Newsletter

Celebrating 31 years serving Central, N.C. *September 2021*

5 Ways to Strengthen Cybersecurity in a Hybrid Workplace

Currently, employees are more connected than ever. The hybrid workplace is here to stay, and for employees, this means relying on connected devices from their home office setups. According to recent data, Smart home systems will rise to a market value of $157 billion by 2023, and the number of installed connected devices in the home increases by a staggering 70% by 2025. In this new normal where Smart devices are constantly online and safety is a must, here are some tips for securing those devices.

Remember, Smart devices need smart security

Make cybersecurity a priority when purchasing a connected device. When setting up a new device, be sure to set up the privacy and security settings on web services and devices, bearing in mind that you can limit with whom you share information.

Put cybersecurity first in your job

Make cybersecurity a priority when you enter a new role. Of course, good online hygiene should be part of any organization's onboarding process, but if it is not, then take it upon yourself to exercise best practices to keep your company safe. Some precautions include performing regular software updates, patching, and enabling Multi-Factor Authentication any time it is available.

Make passwords and passphrases long and strong

Whether or not the website you are on requires it, be sure to use at least 12 characters, combine capital and lowercase letters with numbers and symbols to create the most secure password. Generic passwords are easy to hack. If you need help remembering and storing your passwords, do not hesitate to turn to a password manager for assistance.

Never use public computers to log in to any accounts

While working from home, you may want to change scenery and work from a coffee shop or another type of public space. While this is a great way to keep the day from becoming monotonous, use caution to protect yourself and your company from harm's way. Ensure that security is always top of mind, especially while working in a public setting. Imagine that all your online activities are visible and that should help you stay safe. If you must connect securely from a public WiFi at the coffee shop or airport use your phone as a hotspot and make sure it is on the cellular not the WiFi network.

Turn off WiFi and Bluetooth when idle

Upcoming Events

Lunch & Learn: Cyber Insurance, Why It Is Important for Your Business
September 22, 2021

5th Annual Cybersecurity Panel Discussion
October 7, 2021

Webinar: Safeguard Your Organization from Growing Cyber Threats
October 19, 2021

For more information on our upcoming events, please visit www.tcsusa.com.

The uncomfortable truth is, when WiFi and Bluetooth are on, they can connect and track your whereabouts. So, to stay as safe as possible, if you do not need them, switch them off. It is a simple step that can help alleviate tracking concerns and incidents.

These are just a few simple steps towards achieving the best online safety possible. Staying safe online is an active process that requires constant oversight at every stage - from purchasing and setting up a device to ensuring that your day-to-day activities are not putting anyone at risk. By following these steps, you are doing your part to keep yourself and your company safe from malicious online activity.

Why You Cannot Buy Cyber Insurance Without Multi-Factor Authentication

Insurance policies are designed to help you manage risk, and right now, cybersecurity risk is through the roof.

There are so many infected websites and automatic malware programs out there that even if every hacker gave up the Internet for life, hacks would continue for a decade or more after their departure. The cost of a data breach, unfortunately, is also higher than ever.

Today, one lost archive of client data could lead to hundreds of identity theft incidents, possibly thousands. The necessary post-breach recovery process can often cost a company into the millions. Rebuilding the breach, paying data security fines, notifying and compensating affected parties, and rescuing your data is a deep investment, one most companies aren't prepared for when a hack or malware strikes. This is the purpose of cyber insurance.

However, an insurance provider will not grant a policy to any company that does not have multi-factor authentication, or MFA.

What is MFA and Why Does My Cyber Insurance Require It?

MFA stands for Multi-factor authentication. Each MFA is an alternative to a traditional password, acting as a second layer of protection for authorized access. Anything an employee might need to log-in for, MFA gives them a second way to authenticate. Sometimes, your team may choose which method they prefer to login with. Others, the second method will be used to double-confirm the identity and authorization of the user.

When it comes to hackers and stolen accounts, MFA often trips up a hacker who has stolen the primary password - unprepared for a second question or test only the user would know.

Cyber insurance requires businesses to have an MFA because they can significantly reduce the risk of both remote and internal hacks. Considering that 50% of businesses were hacked remotely and 33% were hacked internally, this is an essential precautionary measure. Insurance companies survive by reducing the risk that a claim will be necessary. Multi-factor authentication has been found to be a reliable indicator of a business that has a much lower malware risk.

Types of Multi-Factor Authentication

So what counts as Multi-Factor Authentication in the eyes of your cyber insurance provider? A 2FA or 2-Factor Authentication must be made of two different categories of authentication. Two passwords would not be sufficient, but a password and a PIN would be. Of course, your company can choose from a full selection of potential second-factor authentication options and letting your team choose their own second factor both tailors the method to their memory and adds an element of randomness to stop methodical hackers.

Here are the types of multi-factor authentication to choose from:

- PIN Number
- Security Questions
- Fingerprints and Biometric Data
- Emailed Authentication Tokens
- Image-Based Codes
- Phone SMS Authentication Tokens
- Previously Downloaded Token File
- Third-Party Authentication

How to Protect MFA Security Integrity

Just as passwords can be compromised, so too can any MFA unless we protect its integrity. Here's how you can ensure your MFA methods really do add an extra layer of anti-hacker security.

Send One-Time Codes with a Time Limit

Minimize the validity of any MFA token or code. Send one-time codes so there's no use in stealing them and provide a limited time window so hackers don't have time to scam or hack their way to a working code.

Provide Creative or Custom Security Questions

A choice of five cookie-cutter security questions often leads to insecure and careless answers. Instead, use a deep well of more personal questions and/or let your team write (or

ad-lib) their own security questions for custom and more obscure security answers.

Assess Risk-Based Factors

Pay attention to factors that might indicate a hacker. For example IP or MAC address, the location of the user, and even time of day can flag a log-in as suspicious. A hacker in another city might give themselves away simply by not being at the hacked account-holder's home or work.

How to Get MFA for Your Business

So how do you get the multi-factor authentication your team needs for full cyber insurance coverage? Turn to your IT team or internal team. If your team is swamped or you don't have internal IT, do not sweat it. An outsourced professional or team can help you set up your system with MFA defenses on your network and your enterprise software. Once MFA is built for your business and you're team has designed their secondary (and beyond) alternate logins, you'll be ready to secure your business with a well-built cybersecurity insurance policy.

Contact us today to discuss your business IT services and MFA implementation needs.

Cyber Insurance, Why It Is Important for Your Business

Date: Wednesday, September 22nd
Time: 11:45 AM ET
Cost: Free
Location: Undercurrent Restaurant, 327 Battleground Ave. Greensboro, NC 27401
Registration: Visit tcsusa.com/events/ or call 336.804.8449
Presenters: Kyle Smythe, President, Pilot Risk Management Consulting and Andy Purcell, Business Consultant, Total Computer Solutions those threats.

Cybercrime is continuously evolving, with many businesses becoming prime targets for cybercriminals. With such a reliance on technology and remote work, cyber risks have become a top-of-mind issue. As a result, organizations can no longer rely on traditional insurance coverage and must consider cyber insurance. In addition, they must take a high-level, comprehensive approach to promote a culture of security awareness to develop their operations.

Key Topics for Discussion

- Overview of Cyber Insurance
- Current Policies and Essential Coverage
- Need for Cyber Insurance--Breaches & Ransomware
- Real-Life Claim Examples
- Ongoing Market Conditions
- New MFA Requirement

This event is following restaurant policies and guidelines for COVID-19. Tables will be socially distanced based on registration.

PILOT
RISK MANAGEMENT CONSULTING

webinar

Safeguard Your Organization from Growing Cyber Threats

Date: Tuesday, October 19th
Time: 11:00 AM ET
Cost: Free
Registration: Visit tcsusa.com/events/ or call 336.804.8449

This past year, the world has seen the most significant increase in cyber-attacks on companies, government, and individuals. The sophistication of these threats is continuing to increase. The costs of cleaning up a breach can be devastating, both from a financial and a PR standpoint. Therefore, it is essential to protect your data proactively by effectively educating your workforce about the security threats and ensuring they understand how to protect their computers and your company from those threats.

Key Topics for Discussion

- Minimizing the Risk for Ransomware
- Protecting Corporate Network and Wireless
- Safeguarding Remote Workers
- Educating Your End-Users in Phishing Attacks

Attend this webinar to understand better how to protect your organization from cyberattacks and increase your security awareness.

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Is Your Team Prepared to Prevent Cyber Breaches?

SCHEDULE YOUR FREE ON-SITE CYBERSECURITY AWARENESS TRAINING TODAY!

During this 30-minute presentation, we will help your team become aware of how hackers try to attack your network and educate employees on how to protect your business.

CALL 336.804.8449 OR EMAIL INFO@TCSUSA.COM TO SCHEDULE YOUR TRAINING TODAY!

Mention This Offer