



CYBER DIGITAL WORLD

NEWSLETTER

Volume 8: Issue No. 1

April 2022

PCDS CELEBRATES 1 YEAR



Dr. Ronald Walcott
Managing Director

On Thursday 7th, April, Precision Cybertechnologies and Digital Solution Limited (PCDS) celebrated its one-year anniversary. Cybercrime has increased exponentially globally and even right here in Trinidad and Tobago. As such, one of our strategic initiatives is to assist and inform organizations about the importance of understanding their cybersecurity posture, particularly as it relates to their digital transformation strategy.

One of the ways we intend to do just that is by offering an anniversary gift to corporate T&T, as the country re-

turns to full operation. Twenty companies are set to benefit from PCDS's celebrations. Our gift to you will be to assist 20 companies with a FREE Cybersecurity Assessment for your organization to have a better understanding of your cybersecurity posture, maturity, vulnerabilities, and exposures, along with recommendations for remediation.

We've read about the benefits of VPNs and how they can add a layer of security to our network and devices. An integral part of our computer usage revolves around searches which usually take place through a browser. Most people would be familiar with the top three are Google Chrome, Firefox, and Microsoft Edge. While many browsers

do include some level of security, there are still privacy and security threats that you are vulnerable to. Even in private browsing or incognito mode, you expose specific data to third parties.

Cyber-secure means staying up to date and taking precautions, as no system is 100% secure. Many secure browsers exist, which add more robust privacy and security features. They help prevent tracking and software vulnerabilities and even keep you anonymous. It should be noted that even the most secure applications have flaws.

RISKS WITH INSECURE BROWSERS

An insecure browser is easy to infiltrate. It can allow malware and spyware to be installed on users' computers without their knowledge.

A web browser that is not safe can allow hackers to take control of your computer. As a result, hackers can



In this Issue:

PCDS CELEBRATES 1 YEAR

**HEADLINE NEWS:
INCREASED ENTERPRISE
USE OF IOS, MAC MEANS
MORE MALWARE**

UPCOMING EVENTS



access and steal information. They could even use your computer to commit other crimes.

If you store your bank and financial details on your PC, an insecure web browser can be used as a gateway through which attackers can gain access to that vital information.

Also, most insecure web browsers are used by advertisement companies to gather your online history to create targeted ads. Although this might look harmless, it is gross misconduct of the browser company to breach user privacy.

SECURE BROWSERS

You need to ensure your web browser has vital privacy and protection features. Below are some of the things that make a browser secure:

- Has a Built-in VPN or a VPN Extension: The built-in VPN

feature will allow you to browse the internet hassle-free from any third-party monitoring. It is worth noting that subscribing to a dedicated VPN service provider is always the best bet.

- Has a Built-in or Malware Checker Extension: A malware checker is an essential feature as it allows you to surf the internet comfortably without the worry of malware. Some websites and portals on the internet contain malware that has the potential to steal your data and destroy your device.
- Boasts an Auto-Update Function: A web browser that does not have an auto-update function is an insecure web browser. That is because of the security risks and vulnerabilities attached to a web browser that does not have such a feature. An outdated browser is a bad idea due to its vulnerability to being hacked and attacked.

- Should have added privacy options: A credible secure web browser should present its users with a wide array of privacy features and options. For example, it should allow you to disable data monitoring activity whenever you want. Also, a quality privacy-focused browser should have basic privacy settings such as ad blocker and incognito mode.

Two known browsers that are quite secure;

Brave — Good for blocking ads, prevents browser fingerprinting and has high-level security features.

Tor Browser — Routes your traffic through the Onion network for total anonymity and has secure add-ons, but the extra layers of protection make it slow.

Some browsers utilize a built in VPN to route traffic, however, a dedicated paid service would ultimately carry more benefits. The combination of VPN and secure browser adds an additional layer of security to safeguard users.

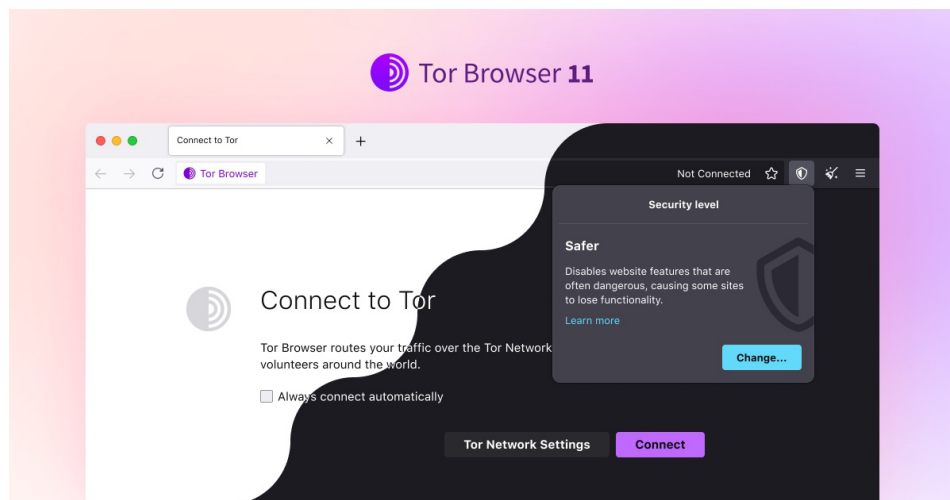


Upcoming Events

VIRTUAL INDIA & SAARC SUMMIT
May 17, 2022

UKI CYBERSECURITY SUMMIT
MAY 24, 2022

FRAUD SUMMIT
JUNE 16, 2022





Frequently Asked Questions:

WHAT IS BROWSER CACHE?

The cache remembers parts of HTML pages and collects data to display information. Cached data includes images, videos, and audio.

When you visit a site that contains graphics, it will store in its temporary storage to enhance your user experience.

When you surf the same website the next time, it will load immediately. It cuts down our loading time.

WHAT ARE COOKIES?

Netscape introduced the concept of cookies. Cookies are the files stored in the storage of the computer that contains user-specific information.

It is a small file that comprises helpful information for the website. Such as password, preferences, and browser.

It tracks information about your visit to a specific site and the time you spend on that site, for example, selection in a form, shopping cart content, or authentication data.

HEADLINE NEWS: Increased Enterprise Use of iOS, Mac Means More Malware



Once, Apple devices were associated with home users and the creative industries, but today their use in the enterprise is more pronounced. Malicious actors have noticed the growing adoption of iOS and macOS platforms in the enterprise and as a result, viruses and malware for MacBooks - once a rarity - are becoming more common.

GROWING FOOTPRINT

According to IDC, macOS devices were used in 23% of U.S. enterprises in 2021, iPhones accounted for 49% of business smartphones and iPads were the most-used tablets in the workplace.

"Growth in Mac usage among business users, especially for employees working remotely and given their choice of PC device, is pushing more businesses to formally adopt management tools and strategies around macOS, along with iOS/iPadOS and tvOS," said Phil Hochmuth,

program vice president, enterprise mobility and client endpoint management, IDC, Boston.

Alcyr Araujo, founder and CEO of Mosyle, a Florida-based provider of MDM and Apple enterprise security solutions, tells Information Security Media Group that a new generation of workers is embracing Apple devices, especially in startups. He says that in 10 to 15 years, "Apple devices will be highly relevant in the enterprise."

While there is a perception of Apple devices as inherently secure, a lax attitude to securing Apple devices with the notion that these devices are secure by default could be a costly mistake for enterprises. Apple devices must be included in security assessments and auditing, as applicable to other devices, data and resources within the enterprise.

Source: databreachtoday.com



868-610-7237



salesinfo@precision-cyber.com



www.precision-cyber.com



1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad