onestep
Secure IT Services

THE LATEST BYTE

CYBER-SECURE SAFE TRAVELS

Vol. 3 | 2023

With summer in full swing,

many of us are preparing for exciting journeys, whether for business or pleasure. In this edition of The Latest Byte, we shine a spotlight on an essential topic that often gets overlooked amidst the excitement of travel—security.

While the ability to stay connected on the go is undoubtedly convenient, it's crucial to be aware of the potential risks that come with it. From public Wi-Fi networks to charging stations, cyber threats can lurk in unexpected places, putting your personal and business information at risk.

In this edition, we delve into the world of cybersecurity while traveling, equipping you with the knowledge and tools you need to protect your digital footprint wherever your adventures take you. We have gathered insights from our very own CEO, Scott Kreisberg, who shares his expertise on maintaining cybersecurity while on the road.

Whether you're jetting off to an exotic destination, embarking on a business trip, or planning a weekend getaway, join us on this journey through the realm of security while traveling. Together, let's ensure that your travels are not only exciting but safe and secure.

Safe travels

ABOUT ONE STEP SECURE IT

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.

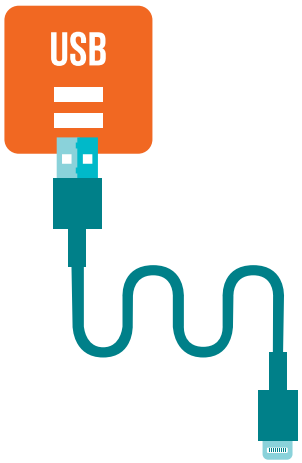
We understand that as the customer journey continues to evolve so do the threats to your business. Our team works with you to develop an IT strategy, identify vulnerabilities, and close gaps to strengthen your IT environment.

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

www.OneStepSecureIT.com

Cyber Safety Tips While Traveling

Use Caution with Public Charging Stations



The FBI cautions the public against using free, public charging stations with built-in cords at airports, hotels, malls, or other areas. **"Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices that access these ports,"** the agency warns.

Scammers can install malware on public charging stations that lock your phone and export your personal information. According to the Federal Communications Commission, scammers will use your personal information to gain access to your online accounts or sell it to other criminals.

It's difficult to tell if these charging stations have been tampered with; the safest bet, according to the FBI, is to **"carry your own charger and USB cord and use an electrical outlet instead."**

Staying Cyber Aware When Working Remote

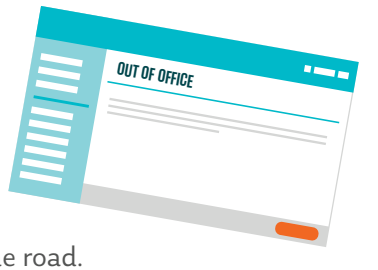
U.S. cyber officials warned that hackers have been exploiting the growing demand for remote work by passing off their malicious tools as remote collaboration software produced by Zoom and Microsoft. Hackers have also been targeting virtual private networks, allowing an increasing number of employees to connect to their offices remotely.

It is crucial to keep a few cybersecurity guidelines in mind when working remotely:

- Use a VPN to secure and mask your network
- Have multifactor authentication enabled on your online accounts
- Have up-to-date software installed
- Have anti-virus and anti-malware installed
- Schedule a routine backup of your data
- Do not click on any unknown links online or in your emails
- Do not open or download any unexpected attachments
- If possible, only use company-provided equipment and resources
- Follow your company's security policies at all times

Are Those "Out of the Office" Emails Acting as Hacker Bait?

You may not mind if co-workers or clients know that you are going to the beach for a week. But what if you are telling your business to a cyber criminal? The details you provide in your automatic email could be used for malicious purposes.



When writing your "out of the office" email, think twice before including the following:

- Direct business phone numbers for you and other co-workers
- Personal cell phone numbers
- Concrete dates and details about your absence

Automatic replies to phishing emails could cause your business problems down the road. PhishLabs warns that replying to a phishing email can lead to further attacks. Most phishing campaigns are automated, and replying to them puts you on a scammer's radar.

Creating two separate "out of the office" emails—one for internal emails and one for external—is an easy way to avoid sending too much information to the wrong person. Unless you feel it's necessary for your business, consider only sending the "out of the office" email to internal addresses.

Lost or Stolen Device with Personal Info?

With the increased use of digital payment options such as Apple Pay—many people have easily accessible debit and credit card information on their smartphones. It's easy, fast, and convenient, but it could mean losing much more data if your phone goes missing.

However, if you prepare, there is a way to track those lost or stolen electronic devices via GPS and ideally get them back in your hands. If you are unable to get the device back or you fear it has already fallen into the wrong hands—you have the option to remotely wipe all of your sensitive data from your device before it is used for malicious purposes.

For Apple users, the tracking service is called "Find My" and Android users can use Google's "Find My Device". You can track smartphones, computers, smartwatches, headphones, and other electronics that are trackable through your chosen device-tracking app. Within each of the tracking services that can be accessed from another device with internet access, you can wipe all data from the lost or stolen device.

Be Wary of Scanning QR Codes

The FBI has warned that cyber criminals have been tampering with legitimate QR codes to trick users into visiting malicious websites.

Earlier this year, the FBI issued a public advisory about fraudulent QR code stickers placed at over 20 parking stations in Austin, Texas. The QR codes looked like an easy way to pay for parking, but those payments went to a fraudulent vendor. QR Codes are easy to create, and it is difficult to determine a legit code from a fraudulent one.

Unfortunately, there's no way to tell where a QR Code will direct you until it is scanned, so only scan QR codes from trusted sources.

Get to Know the CEO
SCOTT KREISBERG

Running a Successful Business...

...requires a combination of passion, foresight, and the ability to adapt to evolving technologies. Scott Kreisberg, the CEO of One Step Secure IT, knows this firsthand. With over three decades of experience in the technology industry, Scott has expanded his expertise to help businesses of all kinds.

Reflecting on the early days of building his business, Scott was motivated to help people run their businesses better using technology. After spending many years assisting retailers, he extended his expertise to other companies beyond the retail industry.

Today, going on 37 years as a business owner in the tech industry, Scott shared what he has learned over the years and what actions he has taken to get where he is today.

Guiding the One Step Ship

At the heart of One Step Secure IT's success is Scott's role as CEO, guiding the ship. "I need to be 3 to 5 years ahead of the business, acting as a guiding light," he said. Scott emphasized that he doesn't take the role of steering the ship lightly; it requires staying focused on the long-term vision and avoiding the allure of every passing trend or newest "shiny object."

Scott shared that his curiosity and love for learning play vital roles in his leadership style and business decision-making process. He dedicates a significant amount of time to researching and staying up-to-date with the latest technologies and trends. Reading books, articles, and news outlets—"I don't rely on any one source," he shares.

Scott credited the value of education in shaping his journey. "Get an education in areas that will benefit you," he advised. Armed with a double major in finance and marketing, and a minor in computer science, he possesses a versatile skill set.

"I believe in knowing and doing every role within my business so that I fully understand it. So, I've done literally every single job in this business—I did all of the studying and learning so I can better understand and guide the business," he said.

Scott Kreisberg's Entrepreneurial Advice

As a seasoned entrepreneur with a storied history of operating and growing One Step through recessions and the 2020 pandemic, Scott shared valuable advice to his younger self and aspiring business owners:

Take a Breath Amid the challenges and uncertainties, it's crucial to pause, take a breath, and maintain a sense of calm. Overcoming obstacles requires a clear mind and strategic thinking.

Be Receptive to Change Don't be afraid to venture into uncharted territories, even if others discourage you. Entrepreneurship is an art form that requires finesse and open-mindedness. Trust your instincts and explore new possibilities.

Engage in Continuous Learning Never stop learning and expanding your knowledge base. Gain education in areas that will benefit your chosen path. The more diverse skills acquired, the better equipped you will be to face future challenges.

Surround Yourself with Positive Energy Positive energy is contagious and vital for personal and professional growth. Surround yourself with individuals who uplift, inspire, and contribute positively to your environment.

Value Loyalty Recognize and nurture relationships with loyal friends and business associates. Building a trusted circle of support is invaluable in times of need and fosters a sense of community and collaboration.

Looking to the Future

As for the future of technology, Scott sees AI and quantum computing continuing to emerge and become major components of the tech industry.

> It's going to create a completely different environment. People's dependency on technology will grow, and it will barely be noticeable because interacting with it will be seamless.
>
> When it comes to cybersecurity, AI-powered systems can analyze vast amounts of data and detect patterns that indicate potential cyber threats. Machine learning algorithms can identify anomalies in network traffic, behavior patterns, and known attack signatures—enabling early detection and proactive prevention of cyber attacks. However, cyber criminals have also started using these same systems to enable them to crack passwords in seconds due to the speed of AI-powered decision-making.

As for protecting businesses from cyber threats, "the game's not going to change; it's going to be powerful computers and AI battling it out with different toolsets," Scott said.

Cybersecurity Tips From Scott

As a cybersecurity expert, Scott understands the importance of protecting sensitive information and staying ahead of potential threats. Here are some tips that Scott recommends:

1. **Strong Passwords and Unique Usernames**
Scott recommends using strong, complex passwords for all accounts. He even suggests using unique usernames that are unrelated to personal information, making it more challenging for hackers to gain unauthorized access.

2. **Password Management Tools**
To handle the complexity of managing numerous passwords, Scott recommends using password management tools. These tools securely store and generate passwords, making it easier to maintain strong and unique credentials.

3. **Unique Email Addresses**
Scott utilizes a tool that allows him to create unlimited unique email addresses. By signing up for services using unique email addresses, he can quickly identify which services may have been compromised in case of a breach.

4. **Credit Freezes and Financial Monitoring**
Scott emphasizes the importance of credit freezes with all credit bureaus to prevent identity theft. Additionally, he utilizes multiple services that monitor financial activity, providing real-time notifications if any suspicious activity occurs.

5. **Secure Technology Usage**
Scott ensures that his technology is encrypted, particularly when it comes to laptops and other portable devices. Encryption adds an extra layer of protection, rendering stolen devices useless to potential attackers.

6. **Public Wi-Fi and VPNs**
Scott advises against using public Wi-Fi networks whenever possible. Instead, he relies on the cellular service on his phone. When using public Wi-Fi becomes necessary, he employs a VPN (Virtual Private Network) to encrypt his internet traffic and enhance security.

What Is Shadow IT and How Can It Affect Business Operations?

A concerning issue that often arises for businesses is "shadow IT."

If you haven't heard of it, shadow IT refers to the use of technology solutions that haven't been approved by the IT department. This encompasses a range of situations, including employees accessing company systems using their personal devices or utilizing cloud-based services without obtaining proper authorization.

While employees may engage in shadow IT to work more efficiently, it can cause a whole host of problems for your organization. It can create security risks, cause data loss, reduce productivity, and even create more work for everyone involved.

How shadow IT affects small businesses.

1. Security Risk

One of the biggest concerns with shadow IT is that it can create security risks for a business. Since these technologies are not managed by the IT department, they may not have the same level of security measures in place as the organization's approved systems. This could lead to vulnerabilities and make it easier for cyber criminals to access sensitive company data.

Additionally, since the IT department is not aware of the existence of these systems, they may not be monitoring them for security issues or applying security updates to them in a timely manner. This can leave the organization at risk of cyber attacks and data breaches.

2. Data Loss and Duplication

The use of unauthorized technology solutions can also result in the duplication of data and applications, which can make it difficult to track where data is stored and who has access to it. This could lead to data loss, leaks, or misuse of sensitive information.

For example, if an employee is using a personal device to access company systems and data, the device may not be properly secured or managed. If the device is lost or stolen, the data stored on it could be compromised.

Similarly, if employees are using different cloud storage services to store and share files, it can be challenging to keep track of where data is stored and who has access to it. This could lead to data breaches or loss of control over sensitive information.

3. Reduced Productivity

While employees may use shadow IT to work more efficiently, it can actually lead to reduced productivity for the business as a whole. If different departments are using different software solutions to manage projects or analyze data, it can be challenging to integrate the different systems and ensure that everyone is working from the same data sets.

This can lead to delays in decision-making, duplication of effort, and missed opportunities. It can also create more work for the IT department, as they may need to troubleshoot issues related to multiple software solutions rather than just one.

4. Increased Costs

Finally, shadow IT can lead to increased costs for a business. If employees are using personal devices or unauthorized software solutions, the organization may need to invest in additional security measures or software licenses to ensure that data is properly protected and managed.

Similarly, if different departments are using different software solutions to manage projects or analyze data, it can be challenging to negotiate enterprise-level pricing or get volume discounts on software licenses.

Real-world examples of shadow IT.

Here are a few examples that demonstrate how shadow IT can infiltrate a company and the harm it can cause.

Personal file-sharing service: A small marketing agency discovered that one of its employees was using a personal file-sharing service to store and share sensitive client data with team members. The employee believed the service was more user-friendly than the company-approved solution. However, the IT department had no control over the security settings or access permissions of the personal file-sharing service, putting sensitive client data at risk.

This incident led the company to implement a clear policy on approved file-sharing solutions and provide training to employees on their proper use.

Unauthorized customer relationship management (CRM) software: A medium-sized manufacturing company discovered that its sales department had used an unauthorized CRM tool to manage customer interactions. Although the tool was not approved by the IT department, the sales team found it more convenient and efficient than the company's existing CRM system.

The use of the unauthorized tool led to data inconsistencies and increased the risk of data breaches. The company addressed the issue by working closely with the sales team to understand their needs and identify a suitable CRM solution that met both the sales team's requirements and the company's security standards.

Unsecured employee devices: A small e-commerce business discovered that several employees were using their personal smartphones and laptops to access company data and work on projects outside office hours. The IT department had not approved these devices and had no control over their security measures or the data stored on them.

This situation left the company vulnerable to data breaches if an employee's device was lost, stolen, or compromised. To mitigate this risk, the company implemented a bring-your-own-device (BYOD) policy and provided training to their employees on how to secure their devices and protect company data.

How can businesses prevent shadow IT?

Here are some steps you can take to help reduce the risk of shadow IT and ensure that your technology solutions are secure, efficient, and effective in meeting the needs of your employees and your business.

STEP 1 **Develop Clear Policies & Guidelines**

Having clear policies and guidelines is important because it establishes expectations for how employees should use technology solutions in the organization, reduces ambiguity around what is allowed, and helps prevent employees from using unapproved technology solutions that may pose security risks.

- Conduct a thorough assessment of all technology solutions used within the organization to identify potential risks.
- Develop policies that are easy to understand and provide examples of what constitutes approved and unapproved technology solutions.
- Ensure that the policies are regularly updated and communicated to all stakeholders, including new employees and contractors.

STEP 2 Educate Employees

Educating employees helps them understand the risks associated with using unapproved technology solutions and reinforces the importance of following IT policies. It also helps create a culture of security awareness, which can help prevent employees from engaging in risky behavior that could compromise security.

- Develop training programs that help employees understand the potential risks associated with shadow IT and the importance of following IT policies.
- Use real-life examples to illustrate the consequences of using unapproved technology solutions.
- Encourage employees to report any suspicious activity related to technology use.

STEP 3 Foster Collaboration

Fostering collaboration between IT and other departments helps ensure that technology solutions meet the needs of employees and the organization. It also helps identify potential technology solutions that may be more effective than current options and reduce the likelihood of employees seeking out their own solutions.

- Create cross-functional teams that include IT and other department representatives to work together on technology solutions.
- Conduct regular meetings to identify opportunities for collaboration and to discuss the use of technology solutions.
- Encourage communication and transparency among all stakeholders to ensure that everyone is aware of the approved technology solutions.

STEP 4 Monitor Network Traffic

Monitoring network traffic is important because it can help detect unauthorized technology solutions that employees may be using and identify potential security risks associated with those solutions. By tracking network traffic, IT departments can detect and respond to security breaches before they become serious problems.

- Use network monitoring tools to track the use of technology solutions within the organization.
- Regularly review reports to identify any unauthorized technology use and take appropriate action.
- Use analytics tools to identify patterns and trends related to technology use that could be indicative of shadow IT.

STEP 5 Provide IT Support

It is important to help employees resolve technology issues in a timely manner, reducing the likelihood that they will turn to unapproved technology solutions as a workaround. It also fosters a culture of support and collaboration between IT and employees.

- Develop a user-friendly IT support system that quickly and effectively solves employee technology issues.
- Offer training and guidance on how to use approved technology solutions.
- Create a culture of support by encouraging employees to seek IT assistance when needed.

STEP 6 Regularly Review Policies & Procedures

Regularly reviewing policies and procedures ensures they remain up-to-date and effective in preventing shadow IT. It also helps organizations stay ahead of emerging security risks and technology trends and ensures that policies and procedures are effective over time.

- Conduct regular reviews of policies and procedures to ensure they are up-to-date and effective in preventing shadow IT.
- Solicit feedback from employees and other stakeholders on how to improve policies and procedures.
- Stay up-to-date on emerging security risks and technology trends to ensure that policies and procedures remain effective over time.

Ever wonder if your business credentials are being sold on the Dark Web? There is a way you can find out!

It only takes one wrong click by a well-meaning employee and sensitive information is exposed.

Get concrete answers about whether or not your business information is being sold on the Dark Web with our **FREE DARK WEB SCAN.**

Scan QR Code or call (623) 227-1997 to learn more.

Unleash Your Inner Tech Explorer

Learn about Groundbreaking Technology!

In a world where technology has become an integral part of our lives, it's fascinating to imagine a time before the gadgets we rely on today were even invented. By learning about the sites where these ground-breaking technologies were born, we can better understand the incredible effort and ingenuity that went into their creation.

Let's take a closer look at some extraordinary locations around the globe to gain a fresh perspective on the gadgets that have become indispensable in our daily lives.

1. First Scanned Barcode

Can you picture the grocery store checkout line before barcodes were invented? In the summer of 1974, at a grocery store in Ohio, the very first scanning of a UPC code took place. As the 10-pack of gum glided down the conveyor belt at Marsh supermarket, it marked a significant milestone as the inaugural grocery item was scanned. This groundbreaking moment paved the way for barcode technology to become the industry standard, revolutionizing pricing information storage and expanding its applications for both consumer-facing and internal tracking purposes.

2. Invention of Photoshop

In the realm of digital wonders, few apps rival the indispensability of Photoshop. Although its development began in 1987, this iconic photo-editing software didn't grace the commercial scene until 1990. Since then, it has earned its well-deserved place as a staple on our devices. Created by Thomas Knoll, a Ph.D. student at the University of Michigan, Photoshop has transformed the way we manipulate and enhance images, becoming an integral part of our digital lives.

3. World's Fastest Computer

Oak Ridge National Laboratory in Tennessee is world-famous for its groundbreaking contributions. Housing several of the planet's top supercomputers, including the unrivaled Frontier, it holds the title of the world's most powerful computer according to the prestigious TOP500 ranking. With its extraordinary processing power, Frontier continues to dominate as the sole supercomputer surpassing one exaFLOPS, performing an astonishing 1.194 quintillion floating point operations per second. Additionally, Oak Ridge is a trailblazer in neutron and nuclear power research, boasting exceptional facilities like the Spallation Neutron Source, the High Flux Isotope Reactor, and the Center for Nanophase Materials Sciences.

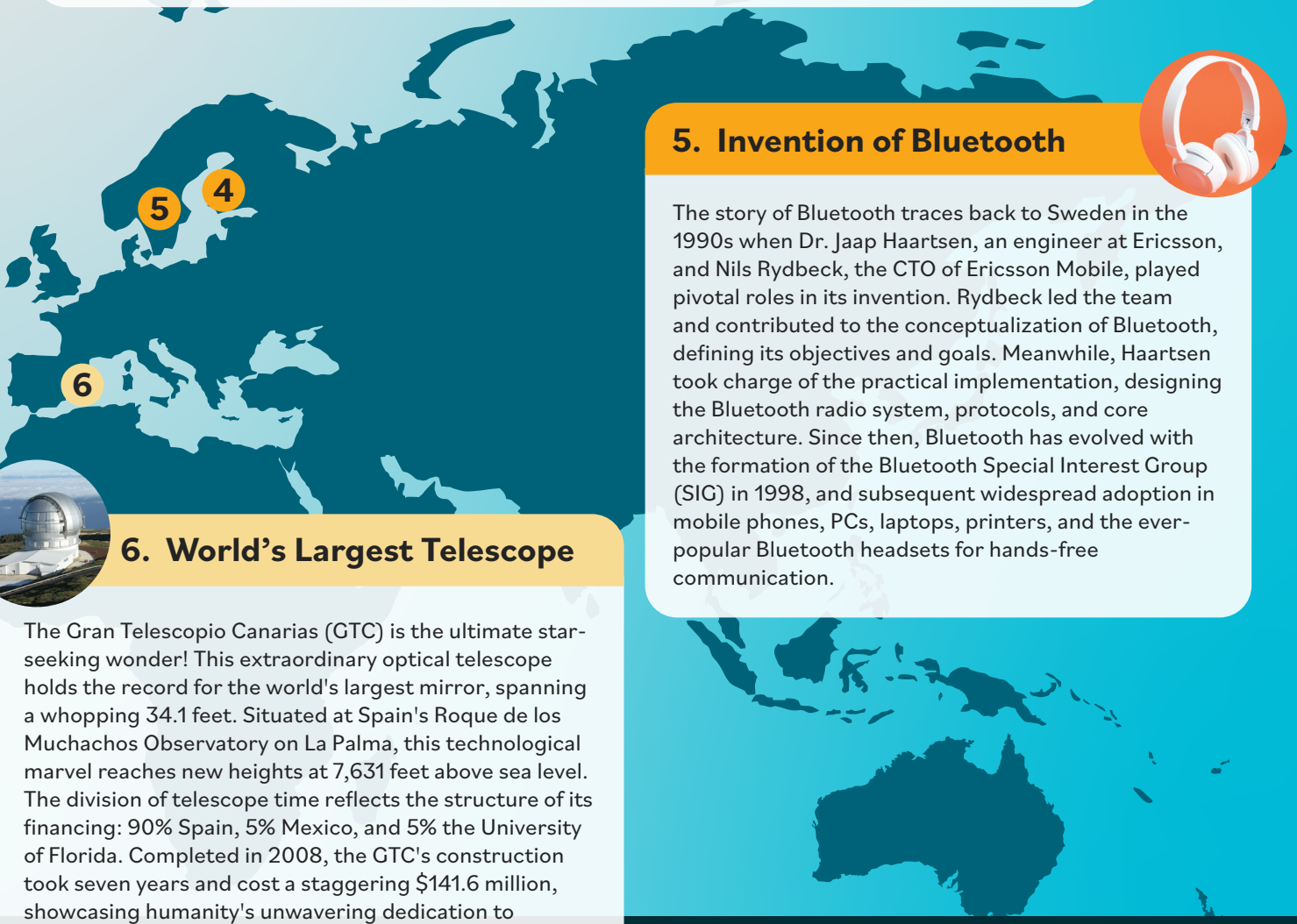
This September, find One Step Secure IT at...

06 SEPT

LOS ANGELES
The Small Business Expo
LA Marriott Burbank Airport
10 AM-5 PM PST | **Booth 220**
thesmallbusinessexpo.com/city/los-angeles/

4. Malware Museum

Mikko Hyppönen, a computer security expert, is the mind behind The Internet Archive's captivating Malware Museum. Since 2016, he has curated this unique digital collection, showcasing his expertise as a renowned computer security expert from Finland. Visitors to the Malware Museum embark on a mesmerizing journey into the past, witnessing the impact of computer viruses firsthand without any real harm. It's a one-of-a-kind experience, offering a glimpse into a world of corrupted files and the infamous blue screens of death. Mikko is also known for the Hyppönen Law, which highlights the inherent vulnerabilities in "smart" IoT devices and states that whenever an appliance is described as being "smart," it is vulnerable.



5. Invention of Bluetooth

The story of Bluetooth traces back to Sweden in the 1990s when Dr. Jaap Haartsen, an engineer at Ericsson, and Nils Rydbeck, the CTO of Ericsson Mobile, played pivotal roles in its invention. Rydbeck led the team and contributed to the conceptualization of Bluetooth, defining its objectives and goals. Meanwhile, Haartsen took charge of the practical implementation, designing the Bluetooth radio system, protocols, and core architecture. Since then, Bluetooth has evolved with the formation of the Bluetooth Special Interest Group (SIG) in 1998, and subsequent widespread adoption in mobile phones, PCs, laptops, printers, and the ever-popular Bluetooth headsets for hands-free communication.

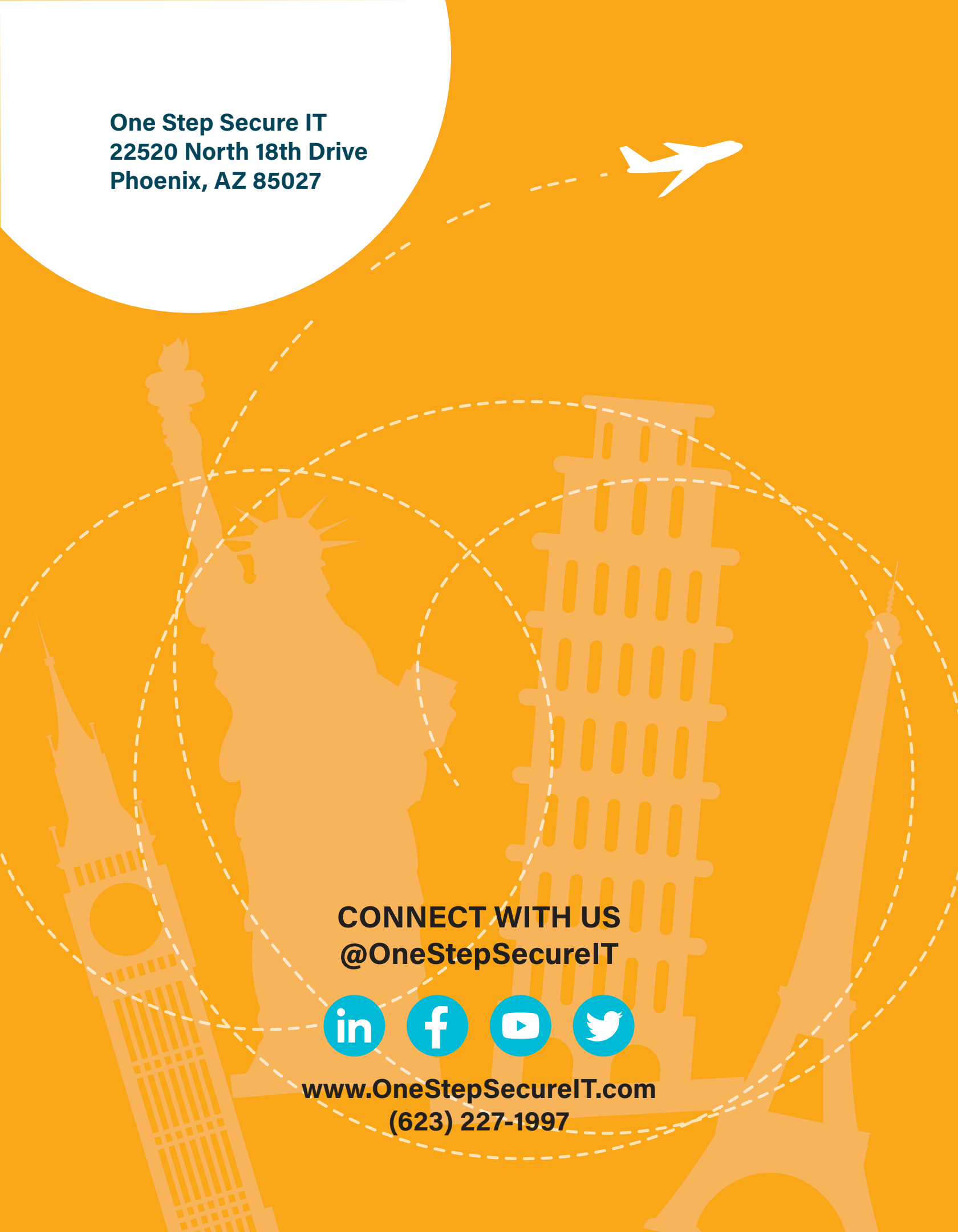
6. World's Largest Telescope

The Gran Telescopio Canarias (GTC) is the ultimate star-seeking wonder! This extraordinary optical telescope holds the record for the world's largest mirror, spanning a whopping 34.1 feet. Situated at Spain's Roque de los Muchachos Observatory on La Palma, this technological marvel reaches new heights at 7,631 feet above sea level. The division of telescope time reflects the structure of its financing: 90% Spain, 5% Mexico, and 5% the University of Florida. Completed in 2008, the GTC's construction took seven years and cost a staggering $141.6 million, showcasing humanity's unwavering dedication to exploring the mysteries of the universe.

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

27 SEPT
PHOENIX
The Small Business Expo
Phoenix Convention Center
South Hall F | Booth 507
10 AM-5 PM MST
thesmallbusinessexpo.com/city/phoenix/

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



CONNECT WITH US
@OneStepSecureIT

www.OneStepSecureIT.com
(623) 227-1997