

## Security Update

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.


### April 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



## Understanding Cyber Security Compliance Standards

There is an endless number of things a business owner should do for their business to be successful. They must develop a product or service that can attract customers, hire and train a team to oversee day-to-day operations, implement marketing strategies and so much more. While all these tasks are essential for your business to be profitable, your business will never get off the ground if you aren't compliant with standards that affect your industry.

Compliance standards are guidelines or rules that organizations must follow to meet legal, regulatory or industry requirements. These standards are designed to ensure organizations ethically conduct business - by protecting the rights and interests of their customers, employees and other stakeholders. When an organization does not maintain its compliance standards, it will be met with fines, legal action and other penalties.

Many compliance standards that apply to most organizations involve sensitive information protection. Here are a few examples.

### National Institute Of Standards And Technology (NIST)

The NIST is a nonregulatory agency of the United States Department of Commerce that promotes innovation and industrial competitiveness. As a business leader, you must be aware of the various cyber security standards and guidelines set by the NIST. One such standard is the NIST Cyber Security Framework, a voluntary framework that provides a way for organizations to better manage and reduce cyber security risks. It's built on the following five core functions:

- **Identify**

It's vital to understand the organization's cyber-security risks, assets, and the people responsible for them.

- **Protect**

Implementing the necessary safeguards to protect Organization's assets from cyberthreats can shield companies from increasing risks.

- **Detect**

It's important to detect when a sec-

*Continued on pg.2*

Continued from pg.1

- **Respond**  
By responding to security incidents as they occur and containing the incidents, people can eradicate the threat and recover from it.
- **Recover**  
After a security incident does occur, organizations must know how to restore normal operations as well as their systems and data. This process often helps people understand the importance of implementing safeguards to ensure similar incidents do not occur in the future.

### Health Insurance Portability And Accountability Act (HIPAA)

The compliance standards set by HIPAA are some of the most well-known as they pertain to protecting personal health information (PHI) in the United States. HIPAA requires covered entities, such as health care providers and health plans, to ensure the privacy and security of PHI. The Security Rule and the Privacy Rule are the two main sets of regulations under HIPAA that covered entities and their business associates must follow. The Security Rule sets standards for protecting the confidentiality, integrity and

availability of electronic PHI and requires covered entities and business associates to implement certain administrative, physical and technical safeguards. On the other hand, the Privacy Rule sets standards for the use and disclosure of PHI and gives individuals certain rights concerning their PHI – such as the right to access their PHI and the right to request their PHI be amended. Failure to comply with HIPAA can lead to significant financial penalties, reputational damage and, in some cases, the loss of a license to practice medicine.

### Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a relatively new set of compliance standards developed by the Department of Defense to protect Controlled Unclassified Information. The CMMC is mandatory for all DoD contractors and subcontractors that handle CUI. This is a tiered certification system with five levels of maturity. Each level has a specific set of practices and processes that organizations must implement to achieve certification. As a business leader, you should be aware of the CMMC and the specific level your organization will need to achieve to comply with the DoD contract requirement. CMMC certification is audited and managed by a third party. Keep in mind that getting this certification will take ample time and effort. You'll need to implement robust security protocols and practices that may not have been in place before.

These are just a few compliance standards that may be required in your industry. Complying with these standards will help protect your business, customers and employees.

**“Your business will never get off the ground if you aren't compliant with standards that affect your industry.”**

## Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo And Target Did?



If the answer is “NO” – and let's be honest, the answer is no – you are leaving yourself and your company open to massive liability, *millions* in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time before they destroy your business, scare away your customers and ruin your professional and personal life.

### Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers. *Reserve your exclusive CEO Dark Web Scan now!*

**Get your free Dark Web Scan TODAY**  
**[www.FairoaksIT.com/DarkWebScan](http://www.FairoaksIT.com/DarkWebScan)**

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

## Elementor Pro's Security Issue: How It Impacts Business Owners

Elementor Pro is a popular website builder plug-in among WordPress users. Over 11 million websites use it to access professional themes, customize elements, and design forms. However, researchers have discovered some security issues with the extension that users should be wary of.

### The Possible Risks of Elementor Pro's Security Flaw

Elementor Pro's security flaw allows authenticated users to set up an administrator account. Unfortunately, that means unauthorized people can take over the site and perform malicious acts. For example, they can enable the registration page, switch their role to administrator, and gain various privileges.

Threat actors are using the flaw to divert traffic to a malicious website. This vulnerability exists because of faulty access control on Elementor Pro's WooCommerce module. Cybersecurity company NinTechNet was the first to uncover the vulnerability in March 2023.

According to PatchSack, threat actors use the flaw for backdoor attacks. They upload malicious content to comprom-

ised sites such as wprate.php, III.dip, and wpresortpack.zip. The WordPresssecurity firm says it sees attacks from several IP addresses.

It is not Elementor Pro's first high-severity security issue. In April 2022, cybersecurity researchers at Wordfence identified a flaw that lets authenticated users transfer arbitrary PHP code. It was a new Onboarding module that opened the vulnerability.

Elementor Pro Users Should Upgrade to the Latest Version

Elementor Pro's current security flaw has a vulnerability rating of 8.8 out of 10. That earns it a critical status. Older versions of the plug-in are at greater risk for malicious attempts. Users should upgrade to Elementor Pro 3.11.7 or later as soon as possible to mitigate risks. The improved security code provides better protection of user data against hackers.

Protect Your Website from Cybersecurity Threats

Business owners must be vigilant about the platforms they use for their online operations. The Elementor Pro security issue proves that even a seemingly harmless plug-in can be the gateway to



malicious attacks. Do research before using any software and check for past security lapses.

Also, always upgrade to the latest versions to ensure maximum protection for your data.

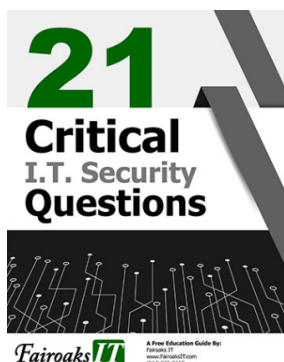
Lastly, have security measures in place to mitigate risks. That includes creating data backups, installing firewalls, and using strong passwords. Business owners must also conduct regular cybersecurity training for their employees.

*\*Used with permission from Article Aggregator*

## IT Support For Eastern Massachusetts And Rhode Island

### Are You Ready To Put An End To Expensive, Frustrating Computer Problems Finally and Forever?

If so, call us today at, 774-222-5500 and we'll show you how we can make your computer problems go away finally and forever!



### FREE GUIDE

21 Critical Questions Your IT Consultant Should Be Able To Say "Yes" To



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



## Fairoaks IT Tech Heroes



"Usual EXCELLENCE!"  
April 6, 2023

"Sam was terrific!"  
April 21, 2023

"Quick service. Great interaction to  
solve the problem."  
April 21, 2023

Quick service. Great  
interaction to solve problem.  
April 21, 2023

"Great service, turned out to be a  
simple fix for an IT guy, not so  
much for a cave man. :)"  
April 4, 2023

"Excellent support as  
usual."  
April 22, 2023

## Tom Recommends: Scareware: A Story



Warning! Your computer is infected with Black Basta ransomware. Call this phone number right away to fix your computer! - If you saw this warning pop-up on your computer, would you call the phone number?

### The Attack

After thirty years of working hard, Deborah had saved enough money to retire with her husband. Wanting to review her retirement accounts, she typed in the name of her bank into her browser. What she did not realize is she had mistyped the bank name, taking her to a different website that immediately displayed a scary warning banner that claimed her computer was infected and instructed her to call tech support immediately. The pop-up warning was very professional. It detailed which malware infected her computer, had an official company logo, and provided an emergency number for her to call.

Deborah immediately called the number, which was answered by a seemingly professional support agent. The agent explained that her computer was indeed infected and that they needed access to her computer to fix it. She had to visit a specific website, download their security software, and then install it. She did as requested and the support agent informed her they had access, after which they started searching her computer.

Soon they confirmed her worst fears, not only was her computer infected, but it appeared her bank account had been broken into. Fortunately, the tech support company had a direct connection with her bank, and they quickly transferred her to a fraud agent. The fraud agent confirmed her account was indeed compromised and was being used to transfer fraudulent funds. They told her to immediately transfer all of her money into a different bank account to protect it. Deborah did as instructed. They then informed her that her retirement account was also compromised. Fortunately, they also had a partnership with the government tax agency. She was then connected to a government agent who explained that to secure her retirement account, she needed to cash in her life savings and move it to another account before criminals were able to access all of it. She did this.

It was a long and terribly emotional night, but Deborah was glad to not only have fixed her computer but saved all of her money by moving it to new, safe accounts. She went to bed exhausted.

The next morning, she logged into her new bank account to access her recently moved savings and retirement accounts, but all the money was gone. In a panic she called the tech support number she had called yesterday. There was no answer. She soon realized her entire life savings was gone. She had just given it away.

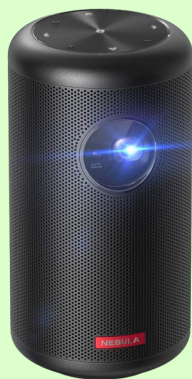
### How to Avoid This Happening to You

Cyber criminals have learned that the easiest way to infect your computer or steal your money is to simply ask. Scareware is a common way they do this - by tricking you into thinking your computer is infected when it's really not. They then rush you into taking hasty actions so they can take advantage of you. This story is based on real events that happened to real people. Deborah's computer was never infected, instead she accidentally visited the wrong website. The tech support company was not a real company, but a team of cyber criminals half-way around the world. Even the bank fraud and government agents were just different members of the same cyber criminal team. Once cyber criminals get you on the phone, they will try anything possible to make money. So how can you protect yourself?

- Being suspicious is your best defense. Any time someone is trying to rush you into taking an action, it may be an attack. The greater the sense of urgency and the more they are pressuring you, the more likely it is a scam.
- No legitimate company will ever ask you for your password. No bank is going to ask you to move your money.
- Never use contact information provided in an alert or pop-up. If you want to check the legitimacy of an alert, always use contact methods that you already know, such as phone numbers on your bank statements or credit cards or use links bookmarked in your browser.

Subscribe to OUCH! And receive the latest security tips in your email every month - [www.sans.org/ouch](http://www.sans.org/ouch).

## Shiny New Gadget Of The Month:



### Anker NEBULA Capsule II Smart Portable Projector

There's nothing quite like watching your favorite movie under the stars. Now, doing so has become easier with the Anker NEBULA Capsule II Smart Portable Projector. This projector is great for indoor and outdoor use since it has a great picture and built-in speakers. It runs on Android TV 9.0, which allows you to access a wide range of streaming services - Hulu, YouTube and more - without needing an external device. This projector is as portable as it gets since the NEBULA Capsule II is only the size of a soda can. It is the perfect device for any situation, whether you're going camping, hosting an outdoor party or simply want a large screen for video games or movies.

## How Recessions Benefit Great Companies

Recessions are bad for most people, and I won't make light of how horrible these times can be for the vast majority of companies and their employees. It's true that for most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, raised board and shareholder pressure, increased financial strain and extreme anxiety. It's no fun to wake up to that every day! But for great companies, people can turn things around and make recessions awesome.

So, what are great companies? They're the ones that make great products or deliver exceptional services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take good care of their customers and employees, great companies don't have a dangerous debt burden. They are profitable, can pay their bills to suppliers and deliver an attractive return to investors in dividends and equity appreciation.

Recessions are awesome for certain companies for the following reasons.

### Losing The Cobwebs Of Complacency

"Success breeds complacency." Andy Grove, the legendary CEO of Intel, wrote that. And while I'm not here to suggest everybody embrace full-on "pania" in the workplace, I am suggesting that successful companies must keep hustling to stay on top. A recession provides an opportunity for a wake-up call to companies that may otherwise start coasting. Now is the time for them to get back on track.

### Taking Customers And Colleagues From Undeserving Companies

I'm not sure why customers buy products or services from lesser companies. And I'm not sure why talented people work at lesser companies. Maybe it's due to convenience, connections or just habit. In any case, as lesser companies stumble during a recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more of these customers and talented people.

### Increasing The Rate Of Learning For Your Leaders

I don't know about you, but time seems to move more quickly for me during harder times than when things seem easy. This can enhance the learning curve of your up-and-coming leaders. Just remember not to make too many decisions for them that will stunt their growth. Allow your leaders to come to you with problems and solutions so you can aptly coach and support them. Let them test and learn various approaches to leading through uncertain times.

If you buy from a lesser company or work at one, the next recession is likely to be a bummer for a couple of years. But if you work at a great company, fear not. This will be an awesome opportunity to shake loose some cobwebs of complacency, take customers and colleagues away from lesser companies and increase the rate of learning of your leaders.



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 bestsellers. 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

*You Manage Your Business.*

*We'll Manage the Technology Behind It.*

1000 Franklin Village Drive - Suite 303 Franklin, MA 02038

## Inside This Issue:

Understanding Cyber Security Compliance Standards  
1-2

Elementor Pro's Security Issue: How It Impacts  
Business Owners | 3

Scareware: A Story | 4

How Recessions Benefit Great Companies | 5

Let Your Employees Know You Care With  
These 3 Tactics | 6

Are You Micromanaging Your Team? | 6

## ■ Let Your Employees Know You Care With These 3 Tactics

If an employee is unhappy working for your company or doesn't feel appreciated by their leadership team, they will search for a new job. This has left many leaders questioning what they can do to show their employees they actually care about them and their well-being. Here are a few different ways to show your team you care.

### Growth Opportunities

Most employees want to work somewhere with the potential for advancement. It's important to connect with your employees through one-on-one meetings so you can determine how they want to grow professionally and personally.

### Foster A Supportive Work Environment

Nobody wants to work at a business where they don't feel accepted, supported or appreciated. Go out of your way to create an inclusive environment and give your team a sense of belonging.

### Recognition

your employees want to hear about it when they do well. Don't be afraid to recognize or reward them when they're doing a great job. Simply thanking your employees for their hard work can go a long way toward improving overall morale.

## ■ Are You Micromanaging Your Team?

There are many different management styles, but one that always seems to upset employees and take away from productivity is the act of micromanaging or over-coaching.

Micromanaging occurs when a leader provides instructions that are too specific while watching over the team as they perform their tasks, looking for any lapse in perfection they can then bring up to the employee. It's a frustrating practice that can send well-qualified employees running out your doors. So, how do you know if you're micromanaging your team? Pay attention to how you're directing them. You won't get a preferred response if you tell your billing manager how to do their job. You hired these employees to perform specific roles, and they have the experience to do it well. So, let them work until there's a need to redirect or re-analyze the situation. Ask for feedback when you conduct one-on-one meetings with your team. Listen and make the necessary adjustments if they say you're micromanaging. This will help boost productivity in your business while you still get the most from your team.



"Production has really picked up since we installed the coffee pots."