deck. In fact, this is the perfect gaming system for anyone who is looking for a powerful and portable console.

The handheld system is capable of playing the most advanced AAA games available and comes in three different storage sizes. If you've used Steam in the past on your PC, you'll immediately gain access to your library of games and will be able to purchase any other games from Steam directly on the device. Check out the Steam Deck if you're in the market for an affordable, powerful and portable gaming PC.

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 the chairman and 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.

Do you know anyone we can help?

We **LOVE** our clients and we want more like you! If you know of any business owners that could benefit from one or more of our services, we would appreciate an introduction. I promise we will treat them with kid gloves! Or You can just drop us an introduction email :

Sales@FairoaksIT.com

Fairoaks **IT**

*You Manage Your Business.
We'll Manage the Technology Behind It.*

1000 Franklin Village Drive - Suite 303 Franklin, MA 02038

Inside This Issue:

Keep Your Business Protected By Becoming Aware
of The Most Common Types Of Cyber-Attacks 1 | 2

SBE Trade Show - Boston | 3

News Corp Cyberattack | 3

Digital spring Cleaning | 4

The Important Word In Business? | 5

2 Selling Strategies Your Business Should Avoid | 6

Become A Better Business Leader By Ditching These
Habits | 6

■ 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 selling 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.



© D. Fletcher for CloudTweaks.com