Tech Times

IT Support and Technology News from Networking Solutions / October 2020

What Private Browsing Can and Can't Do

As you surf the web, it's nearly impossible to keep your internet activity completely private. Certain websites collect personal information for marketing purposes and your browser keeps track of all the websites you visit. That browsing information can also fall into the wrong hands, which is why you should consider using private browsing if you want to keep your online activities to yourself.

What is private browsing?

Your web browser — whether it be Chrome, Edge, Firefox, Safari, or Opera — remembers the URLs of the sites you visit, cookies that track your activity, passwords you've used, and temporary files you've downloaded.

This can be convenient if you frequently visit certain pages, can't remember your login details, or if you're trying to recall a website you visited a few days ago. But if someone else uses or gains access to your computer, your most private (and embarrassing) internet activities are exposed for anyone to see.

With private browsing — also called Incognito Mode in Chrome and InPrivate Browsing in Edge — all the information listed above does not get recorded. In fact, all the websites and information you accessed in the private browsing session are immediately discarded without a trace as soon as you close the browser. This can come in handy when you're using a public computer because you're instantly logged out of all the accounts you accessed after closing the window.

Your cookies also won't be tracked. In a normal browsing session, sites like Facebook will display highly targeted ads based on the sites and pages you've visited. But in private browsing mode, your internet activity can't be tracked by marketing companies.

Another benefit of private browsing is that you can use it to log in to several accounts on the same site, which is useful if you need to log in to two different online accounts at the same time.

What are the limitations of private browsing?

Although private browsing does prevent your web browser from storing your data, it doesn't stop anyone from snooping on your online activities in real time. If your computer is connected to the company network, system administrators can still track what you're browsing, even if you're in Incognito Mode.

Also, if spyware or keylogger malware is installed on your computer, hackers will still be able to see what you're doing online. Even though private browsing has quite a few benefits, you shouldn't solely depend on it for online privacy. Instead, you should use a virtual private network (VPN) when you go online. These encrypt your internet connection and prevent anyone from intercepting your data. And don't forget to use a strong anti-malware program to scan your computer and keep spyware and other malicious web monitoring software at bay.

If you want to know where you can get these solutions or learn more about web browser security, call us today. We have the tools and expert advice you need to prevent anyone from snooping on your internet browsing.

Article posted in https://www.techadvisory.org

4 Things to Consider Before Selecting an MSP

Incorporating technology into business operations can be challenging given its complexity and constantly evolving nature. Many companies simply can't keep up — this is why many of them are turning to managed IT services providers (MSPs) to handle their tech needs.

MSPs defined

MSPs are companies composed of specialists from various IT fields. They deliver various IT services (e.g., cloud computing, cybersecurity, backup and disaster recovery) and proactively manage their clients' IT systems under a subscription model.

Selecting the best MSP

While there are many MSPs out there, not all of them are equipped to meet your company's unique needs. You can only achieve optimum IT results by selecting the right MSP.

Keep in mind these criteria when choosing an MSP:

- **Depth of skills and experience** – Any MSP should have the skills and experience that go beyond basic software installation, maintenance, and upgrades. They should also have strong expertise in advanced IT functions, such as database management, cloud technology, security, and cross-platform integration, so they can keep up with your company's growing IT requirements.
- **Financial stability** – With IT being the backbone of your business operations, you need an IT partner who will be there for the long haul. Assess their stability by looking into their annual reports and financial statements. Check how many clients they have and their customer retention numbers. Also ask the MSP to provide customer references and testimonials.
- **Competitive service level agreement (SLA)** – An SLA is a contract that dictates the standards that your MSP should be able to meet. It should be able to answer these questions: Do they offer 24/7 support? Can they conduct remote and on-site support? What is their guaranteed response and resolution times? If they fail to meet their committed service levels, are there corresponding rebates or penalties.
- **Third-party vendor partnerships** – Pick an MSP with an ongoing relationship with the technology vendors (e.g., Microsoft, Oracle, Salesforce) whose products you already use in your IT environment. What type of partnership does the MSP have with those vendors? The higher the partnership level, the more vendor certifications the provider has, which means they can bring a lot of expertise to your business.

Choosing the right provider is a very important step that will impact on the performance and success of your business. If you want to learn how MSPs can support your business, contact us today. 916.696.7200

Article posted in https://www.techadvisory.org

3 Ways to Browse the Net Safely at Work

Amidst the current climate of malware, hacks, and phishing scams, companies must take precautions when accessing the internet. Without safeguards, browsers that you or your employees use are vulnerable to cyberattacks that may cripple productivity and profit. Here are steps that your company should take to browse the net safely.

Prevent browser tracking
If you don't like the idea of a third party (reputable or otherwise) being able to track your browsing habits, enable private browsing using built-in tools in your internet browser such as Chrome's incognito mode. This offers protection against tracking by blocking third-party cookies as well as malware. Some browser extensions also boast secure Wi-Fi and bandwidth optimization and can guard against tracking and data collection from social networking sites such as Twitter and Facebook.

Block adverts
While online ads may seem harmless, the truth is they can contain scripts and widgets that send your data to a third party. A decent ad blocking program will stop banner, rollover, and pop-up ads, and prevent you from inadvertently visiting a site that may contain malware. Many blockers contain additional features such as the ability to disable cookies and scripts used by third parties on sites, the option to block specific items, and options to "clean up" Facebook, and hide YouTube comments.

Consider setting up a virtual private network (VPN)
Unfortunately, browser tracking and adware are not the only internet nasties that you need to be concerned about. Hackers can intercept sensitive data between two parties, allowing them to steal and corrupt valuable information such as bank details, login credentials, and other personal information. Installing a VPN can help solve this problem. VPNs encrypt your internet traffic, effectively shutting out anyone who may be trying to see what you're doing.

Install antivirus and anti-malware software
Finally, it goes without saying that having antivirus and anti-malware software installed on your PC, tablet, and smartphone is crucial if you want to ensure your online safety. These software programs are your first defense against malicious parties intent on stealing your data.

Article posted in https://www.techadvisory.org

Happy Halloween!

Tech Times

Microsoft CERTIFIED Systems Engineer

IT Support and Technology News from Networking Solutions | September 2020

"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!" - **Jon Cooper, CEO** | Networking Solutions |916.696.7200 | jcooper@networkingsolutions.net

Cyber Tips | Subscribe | Internet Vigilance | Working Remotely

✨ Introducing Our New Employee ✨

Marketing Coordinator
Sidney Dorris

NETWORKING SOLUTIONS
950 Fulton Ave. Suite 200
Sacramento, CA 95825

Please Join us for our Zoom Webinar

Who is Protecting You from Cyber Criminals?

Do you want to know the most effective ways to keep your sensitive information safe? Join us at our upcoming webinar, as our partner, ID Agent shares their knowledge on securing your data, as well as securing your business.

October 8, 2020 at 11:00 AM

Please email sdorris@networkingsolutions.net to attend our webinar and your chance to win an Amazon Gift Card!