1991 – 2021
30
YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

IP Address: What Is It And Why Do YOU Need To Know? ....Page 1

FREE: Business Owner's Guide To IT Support Services And Fees ....Page 2

Security Corner: 3 Smart Ways To Hide Your Searches In Public ....Page 3

Is Your Online Shopping App Invading Your Privacy? ....Page 3

Learn How To Fight Business Email Compromise ....Page 4

July 2023

Kim Nielsen, CISSP, CCSA
President &
Chief Technology
Strategist at

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

IP Address: What Is It And Why Do YOU Need To Know?

Introduction
IP address, short for Internet Protocol address, is a term that you've likely heard before if you've spent some time online. Although it sounds and might even seem like some sort of technobabble, the concept is actually quite simple: It's a series of numbers that identifies every individual machine and simultaneously broadcasts their locations.

While you may not think these affect everything you do online, THEY DO!

Why IP Addresses Matter
How much web traffic is your personal blog amassing? Does your search history hold any secrets you don't want someone else to find out? This, and a lot of other data you care about, is linked back to you through your IP address.

Your blog tracker counts unique hits. The search history remembers that you're the IP that typed it out. Your IP address matches the same router that is broadcasting WiFi inside your house right now, which means that all local devices on the network will appear as having the same IP address. That's how your computer knows to recognize other devices nearby, or why you and a friend might have similar targeted ads when you visit their house.

IP addresses also project your geographic location, which is why you get ads for nearby services. If you look up "food near me," it knows where "near you" is even if you aren't using location services. That's also why you might see local event notifications and other relevant advertisements that seem to know more about your hometown then even you do.

Does that mean your IP address changes? Yes, actually. When you log

Continued on pg.2

Continued from pg.1

into a new WiFi, you get assigned a new local IP address. This is a big reason why Internet users have beefed up their cybersecurity by using **virtual private networks**, especially when using public WiFi.

Benefits of VPNs

Virtual private networks (VPNs) allow you to browse the web anonymously. Instead of identifying your machine as well as its location, VPNs hide the IP address so your search history remains clean and disconnected from you. Trackers can't follow, cookies won't work, and advertisers will have a hard time following you from website to website. Say goodbye to those sidebar ads for camping equipment because you Googled a s'mores recipe three months ago.

Why else does privacy matter? Public WiFi is inherently unsafe. Without password protection, hackers can more easily use it to capture your sensitive information when you use the same network they are on. With a VPN, you can more safely browse in public spaces even if you need to check your bank statement or sensitive work emails.

VPNs have another use, though. IP addresses also broadcast the location of your computer. Say, however, that you really wanted to watch a show that's only available in the UK, and you're outside of it. As the middleman to your internet connection, VPNs will broadcast your location as the same place where the VPN servers lie. Therefore, you could purchase a VPN that both hides your activity and makes it seem like you're operating from within the UK. There are free VPN services too, but those tend not to let you choose where you want to appear to be from.

Conclusion

IP addresses aren't inherently good or bad, scary or safe. They're like your driver's license; identifying a machine and where it lives. There's just an inherent danger of that private, identifying information falling into criminal hands. Understanding what IP means and how you or others might use that information lets you make your own decisions about when to stay anonymous online. When you're using public WiFi, for instance, it's not really anyone's business where you're logging in from while you transfer around some funds and approve a couple of orders.

Technology competence and cybersecurity go hand in hand. The more you know about the machines you rely on every day, the safer you'll be using them — no matter why or where you go.

Free Executive Guide Download:
The Business Owner's Guide To IT Support Services And Fees

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

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

Claim your FREE copy today at
https://www.cti-mi.com/itbuyersguide-723/

Security Corner

3 Smart Ways To Hide Your Searches In Public

Our modern world is extremely digitized; because of that, we constantly use Internet-connected devices, even when we're on the go. Here are 3 ways you can make sure you're a little more secure next time you do it.

Biometric Identification
Do you need a PIN or a passcode to open your mobile device? If not, then your mobile data is at risk from anyone walking by.

Adding biometric identification as a way to access your phone prevents anyone from unlocking your mobile device without your face or fingerprint, thereby making it much more secure.

Virtual Private Networks
VPNs are pretty popular for anonymous browsing from your desktop computer, but did you know that there are also VPN mobile apps ready to secure your smart phone, too?

Privacy Screen
Did you know that there are physical ways to protect your phone screen from wandering eyes? Most smart phones come with a screen protector … but did you know that some can actually darken your screen to passersby?

Whether through extra security steps or simple hardware accessories, these three tips above will help you better protect your phone searches while in public.

For more information about staying safe while online and other cyber threats, call us at 248-362-3800 or visit: https://tinyurl.com/3us4y3v9

Is Your Online Shopping App Invading Your Privacy?

Online shopping has become a common activity for many people. It's convenient, easy, and allows us to buy items from the comfort of our homes. But with the rise of online shopping, there are concerns about privacy and security.

Not all shopping apps are created equally. Often people get excited and install an app without checking privacy practices. Apps can collect more data from your smartphone than you realize. Whether you use your phone for personal use, business use, or both, your data can be at risk. So can your privacy.

Shady Data Collection Practices from Popular Shopping App SHEIN

Recently, security experts found a popular shopping app spying on users' copy-and-paste activity.

This app was tracking users' keystrokes, screenshots, and even their GPS location. This raises the question: Is your online shopping app invading your privacy?

SHEIN is the app in question, and it's a popular shopping app with millions of users. According to reports, researchers found the app collecting data from users' clipboards. This included any text that users copied and pasted. This means that if the user copied and pasted sensitive information, the app would have access to it. Including things like passwords or credit card numbers.

Not only that but the app was also found to be tracking users' GPS location. SHEIN was also collecting data from device sensors, including the accelerometer and gyroscope. This means that the app was able to track users' movements. As well as collecting information about how they were using their device.

The app's developers claimed that the data collection was for "optimizing user experience." A very vague explanation that's used by other app developers as well. The developers stated that the collected data was only used for internal purposes. But this explanation wasn't enough to please privacy experts. Those experts raised concerns about the app's data collection practices.

Temu Data Collection Practices Questioned
This isn't the first time people caught an app grabbing data without users' knowledge. Many popular apps collect data from their users, often for targeted advertising purposes.

The popularity of the shopping app Temu has been exploding recently. Since the app appeared in a Superbowl Ad in 2023, people have been flocking to it.

But Temu is another shopping app with questionable data collection practices. Some of the data that Temu collects includes:

- Your name, address, phone number
- Details you enter, like birthday, photo, and social profiles
- Your IPS address and GPS location (if enabled)
- Your browsing data

Tips to Protect Your Privacy When Using Shopping Apps
• ***Know What You're Getting Into (Read the Privacy Policy)*** – Yes, it's hard to stop and read a long privacy policy. But, if you don't, you could end up sharing a lot more than you realize.

• ***Research Apps Before You Download*** – It's easy to get caught up in a fad. You hear your friend talk about an app, and you want to check it out. But it pays to research before you download.

• ***Shop on a Website Instead*** – You can limit the dangerous data collection of shopping apps by using a website instead. Most legitimate companies have an official website

Small Business Tips To Get You Ready For The Unexpected

What would you do if your business suffered a ransomware attack tomorrow?

Do you have a contingency plan in case of any disaster? The unexpected can happen anytime, and small businesses can get hit particularly hard. Here are 10 helpful tips to get ready for anything:

1. Create a Contingency Plan
2. Maintain Adequate Insurance Coverage
3. Diversify Your Revenue Streams
4. Build Strong Relationships with Suppliers
5. Keep Cash Reserves
6. Build Strong Outsourcing Relationships
7. Check Your Financials Regularly
8. Invest in Technology
9. Train Employees for Emergencies
10. Stay Up to Date

Learn How To Fight Business Email Compromise

A significant cyber threat facing businesses today is Business Email Compromise (BEC). BEC attacks jumped 81% in 2022, and as many as 98% of employees fail to report the threat.

What is Business Email Compromise (BEC)?

BEC is a type of scam in which criminals use email fraud to target victims. These victims include both businesses and individuals. They especially target those who perform wire transfer payments.

"Cancel that call to tech-support. This may be beyond their capabilities."

CartoonStock.com

BEC attacks are usually well-crafted and sophisticated, making it very difficult to identify them.

Scammers send emails to employees, customers, or vendors. These emails request them to make payments or transfer funds in some form. The email will often contain a sense of urgency, compelling the recipient to act quickly. The attacker may also use social engineering tactics. Such as posing as a trusted contact or creating a fake website that mimics the company's site.

According to the FBI, BEC scams cost businesses about $2.4 billion in 2021.

How to Fight Business Email Compromise

BEC scams can be challenging to prevent. But there are measures businesses and individuals can take to cut the risk of falling victim to them.

- Educate Employees
- Enable Email Authentication
- Deploy a Payment Verification Processes
- Check Bank Transactions.
- Establish a Response Plan
- Use Anti-phishing Software