onestep
Secure IT Services

The Latest Byte

YOUR IT & SECURITY ALL-STAR TEAM

Vol. 4 | 2023

onestep
Secure IT Services

THIS QUARTER'S LATEST BYTE

What's more vital to success than a strong team?

Protecting your business from cyber attacks and IT issues that cause downtime and productivity issues is no small feat. It takes a team of experts to guard your digital assets, ensuring your business stays strong.

Having a knowledgeable and experienced group of IT and security experts can be the difference between bouncing back quickly after a cyber attack and the worst-case scenario—closing shop.

Unfortunately, that worst-case scenario happens more often than you'd think—a staggering 60% of businesses hit by cyber attacks shut down within six months.

At One Step Secure IT, we're more than just a service provider; we are your trusted teammates. Our team of IT and security experts is dedicated to safeguarding the business you've built.

Together, we'll tackle digital challenges head-on, emerging even more resilient than before.

Don't forget to listen to the latest episode of the *One Step Beyond Cyber* Podcast!

About One Step Secure IT

We are an outsourced IT company with over three decades of protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Our expertise includes Cybersecurity, Managed and Co-Managed IT, Information Security, and Compliance Services.

We understand that as business operations evolve, so do the security threats. Our expert team collaborates closely with you to create a customized IT strategy, identify vulnerabilities, and strengthen your IT infrastructure.

Our corporate headquarters are located in Phoenix, AZ, and we proudly serve businesses across the nation. To learn more about how One Step Secure IT can help protect your company from cyber threats and increase productivity, visit our website at **www.onestepsecureit.com**

ONE STEP SECURE IT TEAM

Out on the Field

From coast to coast, the One Step Secure IT team has taken great pride in the opportunity to shed light on the importance of data security.

Our security and technology experts have been busy meeting business professionals looking to protect their customer data and company assets.

As they continue to venture into the field, our One Step Secure IT Team is committed to helping businesses with education, tech, and strategies that pack a punch!

We hope to see you at the One Step Secure IT booth in your city.

meet ONE STEP'S IT & SECURITY TEAM

30 tim DERRICKSON

HOMETOWN: Fountain Hills, AZ

JOB TITLE: Director of IT & Security Services

EDUCATION/CERTIFICATIONS
U.S. Navy Veteran, A+, CISSP

FAVORITE SECURITY TOOL
My mind.

QUOTE/MOTTO: Life is short, don't stay on the sidelines.

67 roman STANTON

HOMETOWN: Dallas, Texas

JOB TITLE: vCIO & Compliance Specialist

EDUCATION/CERTIFICATIONS
20+ Years of IT

FAVORITE SECURITY TOOL
Knowledge

QUOTE/MOTTO:
If you're happy and you know it, then your face will surely show it.

75 **trystan HAYDEN**

HOMETOWN: Ingleside, Texas

JOB TITLE: Network Administrator

EDUCATION/CERTIFICATIONS
A+, AMT, Microsoft 365 Certified: Modern Desktop Administrator Associate

FAVORITE SECURITY TOOL
Education of End Users

QUOTE/MOTTO:
It is a blessing for a man to have a hand in determining his own fate.

89 **john COLLINS**

HOMETOWN: Phoenix, AZ

JOB TITLE: Network Administrator

EDUCATION/CERTIFICATIONS
CAD Institute

FAVORITE SECURITY TOOL
ThreatLocker

QUOTE/MOTTO:
You never fail until you stop trying.

Securing your business for over 3 decades!

38 justin KREISBERG

HOMETOWN: Northridge, CA
JOB TITLE: Network Administrator

EDUCATION/CERTIFICATIONS
University of Arizona/BA in Management Information Systems (MIS) and Operations, and Supply Chain Management

FAVORITE SECURITY TOOL
Pen Testing

QUOTE/MOTTO:
The moment you give up, is the moment you let somebody else win.
-Kobe Bryant

55 sean NICKOLOFF

HOMETOWN: Denver, CO
JOB TITLE: Network Administrator

EDUCATION/CERTIFICATIONS
15+ Years of IT / Microsoft 365 Modern Desktop Administrator Certified

FAVORITE SECURITY TOOL
ThreatLocker

QUOTE/MOTTO:
You will face many defeats in life, but never let yourself be defeated.
-Maya Angelou

Empower your Business with One Step's IT & Security *All-Stars!*

Discover how One Step can streamline your IT operations, minimize interruptions, and strengthen your security to safeguard your valuable assets.

Are you certain your IT and security are as effective as they should be?

Call us now at **(623) 227-1997** or scan QR code to schedule a free consultation.

Elevate your business with the best in the game!

SCAN ME

One Step signs on as a Cybersecurity Awareness Month Champion

Celebrating 20 Years of Cybersecurity Vigilance

This October marks the 20th anniversary of Cybersecurity Awareness Month, a milestone that highlights how far the field of cybersecurity has come in educating and raising awareness about digital security.

One Step Secure IT has proudly signed on as a Cybersecurity Awareness Month Champion. This program is a collaborative effort among various entities committed to advocating for Cybersecurity Awareness not just in October but throughout the year.

Technology has become an integral part of our daily lives—we rely on smartphones, online learning, and remote work for convenience and efficiency. However, this integration also exposes us to greater cyber threats.

The 2023 Cybersecurity Awareness Month, led by the Cybersecurity and Infrastructure Security Agency (CISA), provides an excellent opportunity to explore the latest insights and gain valuable tips for protecting your digital life.

"Cybersecurity begins with good personal cybersecurity hygiene and is something everyone—and I mean everyone—can constantly improve on," says One Step Secure IT Founder and CEO Scott Kreisberg.

With technology playing a large role in our lives, it's crucial to stay vigilant against cyber threats and brush up on the key themes covered during Awareness Month.

Multi-Factor Authentication (MFA): Your Digital Shield - MFA has emerged as a critical layer of defense against unauthorized access to your accounts. This method requires users to provide two or more different factors to verify their identity. Common MFA methods include push notifications, time-sensitive codes sent to your email and phone number, and security questions. Enabling MFA adds an extra shield of security, even if your password is compromised.

Passwords: The First Line of Defense - Passwords remain the most widely used method for protecting accounts, underscoring the importance of creating strong, unique passwords. Aim for passwords that are long, combining letters, numbers, and symbols while avoiding common phrases and personal information.

Password Managers: Simplifying Security - Managing a multitude of complex passwords can be overwhelming. Password managers securely store and auto-fill passwords for various accounts. They use encryption to protect your passwords, and you only need to remember one master password.

Software Updates: Patches for Protection - Regularly updating your operating systems, applications, and devices with the latest security patches is crucial to prevent attacks. Hackers look for outdated software with known vulnerabilities, making software updates a proactive defense strategy.

Phishing: Recognize, Resist, Report - Phishing remains one of the most prevalent cyber threats. Awareness is key: scrutinize sender addresses, avoid clicking on suspicious links, and don't divulge personal information without verifying the source. If you encounter a phishing attempt, delete the email and consider alerting your IT team or reporting it the appropriate authorities.

The 2023 CISA Cybersecurity Awareness Month emphasizes the importance of staying informed and taking a proactive approach to protecting your sensitive information. By implementing these cybersecurity practices, you can significantly enhance your defenses. Remember, the effort you invest in safe- guarding your digital presence today can save you from potential headaches and financial losses in the future.

As we celebrate Cybersecurity Awareness Month in October, remember that staying safe and cyber-aware is a year-round commitment. If you have any questions about cybersecurity or need further guidance, One Step Secure IT is here to help.

Schedule an appointment to chat with a One Step Secure IT cybersecurity expert by calling (623) 227-1997. Explore more resources at www.onestepsecureit.com and on social media (@OneStepSecureIT) for year-round cybersecurity education.

CYBERSECURITY AWARENESS MONTH

Q&A Demystifying Cybersecurity
Your Frequently Asked Questions Answered

Are you curious about fortifying your business against cyber threats or understanding the strategies experts employ to recover from cyber attacks? Our team of security experts is here to provide you with illuminating answers to your burning questions.

Q: What is One Step's approach to preventing data breaches and responding to security incidents?

A: We have an in-depth and defensive approach when working to prevent data breaches and respond to security incidents for our clients. Here's how we make it happen:

Our primary focus is on implementing security measures—this includes setting up security controls and software that ensure only approved applications can run on their systems. We closely monitor these applications using Managed Detection and Response (MDR) services.

In addition to application whitelisting and MDR, we keep a vigilant eye on each system through our Remote Monitoring and Management (RMM) tools. We regularly apply patches to maintain system security and performance at optimal levels.

Equally important, we prioritize security training for our users and employees. We educate them on the nuances of phishing attacks, helping them understand how these attacks occur and what signs to look for.

In the unfortunate event of a security incident, we assist in developing and executing incident response plans. We ensure that everyone involved has a clear understanding of how to report an incident and the necessary steps to take.

Our approach revolves around being proactive in prevention while also being prepared to respond effectively when needed.

Q: How do you assist with data backup and secure remote work setups?

A: We collaborate closely with our clients to ensure the security and reliability of their data backup systems. Here's how we achieve this:

We establish both image-level and file-level backups in the cloud, separate from the client's network. These backups are carefully managed to prevent any unauthorized access by potential threat actors.

Our team conducts daily testing of image-level backups to verify their functionality and address any issues promptly.

For remote workforces, we implement a cloud VPN (Virtual Private Network) solution. This allows employees to work remotely while securely connecting to the company network, and maintaining data security.

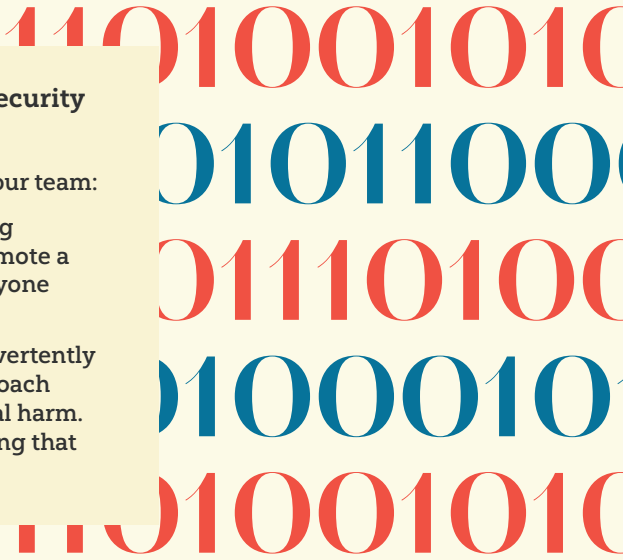
Our approach is centered on securing data backups and facilitating secure remote work, ensuring data protection and accessibility while mitigating potential threats.

Q: How does One Step approach employee training to enhance cybersecurity awareness within an organization?

A: We have a multi-faceted approach to promoting security awareness among our team:

We utilize a phishing simulation tool, helping users gain a deeper understanding of phishing tactics and email threats. We encourage company leadership to promote a security-conscious culture by acknowledging that nobody is infallible and everyone can make mistakes.

We emphasize the importance of reporting incidents promptly if someone inadvertently clicks on a malicious link or opens a suspicious attachment. This proactive approach allows the IT or security team to take immediate action to minimize any potential harm. Our strategy is built on education, awareness, and open communication, ensuring that security remains a collective responsibility within the organization.



WHEN IT COMES TO CYBER CRIME,

THE BEST OFFENSE IS A GOOD DEFENSE

A ONE STEP SECURE IT CASE STUDY

Retail businesses are a major target for cyber criminals because they store large amounts of customer information. Many small business owners assume they won't get hacked, so they don't invest in a cybersecurity strategy, which can be a costly mistake.

Instead of leaving it to chance, Jess Boutique chose to take preventative measures to protect its business assets from cyber criminals before it's too late.

The Business

In July 2011, Jessica Pomerleau founded Jess Boutique in Burlington, Vermont, intending to help women feel more confident. The boutique specializes in women's designer clothing, jewelry, and accessories.

The Cybersecurity Challenge for Retail Businesses

Retail businesses store large amounts of customer data, which is not only their business asset but also the prey of cyber criminals. Since retailers are the most frequent targets of cyber attacks, it's crucial to know the facts about these attacks and take precautions to protect yourself.

- In 2021, 57% of all e-commerce cyber attacks were bot-driven (Imperva Research Labs)
- Survey results from Sophos indicate that 44% of retail organizations have been hit by ransomware in 2020, and 32% of those have paid.
- The lack of adequate cybersecurity makes 62% of retail customers unconfident about their data's security. And 25% say that they know their data is not safe with retailers. (www.Fortinet.com)
- MalwareBytesLabs estimates that retailers lost over $30 billion to cybersecurity attacks in 2019, more than any other industry.

The Results of a Penetration Test May Surprise You

One Step Secure IT ran a vulnerability scan on Jess Boutique systems, including the three computers used in the stores. Jess Boutique thought they were secure, but the scan results proved otherwise when they received a high-risk score of 97 out of 100. One Step provided the estimated cost of these risks if a cyber criminal decided to target their business and Jess Boutique wasn't interested in ever having to pay it.

Some of the security risks uncovered by that scan:

- One Step was able to gain access to 4 company credit card numbers that were being stored on company computers
- Business email addresses were found on the dark web
- Store computers and drivers were not being regularly patched and had 19 missed updates collectively

Jess Boutique did not have a password policy and lacked complex password requirements. The store computers did not have a lock-out feature after multiple failed login attempts. And what they didn't know was that hackers often use bots and password-hacking programs that run thousands of password attempts to break into systems—without an automated lock-out, businesses are left defenseless to these attacks.

Small cybersecurity risks compound to create enormous risks and make a small business an easy target for cyber criminals.

CASE STUDY CONTINUES >>>

Jess Boutique decided it was time to protect the business and implement a cybersecurity strategy with the help of One Step Secure IT. One Step's cybersecurity experts created a plan to get Jess Boutique in the low-risk category and fix the security gaps, including cybersecurity training for Jess Boutique employees to ensure everyone is on the same page. Employees at Jess Boutique now know cybersecurity best practices and can look out for red flags.

One Step's Services for Jess Boutique

Jess Boutique depends on One Step to support its retail technology and IT infrastructure, and are confident that they will handle any IT issues with cybersecurity in mind.

"The customer service at One Step is amazing. The IT is incredible; we really haven't had any security issues. With electronics and systems—things happen; I feel like anytime we have needed some support, it's been really prompt, and they have been a really easy company to work with," Alexis Pomerleau, Jess Boutique's current owner, said.

The Best Offense Is a Strong Defense

Jess Boutique took action to protect their company and customer data proactively, and as a result, they have not experienced a cyber incident, which is more than many small retailers can say today.

"Mainly, we're just really happy. Everyone's been super friendly and really easy to work with. There are check-ins even when there's not a problem, like 'hey, we're still here. Let us know if you need anything. How are things going?' That feels really nice — it's not just when we call for problem-solving, it's the company being really proactive," Pomerleau said.

If IT or cybersecurity issues arise during or after store hours, One Step's IT professionals are just a phone call away.

onestep Secure IT Services

Social Media Highlights

Busting 5 Common Myths! 🚫🔒

Cybersecurity isn't just about passwords and firewalls—it's a world of its own! Let's debunk some common myths:

🤔 **Myth 1:** "I'm Too Small to Be a Target": Size doesn't matter in cyberspace! Cyber criminals will go after anyone with vulnerabilities. Stay protected no matter your size.

🤔 **Myth 2:** "I'm Safe with Just an Antivirus": Antivirus is great, but it's not the superhero you think. Cyber threats evolve, and so should your defense. Layer your cyber protection.

🤔 **Myth 3:** "It Won't Happen to Me": Famous last words! Cyber attacks are on the rise, affecting individuals, small businesses, and giants alike.

🤔 **Myth 4:** "Cybersecurity Is Only for IT Geeks": You don't need a PhD in coding! Cybersecurity is everyone's responsibility. Educate your team about safe practices—it's your digital armor.

🤔 **Myth 5:** "Strong Passwords Are Enough": Sorry, "123456" won't cut it! Strong passwords are step one. Add two-factor authentication for an extra layer of defense.

🚫 Don't fall for these myths—stay informed, stay vigilant, and stay cyber secure.

#CyberMythsBusted #StaySafeOnline #CyberAwareness #SecureEveryClick

Like Comment Share

🌐📱 Ensuring Your Child's Cybersecurity in the Digital Age: A Guide for Parents

Tips to help you keep your child safe online:

💡**Education is Key:** Teach your child about online privacy, the importance of strong passwords, and the potential risks of sharing personal information.

💡**Parental Controls:** Utilize parental control features on devices and apps to limit access to age-appropriate content and monitor their online activities.

💡**Regular Check-Ins:** Have open conversations with your child about their online experiences. Encourage them to report any suspicious or uncomfortable interactions.

💡**Cybersecurity Software:** Consider installing reputable cybersecurity software on their devices to protect against malware and phishing attempts.

💡**Privacy Settings:** Help your child configure privacy settings on social media platforms and apps to control who can see their content.

💡**Safe Browsing Habits:** Teach them how to verify the credibility of websites and avoid clicking on suspicious links or downloading unknown files.

By taking these steps, you can empower your child to navigate the digital world safely and responsibly.

#CybersecurityForKids #OnlineSafety

Like Comment Share

Join us...

on social media at **@OneStepSecureIT,** where we specialize in simplifying complex cybersecurity concepts and delivering practical tips to empower you against cyber crime.

Be the first to explore our informative blogs, gain insights from experts, confront real-world challenges, and stay ahead with the latest cybersecurity updates. **Let's connect on social media—your gateway to a safer digital world awaits!**

In the world of cybersecurity...

the term "risk" can send shivers down any CEO's spine.😱 We've got some pro tips for you on implementing a rock-solid, risk-based approach to cybersecurity! 🔍🛡️

👉**Framework Foundations:** Start with a reliable framework like NIST-CSF. It's like your trusty compass in the wilderness of cybersecurity, helping you navigate potential threats.🗺️

👉**Quantify & Qualify:** It's like the yin and yang of risk assessment. Quantitative for cold, hard numbers, 📉 and qualitative for those subjective insights. Balance is key!

👉**Game On!:**🎮 Gamification spices things up! Create a friendly risk management competition among departments with rewards. There's nothing like a little friendly rivalry to keep everyone on their toes!

👉**Prioritize & Conquer:** Know your enemy! Prioritize risks based on their impact and likelihood. Attack the big fish first!🦈

👉**Mitigate Like a Pro:** A comprehensive mitigation strategy is your battle plan. Lay out those action steps, controls, and contingency plans. Stay ahead of the game!💪

👉**Automate & Adapt:** Automation is your sidekick in this superhero saga. Keep an eagle eye on risks with real-time monitoring, and stay flexible in the face of evolving threats!🤖

Let's build a safer digital world together.🌐🛡️

#OneStepSecureIT

Like Comment Share

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

CONNECT WITH US
@OneStepSecureIT

www.OneStepSecureIT.com
(623) 227-1997