The Tech chronicle

TSA PreCheck

According to a report recently released by Abnormal Security there's been a huge upsurge of instances of people getting scammed after visiting what they thought were Global Entry, NEXUS, and TSA PreCheck service sites. The issue is that scammers are building very convincing fakes of these types of sites and charging busy travelers $140 for pre-check service. Naturally they are not delivering anything at all after pocketing the money.

The surge in such activity began back in March of this year (2021) but has steadily intensified since then. That's no great surprise really.

After all with the holiday travel season fast approaching we can conclude that the purpose of the instances earlier in the year were to give the scammers time to refine their approach in advance of the much busier holiday season. They were anticipating a big boost in travel as the pandemic began to recede.

December 2021

This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Hackers Are Stepping Up Their Game This Holiday Season

The holiday season has almost arrived, and more Americans are expected to turn to online shopping this year than ever before. The ongoing pandemic, combined with convenience, makes online shopping an obvious choice for most consumers.

Unfortunately, online shopping has been muddied with hackers and cyberthieves since its debut. There are still safe places on the Internet where we should feel comfortable to shop, though. If you are careful about where you spend your money or share your personal information, online shopping can feel just as safe as entering a store.

Here are our five best tips to ensure that your online holiday shopping is safe and secure.

Stick To Secure Websites

When shopping online, you want to ensure that every site you visit is secure. Look at the browser bar when entering a new site. If there is a small padlock icon to the left of the web address, the site is secure and you should feel safe to continue. Google Chrome goes an extra step and will label unsecure sites as "not secure" so you know to stay away. Another quick way to tell if a site is secure is by looking at the web address. If it begins in "https," you're good to go. If the "s" is missing at the end and it starts with "http," the site is not secure, and you should find somewhere else to shop.

Don't Be Afraid To Use Your Phone

You can shop on your phone just as easily as you do on your computer, and the portable aspect should not worry you. Major corporations like Amazon and Walmart have secure

Continued on pg.2

Continued from pg.1

apps with seemingly unlimited items to purchase. Making purchases directly on apps avoids the hassle of going to the company's website, where your connection might not be as secure. It also helps to set up an Apple or Google Pay account, as businesses will not be able to get your bank account information from these sources.

If you do decide to shop on your mobile device, make sure that you are not on public WiFi. Public WiFi is rarely secure, and using it could make you an easy target for hackers. They could get any personal information you enter while on the WiFi. It's better to bookmark the products and purchase them when you are on a private connection.

Use A Password Manager

To keep your information secure, it's imperative to utilize strong and complex passwords that are difficult to crack. Avoid using personal information and using the same password across accounts. To make things easier for yourself, utilize a password manager to keep track of all of your different passwords. This way, you can create complex passwords that even the best of hackers can't figure out. Make sure to use a mix of uppercase and lowercase letters, numbers and special punctuation to make the most secure password possible.

> **"If you are careful about where you spend your money or share your personal information, online shopping can feel just as safe as entering a store."**

Take A Pass On Amazing Deals

If you come across a price that just seems too good to be true, chances are it probably is. If you search for an item on a search engine, you may see prices way lower than those of major retailers. These options could be on unsecured sites as a front to try to steal your information or it could be someone who doesn't actually have the item trying to make a quick dollar. While the deal might seem like something you can't pass up, it may cost you more in the long run, and you might not even get the product.

Pay Attention To Bank Statements

You won't always know when someone gets access to your personal information or bank accounts. By paying attention to your bank statements, you can catch overcharges or purchases that you did not make. Always use a credit card when shopping online because hackers will not be able to access any of your actual money. Most credit cards come with fraud protection that prevents you from being liable for charges you never actually made.

As long as you take the necessary precautions, shopping online is a safe and financially responsible practice. If you follow these tips, your holiday shopping will go as smoothly as possible.

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

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 go.ctmaryland.com/ITbuyersguide

Zero Trust Architecture

As a part of an ongoing effort to ensure all systems are secure, we are taking new security measures to protect all our managed systems.

Following the Executive Order on Improving the Nation's Cybersecurity 3a, the Federal Goernment is adopting a Zero Trust Architecture to secure infrastructure and systems.

We are implementing steps to help keep your home systems, SOHO systems, Office systems, Servers more secure than ever before by providing a Zero Trust Architecture upgrade.

This will help stop the rogue programs from running from systems that have often gone without detection.

Attacks are growing and increasing in aggressiveness as well as their covert way of infiltrating our systems that we rely on daily.

We provided some basic information regarding Zero Trust. If you have any questions, please feel free to reach out and see how easy it is to add this next-level protection to your systems.

As always, we are always on the look out to better secure your systems and help you stay safe.

A Winning Strategy To The Game Of Building A Business

Life isn't always easy. Sometimes we sit back and expect things to happen for us or we simply do as we're told and expect great things, but it's not always that easy. While defensive mindsets can be beneficial in some areas, if you want your business to grow, then you need to play aggressive offense.

I first got into real estate not long after Black Monday and the recession that hit in the early '90s. At the time, many other realtors relied on defensive tactics. They waited by the phone for prospective buyers to contact them or they waited at an open house for potential buyers to walk in. But that's not how you get business.

I had no prior training in real estate when I entered, but that didn't stop me from becoming a dominant force in the field. We didn't have millions of dollars to buy subscribers or begin a widespread advertising campaign. Instead, we went after highly targeted strategic partners and I keynoted at large conferences to build our subscriber base. We came out of the recession with more than 5 million subscribers because of our aggressive actions.

During various recessions, companies that have made a point of being aggressive in their campaigns have seen great growth. During the Great Depression in the 1920s, Post was the dominant leader in the breakfast market. They decided to cut their advertising while one of their competitors, Kellogg's, decided to double theirs. Kelloggs's profits grew by 30% during the recession, and they became the top dog in the market, where they have remained ever since.

During the energy crisis of the 1970s, Volkswagen, the car import leader of the time, cut growth spending. Toyota decided to double its spending focused on marketing and growth and became the #1 car import company. Volkswagen was bumped down to fifth. Toyota is still the leader of car imports and is three times larger than Volkswagen.

Elon Musk is one of the greatest offensive businessmen of the last century. In 2016, South Australia's electrical grid was knocked out due to a devastating storm. Elon tweeted that he could provide 100 megawatts of storage in 100 days or less. This would have been the largest battery in the entire world at that point, and Elon won the bid. He produced the battery within 60 days.

The greatest way to grow your business into an empire is by taking an offensive approach. It's been proven time and time again by some of the greatest names in business.

While Darren Hardy was growing up, his father always told him to be the exception. He has taken this philosophy and applied it to his many pursuits in the world of business. Darren has remained at the forefront of success media for over 25 years and is not stopping anytime soon.

Tesla Took This Lesson From Ford's 112-Year-Old Playbook

Ford has been a dominant first in the auto industry since the very beginning. Henry Ford once said, "Any customer can have a car painted any color that he wants, so long as it is black." It now looks like Tesla is following Ford's direction.

While other auto companies are focusing on providing more options to their customers, Tesla has scaled back. Tesla offers a third of the color and model choices when compared to its competitors, but their stock value is much higher than most. Tesla has improved their stock value by doing what it does best instead of attempting to appease every customer.

This same thought process can be applied to business. Businesses that try to do everything to win all customers instead of focusing on their true base usually lose out to the competition. The most successful companies limit their options and make the choice for the consumer easy.

You're Not Getting The Most Out Of Your CRM If You're Not Using This Tool

Businesses use CRMs to provide better service to their customers by organizing and automating certain aspects of the business. There's a vital tool in many of the major CRMs that is unutilized in many businesses. The ticket/case function can be used to address and keep a record of issues reported by clients.

When this function is used in CRMs, it can ensure that the problem is sent to the right person who is capable of addressing the issue. It can catch these problems early and will inform other users of this error so it can be fixed quickly. This helps meet the customers' needs while seeing if there are hidden faults lying beneath the surface of the product or service. A knowledge base can even be created to keep a record of all these problems so that customer service representatives can provide fast service to resolve any consumer issues. Regardless of the size of your business, the ticket/case tool is a valuable resource.

How To Attract Clients With A Connected Culture

When it comes to creating a successful business, hiring a dedicated and engaged team makes all the difference. If you have unhappy employees, chances are that you also have unhappy customers.

Building an engaged team starts with setting core values for the company. If all employees believe in the company's core values, they will have a better work experience. Once you have a team in place that believes in the values, work on creating positive connections. Positive connections help make the workplace enjoyable. Consumers are more likely to buy based on emotion, and a happier employee will create a better encounter for the customer. Creating a culture that everyone buys into goes a long way toward growing your business.

THREATLOCKER®

Protecting Against Fileless Malware Threats

ThreatLocker® RingFencing™ protects businesses against fileless malware by controlling what applications and code a hijacked processes can run.

Fileless Malware is a type of malware that only exists in memory. It does not run from the computer's hard drive like most types of malware.

Malware embedded in a Microsoft Office document that downloads and executes a file, then removes itself, is often considered as fileless. However, this is not technically accurate, and this type of malware is dealt with differently from true fileless malware (see our Macro Viruses and Malware section). True fileless malware does not save any files to the hard drive and is often very difficult to detect by an antivirus.

Fileless malware can operate using several methods. The most common method is when the application that opens a document is able to download and run a script using a built-in windows application such as Rundll32. The script is loaded into memory using RunDll32 and continues to run unbeknownst to the user.

A less common method in fileless malware operation is active when a vulnerability is exploited in an application, such as a PDF reader. A script attaches itself to that process and can be used to copy or CryptoLocker your data. This method is more relevant for computers that are not patched.

ThreatLocker Application Control, in combination with our RingFencing™ technology, is able to control fileless malware by monitoring application behavior and stopping it from stepping outside its normal boundaries. If an application attempts to perform actions that fall outside of acceptable behavior, ThreatLocker® Application Control blocks the action, stopping the threat in its tracks. In addition, even if the application is vulnerable, ThreatLocker is able to RingFence™ the application, so the amount of damage caused by fileless malware or a rogue application is massively reduced.

THREATLOCKER®

"ThreatLocker has given us the control we needed, without causing overhead on our I.T. Resources" - Danielle Hutcheson, Business Manager - Lake Forrest Preparatory School"

How ThreatLocker® helps with real life problems

A user receives an email with a file that executes a program on your computer. Antivirus is unable to detect most of today's malware, which can allow an attacker remote access to your system.	ThreatLocker® blocks all software that is not allowed by your I.T department, virtually eliminating the risk of malware enabling an attacker to gain control. ThreatLocker's whitelisting solution is as close to a silver bullet as you can get.
A user opens a PDF which directly attaches itself to the process, by reading code from an HTTPS site. It is impossible for antivirus to detect this code, which encrypts all of the files on your shared network drive.	ThreatLocker® Ring Fences your applications, so they can only access the data they need to. This massively reduces the risk of a data breach from a hijacked process without interrupting users.
A rogue employee copies customer data files to a USB drive before leaving for a competitor company.	ThreatLocker® Storage Control lets you decide what data can be copied to storage devices, and data that is copied is recorded in a detailed audit.
When trying to download some legitimate software, a user accidentally clicks on the Ad link which has a similar download button. The software contains malware.	ThreatLocker® identifies applications from our built-in database and blocks the user from executing software that is not permitted
A user receives a Word document by email, that when opened swaps out a system DLL file to malware.	ThreatLocker® maintains a system database of all Windows Update files and their matching hash. In the case of a file modified or replaced ThreatLocker® blocks the modified file.