THE LATEST BYTE

onestep
Secure IT Services

Cybersecurity Spring Cleaning

Vol. 2 | 2023

CYBERSECURITY
Spring Cleaning

Spring has sprung! It's an age-old tradition to open all the windows and give your home a deep cleaning as the season turns. In the modern age, clutter accumulates in the digital space, as well as the physical—and clutter in both spaces can be a daily hindrance.

Cleaning out your computer files and deleting those old folders off of your desktop can bring just as much relief and clarity as cleaning out the junk drawer in the kitchen.

Tidying up the digital space is the perfect opportunity for you to implement stronger cybersecurity strategies. A great place to start is changing the passwords you have used across multiple accounts and start storing the new, stronger passwords in an online password vault.

In this edition of The Latest Byte, our IT and cybersecurity experts will give their advice when it comes to starting off this season cyber-secure.

Happy Cleaning, Friends.

About onestep
Secure IT Services

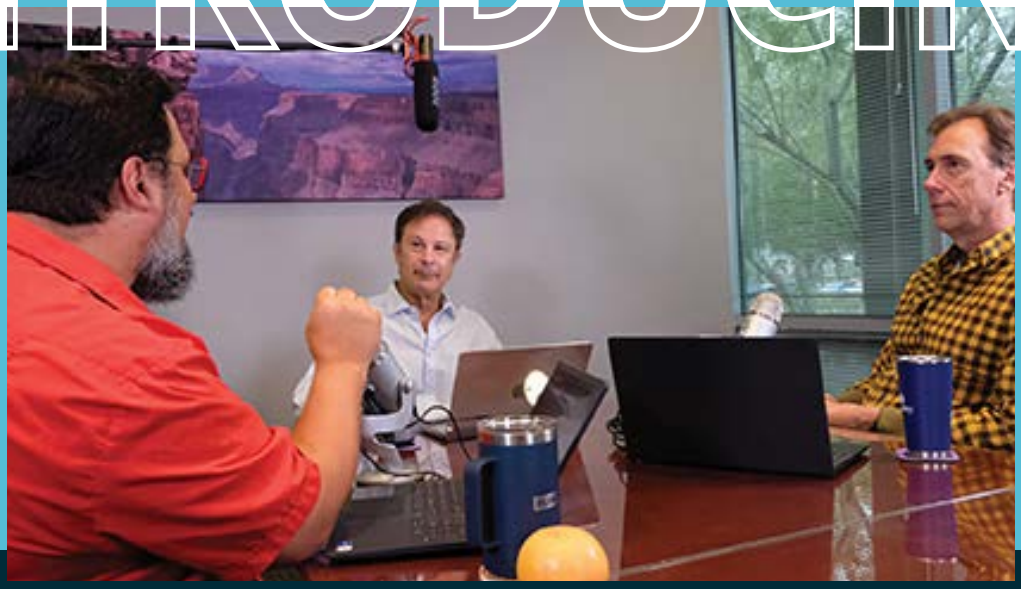
Since our start in 1985, One Step has helped businesses nationwide ensure their technology delivers a competitive advantage so they can focus on business growth and increasing revenue.

We specialize in Cybersecurity, Managed/Co-Managed IT, Information Security, and Compliance Services.

We understand that as the customer journey continues to evolve so do the threats to your business. Our team works with you to develop an IT strategy, identify vulnerabilities, and close gaps to strengthen your IT environment.

One Step corporate headquarters are in Phoenix, AZ and we serve businesses nationwide. For more information about our services, visit **www.OneStepSecureIT.com.**

INTRODUCING



One Step Beyond Cyber Podcast

EPISODE 1

00:11:11 00:30:11

Are you ready to take your cybersecurity knowledge to the next level?

Look no further than One Step Secure IT's podcast,

One Step Beyond Cyber!

Led by our CEO, Scott Kreisberg, and industry experts, Tim Derrickson and Roman Stanton, this podcast offers an exciting deep dive into the world of technology and IT. With tips and strategies on how to simplify tech solutions, recognize red flags, and prevent IT burnout, this podcast is perfect for anyone looking to stay ahead of the game.

No matter your background or experience level, *One Step Beyond Cyber* will provide you with the insights and knowledge you need to protect your business, your data, and your peace of mind.

Tune in to the inaugural episode of *One Step Beyond Cyber*, now available at

www.OneStepSecureIT.com/events

Make sure to follow us on social media **(@OneStepSecureIT)** to stay up to date on the latest episodes and industry news.

Don't miss out on this exciting opportunity to take your cybersecurity game **One Step Beyond!**

ROMAN'S CYBERSECURITY

SPRING CLEANING TO-DO's

Roman Stanton: One Step's Virtual Chief Information Officer/Client Compliance Advisor

What do you do as a vCIO/Compliance Advisor?

My top priority in both my vCIO and compliance roles is to provide the best solutions for my clients. As a vCIO, I serve as a strategic business partner, offering advice on all aspects of technology, including hardware and software recommendations. However, I also recognize that technology is just one piece of the puzzle, and I may need to advise on non-technical matters to help resolve broader business challenges.

In my compliance role, my primary responsibility is to ensure that my clients comply with the laws, regulations, and standards that apply to their company. This involves implementing industry best practices and adhering to governing bodies' regulations to minimize risks. While my focus is not necessarily on defending against specific threat actors, I am protecting my clients from all of Hollywood.

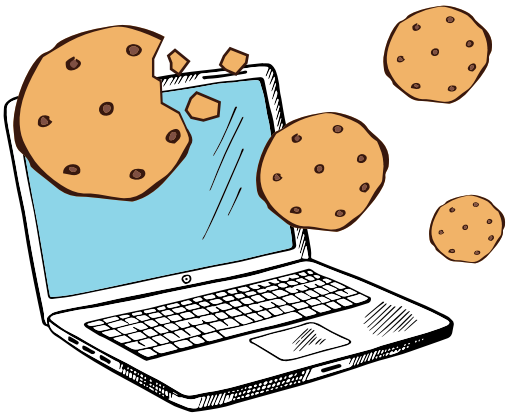
When did you first take an interest in technology?

I remember breaking my toys as a kid and putting them back together. Sometimes they worked again, and sometimes I threw them away so mom didn't know I broke them. However, the tools I used to fix the toys always had me looking at technology in a different way. When I had the chance to work with computers, I was happy that I could change parts, break software, and put it back together again.

Cybersecurity To-Do List

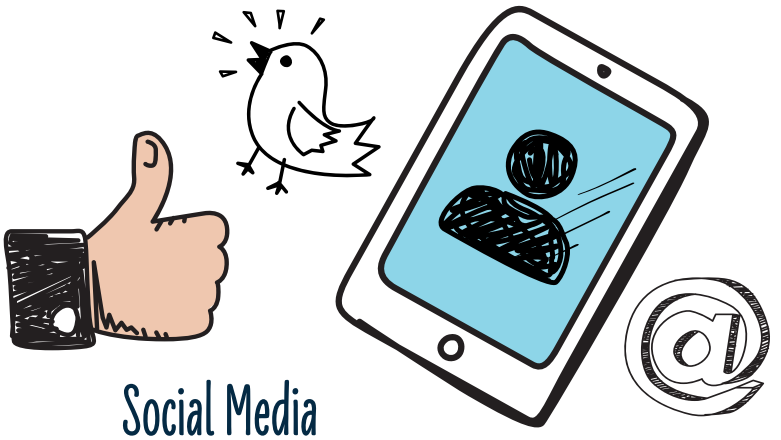
What are some actions you take on a regular basis that help you maintain your cyber hygiene?

On a weekly basis, I go through my personal emails and block, report, and assign to spam. I learned a while back that no one's job is on the line when it comes to stopping spam. Since there is no one in charge of that, it will never stop. Since the easiest way for cyber criminals to get into your system is by sending a phishing email, this is the first line of defense I try to stay on top of. Annually, I like to go over my browser settings. The updates are not supposed to revert changes, but sometimes they do.



Does clearing browser history and cookies regularly make a difference in terms of improving cybersecurity?

I try to clear my cookies regularly, with a nice glass of iced milk. Doc says I should cut back, but it's all in the name of security, I tell him. In all seriousness, clearing the cache, cookies and history is beneficial. Cookies are tracking devices that leave a trail of crumbs to where you have been and what you do online. While it's nice to be reminded of that perfect gift your partner was looking up, threat actors can now get access to your search habits and the history of your browser—allowing them to tailor the perfect scam email. Most of the scams we see are just forms of social engineering. Why would you want to give the bad guys more ammo to use against you?



Social Media

Do you have any tips for cleaning up your digital footprint on social media?

Social media is one of the hardest parts of our lives to clean. The algorithms that guide the social media platforms keep, and use, our data to help themselves grow. The best cleaning is done at the beginning. If it's too late for that, then I would, and do, go to the security tab to see if the settings have changed. Social media terms of service allows them to change your settings, and share your data as they see fit. Remove all public facing options, not only in the "privacy and security" sections, but in the "profile" section too.

My wife had contracted a company to remove her from the web. So there are certain firms that will scour the net, look for similar names, have you verify the data, and then they will remove it from public use. I was amazed. I am more of a public figure than her, so I have not gone through the process but I saw it work. Amazing all the opportunities the WWW offers.

Passwords

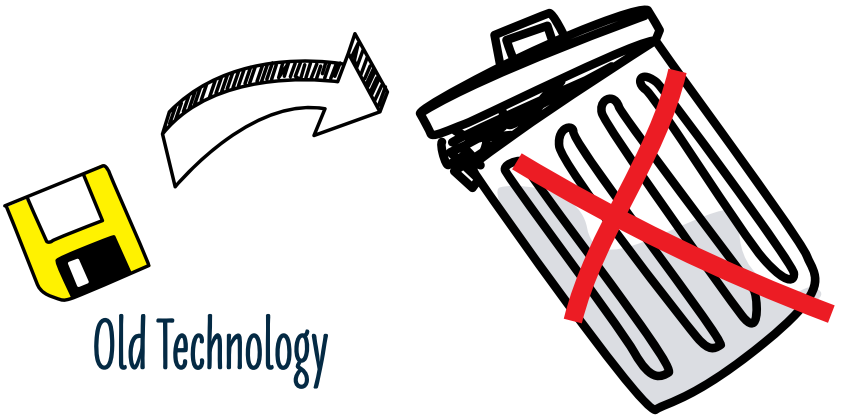
Do you have any tips for cleaning up password habits?

So, back in the day, I was pretty lax about my passwords. I mean, who hasn't used *Password123, letmein,* or *reset123* at least once in their lives? I thought, *hey*, *if someone really wants my stuff, they'll get it anyway.* But, over the past ten years or so, I've really changed my tune. I've learned that there are standards for creating strong passwords—you know, the whole 8 characters, upper and lowercase, numbers, symbols thing. And, even though it's kind of a hassle to deal with, I'd much rather put in the extra effort than have to deal with identity theft.

I actually had a friend go through that, and it took them a whole year to clear it. It was a total nightmare for them, constantly having to prove their identity over and over again.

Anyway, now I use what's called a passphrase for my passwords. They're not really new, but not a lot of people know about them. Basically, it's a password that's a phrase, like "PeanutButterJelly!". You want to make it a bit more complicated, so it takes longer for those bad guys to crack it. So, maybe something like P3@nut8u#erJ3lly^, where you change some of the letters to numbers and symbols. Pick something that you can remember; something that your mom or dad says, or an inside joke with your kids. It should be complex, and not something commonly known about you.

Now, where do you keep this super-strong password? In your head, my friend! It's the one password you remember, and you use it for your password manager. A password manager is a program that stores all your passwords in one safe place—either in the cloud or on your local computer. There are a bunch of different programs out there, like OnePass or PassPortal. So, don't be like me in my younger days— make sure you've got strong passwords and a good password manager to keep' em all safe!



Old Technology

What do you do with old, unused technology?

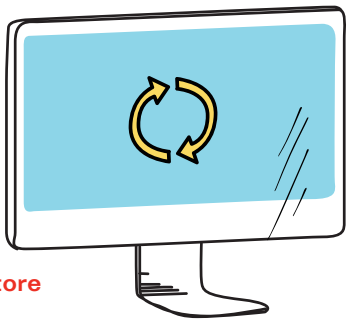
When it comes to getting rid of old personal electronics, the first step should definitely be to clear off any sensitive information. This includes wiping the hard drive of a computer, resetting an iPad to its factory settings, or deleting any personal data. Simply throwing these devices in the regular trash is not a good idea, as they can contain hazardous materials that can harm the environment.

Instead, it's important to properly dispose of these in a responsible manner. This can be done by recycling the devices through certified recycling programs, which can often be found through local government websites or electronic retailers. Many of these programs will accept a wide range of electronic devices, including computers, printers, and cameras.

How should businesses dispose of old technology?

As for businesses, there are often stricter regulations in place when it comes to disposing of old technology. This is because businesses may have sensitive customer or employee data that needs to be protected. Some industries, such as healthcare or finance, may have specific regulations regarding how electronic data should be disposed of. Compliance... compliance...compliance...

Businesses should look for certified e-waste recycling programs that can handle their specific needs. In some cases, businesses may also want to consider working with a specialized e-waste disposal company that can securely wipe data from devices and provide documentation of the disposal process. In any case, it's important for businesses to take the proper steps to protect their data and the environment when disposing of old technology.



Data Backups

What is the best way to store backed-up information?

Backups are clutch for clients. You really need to take those seriously. There are several methods of backup available. I tell my clients to get a backup of their backup.

You should have a Local Backup and a Cloud Backup. These could be file or image level backups, or a combination of both. I know it seems redundant, but it's the best practice for anyone who lives off their data. Now this is not "I backup my old spreadsheets and marketing material, etc." even though those should have two levels too. This is for the clients who keep customer data that they use for daily business.

So, for example, cloud backup is what most people these days think of...*my data is in the cloud*. First off that's great. Let's take the scenario: You are a retailer and there is a fire in the back office, which holds the server, modem, firewall, etc. The fire doesn't destroy the building structure. What happens if you cannot get to the cloud...the Internet Service Provider line was cut? Does this cripple your business? Well, if you have a local image backup that gets sent to the cloud, you can spin up the database locally on a system to act as a server and you are back in business.

90's Roman Would Say

Yo, listen up folks!

Backups are like, super important for all you clients out there. I mean, seriously, you gotta take that stuff seriously. There's like, a bunch of different ways you can do it, but let me tell ya, you should always get a backup of your backup. I know it sounds like overkill, but trust me, it's the smartest move for anyone who relies on their data.

And we're not just talkin' about your old spreadsheets and marketing stuff, ya know? This is especially crucial for those of you who keep customer data that you use on the daily. Let's say you're a retailer and there's a gnarly fire in your back office, where your server, modem, and firewall are all chillin'. What if you can't access your data in the cloud, like if the ISP line got cut or something? That would be a total business-killer, right?

But if you've got a local backup that also gets sent up to the cloud, then you're covered, dude. You can just spin up that database locally on a system to act as a server, and boom, you're back in action. So seriously, don't mess around with backups. They're the bomb-dot-com.

We Asked Our One Steppers

What is your favorite search engine?

Google	79%
DuckDuckGo	17%
Startpage	4%

Do you keep your social media accounts on the private setting?

Yes	82%
No	18%

How often do you back up your photos of family and friends?

Randomly	18%
Everyday*	72%
Monthly	3%
Annually	7%

*Automatic back up.

Where do you store your digital assets?

The Cloud	59%
Hard Drive	28%
Both	13%

If you have been hacked, what account was targeted?

My credit card
Google Drive
Facebook
An older email account
Spotify!
PlayStation account
Home Depot credit card
Yahoo email account
My PayPal

Do you have an email inbox of hundreds or thousands of emails or do you clear it out ASAP?

Hundreds	25%
Thousands	27%
Clear ASAP	48%

How Can the NIST Cybersecurity Framework Save Your Business?

As business owners face cyber threats every day, it can become overwhelming to keep up with all the regulations and strategies to safeguard your business from data breaches and cyber attacks.

Fortunately, tools have been created to help business owners manage security risks and decrease exposure to vulnerabilities. NIST Cybersecurity Framework or NIST-CSF is one such tool.

NIST (National Institute of Standards and Technology) is a non-regulatory agency of the United States Department of Commerce that promotes innovation and industrial competitiveness. NIST's mission is to "advance measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

Back in February 2014, NIST took a significant step to address the growing concerns of cybersecurity threats by releasing a voluntary Cybersecurity Framework. The objective was to reduce cyber risks to critical infrastructure. The framework was developed as a collaborative process that involved input from industry experts, academia, and the government.

This collaboration ensured that the framework met the needs of different sectors and was practical for implementation. The result was a comprehensive cybersecurity framework that businesses of all sizes can use to safeguard their digital infrastructure against potential cyber attacks.

A system scan following the NIST-CSF guidelines exposes specific vulnerabilities as defined by the framework's standards, guidelines, and best practices to help businesses know what security programs should be in place to prevent, detect, and respond to cyber attacks.

NIST compliance standards are a requirement for any business that processes, saves, or sends sensitive information to the Department of Defense (DoD), General Services Administration (GSA), NASA, and other government or state agencies.

However, every business can benefit from following the NIST Cybersecurity Framework. By following this framework, you can enhance your existing security protocols and develop new layers of security to protect your business. It's a proactive approach that helps businesses stay one step ahead of the constantly evolving cyber threats.

The NIST Cybersecurity Framework is organized around five core functions:

Identify, Protect, Detect, Respond, & Recover.

IDENTIFY The first step is to identify your organization's assets, systems, and data that need to be protected from cyber threats.

PROTECT The second step is to protect your assets by implementing security controls.

DETECT The third step is to detect cybersecurity events so that you can respond quickly and effectively.

RESPOND The fourth step is to respond to cybersecurity events in a way that minimizes the impact on your organization.

RECOVER The fifth and final step is to recover from a cybersecurity event so that you can resume normal operations.

By working with a NIST-CSF expert and implementing the five steps outlined in the Framework in detail, you can create a more secure environment for your business.

As a business owner, it's essential to be aware of the potential risks posed by cyber threats and to take steps to protect your business. If you are interested in learning about how to utilize the NIST- CSF framework at your business, contact our experts at **www.OneStepSecureIT.com/contact.**

onestep
Secure IT Services

Is Your Business Prepared for Cybersecurity Threats?

In the last year, a staggering 66% of businesses experienced

ransomware attacks, which cost small and medium-sized businesses an average of $812,000 in ransom payments. These attacks also caused businesses to halt operations for an average of 22 days.

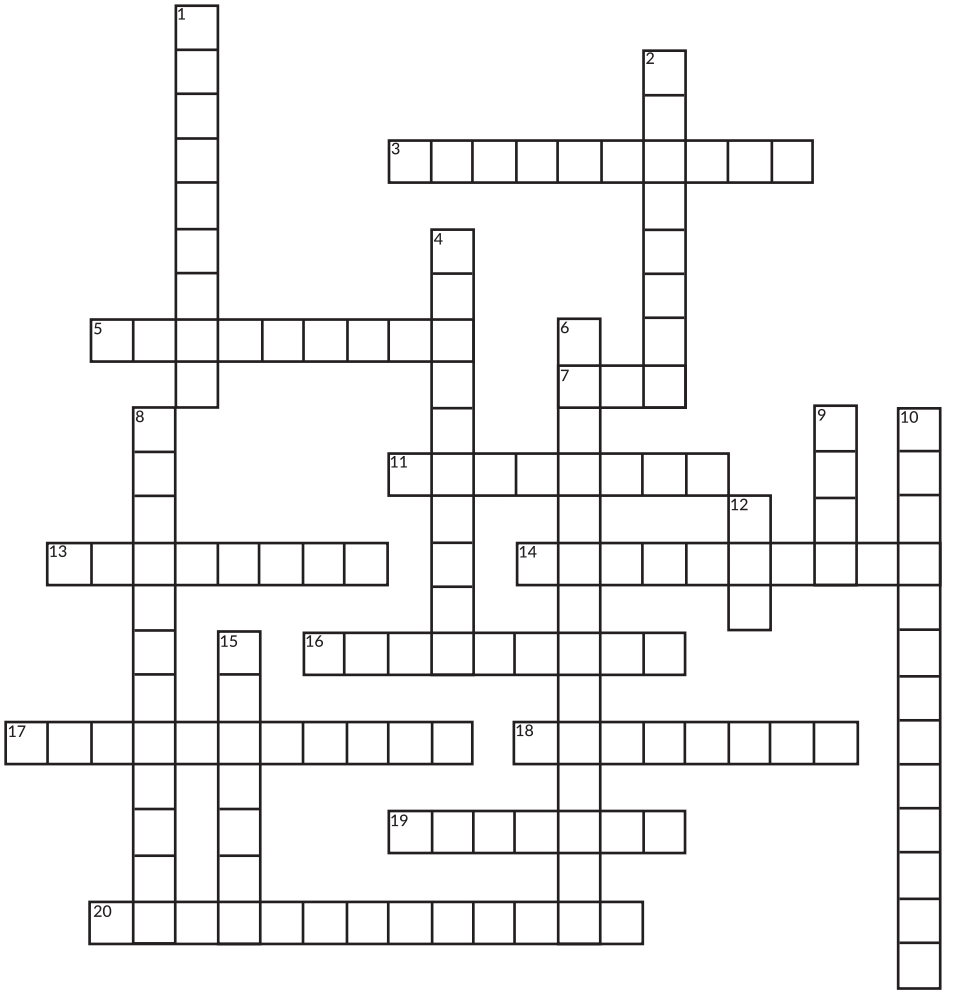
If you're unsure about the level of cybersecurity risk that your business is facing, you can take action to identify potential vulnerabilities and enhance your security strategy before cyber criminals strike.

One Step Secure IT is offering a free comprehensive cybersecurity risk assessment, conducted by a security expert, to help businesses pinpoint potential areas of risk related to cybersecurity and IT. This assessment can help your business take proactive steps to improve its cybersecurity posture.

Claim your Free Cybersecurity Risk Assessment Today!

or call us at:
(623) 227-1997

Cyber Safe Crossword Puzzle



ACROSS

3. A sequence of words or text used to control access to a computer; similar to a password.
5. Unauthorized access to a network, information systems, or application.
7. The address of a webpage. Check the validity of it before clicking on it.
11. Fraudulent text messages purporting to be from reputable companies in order to trick individuals into revealing personal information.
13. A fraudulent email purportedly from a reputable company attempting to get personal information.
14. The process of taking plain text and scrambling it into an unreadable format.
16. The "I" in the C-I-A Triad; protection from unauthorized changes.
17. Facebook, Twitter, Instagram, etc. (Two words)
18. Should be constructed of upper and lower case letters, numbers, and special characters.
19. Fraudulent phone calls or voice messages purporting to be from reputable companies in order to trick individuals into revealing personnel information.
20. Threatening behavior facilitated through electronic means such as texting.

DOWN

1. A wireless technology standard used over short distances using short-wavelength UHF radio waves.
2. Hardware or software designed to prevent unauthorized access to or from a private network.
4. A type of malicious software designed to block access to a computer system until a sum of money is paid.
6. Verifying identity.
8. The "A" in the C-I-A Triad. It ensures authorized users have access.
9. Widely used in-home network technology that allows for wireless connection in interfacing with the internet.
10. A flaw or weakness in a computer system that could be exploited to violate the system's security.
12. Security tool that creates a secure, encrypted connection between you and the Internet (acronym).
15. Harmful computer programs such as viruses, worms, and trojans used by hackers to gain access to your computer and cause destruction.

ANSWER KEY

Scan the QR Code to see the answers or look on the back of this newsletter.

Puzzle provided by https://securityawareness.usalearning.gov/

Upcoming Events

Meet Our Team!

Calling all business owners and tech professionals!

You won't want to miss out on the upcoming Small Business Expos and Arizona Technology Summit. These events provide the perfect chance to expand your network, gain knowledge on industry strategies, and elevate your business.

At the Small Business Expo, you'll have access to informative workshops (one of which is lead by our very own Tim Derrickson!), business solutions, and the opportunity to connect with like-minded professionals. For those in the tech industry, the Arizona Technology Summit offers a platform to learn about new technological advancements and network with others in the field.

Mark your calendars for these exciting events, taking place in three major U.S. cities, and register now using the links below. **Make sure to stop by the One Step booth—we can't wait to see you there!**

23 JUNE

NEW YORK CITY
The Small Business Expo
10 AM-6 PM EST | Booth 3239
New York Hilton Midtown
thesmallbusinessexpo.com/city/new-york-city/

12 SEPT

PHOENIX
Arizona Technology Summit
8 AM-4 PM MST | Booth 503
Phoenix Convention Center
technologysummit.net/arizona.html

06 SEPT

LOS ANGELES
The Small Business Expo
10 AM-6 PM PST | Booth 811
LA Marriott Burbank Airport
thesmallbusinessexpo.com/city/los-angeles/

27 SEPT

PHOENIX
The Small Business Expo
10 AM-5 PM MST | Booth 609
Phoenix Convention Center
thesmallbusinessexpo.com/city/phoenix/

Let's Be Social

Staying on top of your cybersecurity is an ongoing process, and we are here to simplify it. Stay on top of everything Cyber by following us on LinkedIn, Facebook, and Twitter.

@OneStepSecureIT

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

CONNECT WITH US
@OneStepSecureIT

www.OneStepSecureIT.com
(623) 227-1997

CROSSWORD ANSWER KEY—ACROSS: 3. PASSPHRASE, 5. INTRUSION, 7. URL, 11. SMISHING, 13. PHISHING, 14. ENCRYPTION, 16. INTEGRITY, 17. SOCIAL MEDIA, 18. PASSWORD, 19. VISHING, 20. CYBERBULLYING | **DOWN:** 1. BLUETOOTH, 2. FIREWALL, 4. RANSOMWARE, 6. AUTHENTICATION, 8. AVAILABILITY, 9. WIFI, 10. VULNERABILITY, 12. VPN, 15. MALWARE