Newsletter

Celebrating 30 years serving Central, N.C. *October 2020*

TCS Teams Up with Industry Experts for 4th Annual Cybersecurity Panel Discussion

Do you know how to provide security for your organization? Would you like to know how to keep your business safe? Are you worried about cybersecurity threats, but you do not know where to start? 80% of the problem is solved by having the right cyber practices and steps in place, rather than the latest advanced technology.

The 4th Annual Panel Discussion is being brought together for business owners, entrepreneurs, or those interested in cybersecurity, wherever they are, in an all-virtual experience scheduled for October 22nd. The panel will share their expertise and pass along essentials for a cybersecurity plan.

"Unfortunately, many companies do not take cybersecurity seriously until they suffer an attack and real damage," commented Barry Utesch, President, Total Computer Solutions. "Hopefully, our panel discussion will open some eyes that this aspect of IT services needs to be a top priority. There are teams of criminals lurking everywhere online searching for cybersecurity vulnerabilities they can use for their profit and gain."

The panelists will include FBI Cyber Crime Investigator, Adam Scholtz, HIPAA Privacy Expert, Karen Schaede, Partner, Revolution Law Group, SonicWall Security Solutions Expert, Rudy Messex, Cyber Liability Specialist, Murphy Holderness, Marsh & McLennan, and Director of Communities of Excellence, Steven Hunt. This level of expertise and experience from the cybersecurity world is well-rounded and ensures attendees a great deal of value.

The "4th Annual Cybersecurity Panel Discussion" will occur virtually on Thursday, October 22nd, 2020, from 9:00 AM – 10:30 AM.

The panel discussion is free, but registration is required. Register for tickets to this event at https://www.tcsusa.com/events/. If you have any questions, please call 336.804.8449.

DON'T GET TRICKED THIS OCTOBER
TREAT YOURSELF WITH
CYBERSECURITY AWARENESS MONTH
STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH

Upcoming Events

LIVE Webinar: How to Protect Your Business from Cyber Attacks
October 6, 2020

LIVE Virtual: 4th Annual Cybersecurity Panel Discussion
October 22, 2020

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

What to Do After Clicking a Disastrous Malicious Link

It is a Friday night. You are exhausted from the work week. The bed is calling your name, but you are on your laptop, opening up emails from family, friends, and your favorite store is alerting you about its sale for the weekend. All of a sudden you get a new email.

You rub your itchy, half-shut eyes, and open the email out of curiosity. Supposedly your bank is asking you to change your account's password. You click on the attached link, unaware that the bank is not even the one you use.

Your stomach drops, heat surges through your body. You are wide awake now. An expecting page uploads. Your screen reads: MALWARE detects on your computer, take action. You want to press okay, but your mind is telling you otherwise.What if this happened to you? Do you know what to do after clicking a malicious link or a virus?

In today's world, you may face this scenario. Here are a few steps that you should be aware of in case you ever fall victim to a phishing email.

Step 1: Disconnect and Shut Down

First things first, never click 'okay' or 'continue.' This will automatically fill your computer with malware – causing you to lose precious files, downloads, apps, and more. Also, do not just click the 'X,' because if the malicious site uses a JavaScript, then it can still take control of your computer and download malware.

The best response is to hold the power button for 5-7 seconds to 'shut down,' and then unplug your network cable from your computer. When shutting down your computer, do not merely 'sign off' and do not press 'restart.' At this point, if you have an IT partner, call them to see when it is safe to turn your computer back on.

This is not a sure-fire way to stop the malware, but it is the best option that can prevent spreading the malware or virus to other devices.

Step 2: Run a Security Check

Make sure you run a security audit. After rebooting, you might be able to get onto the Internet completely fine, but a virus could have attached itself to your computer before you were able to shut it down.

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

What you do not want to do is go on as if nothing happened, because later on, you might misunderstand why your computer is running slowly or why files are beginning to disappear. If you are not familiar with how to run a check then call a professional for extra support.

Have the partner run a malware check or install an anti-malware that can keep you more secure. It may cost you money, but it will keep you or your business better protected and save you money in the long term.

Step 3: Backup Your Data

Small businesses should back up their data. If you have not, then do not panic, check your files – see if everything you need is there. Begin to backup your data through one of the many Cloud-based sites or install a portable backup device onto your computer.

Step 4: Update Your Passwords

Once you are confident that your machine is clear of malware, another important step is to change your credentials. If malware was found on your computer, or a hacker was able to weasel their way in, the last thing you want is for them to have access to all your private information. As always, create strong passwords and do not reuse passwords for other accounts. If there is ever a necessary time to create new and strong passwords, it is after you fall for a phishing scam.

Tips If You Are Thinking About Clicking

Here are a few other important things to remember:

First, breaking news topics that become big are picked up by hackers because the story interests you. This also happens with popular videos and articles that seem benign at first. You should continuously be wary of flashy news because they often seem normal; at the top of a Google search list or shared through a social media site.

Secondly, if an unknown source sends the email and it seems urgent, you should be wary. Hackers tend to use urgency and fear of loss to make people click links. Just remember, if there is a major issue, then the sender will use various mediums to contact you, such as phone or by mail. So, next time an email asks you to take urgent action, just delete it and communicate with the source.

Third, always check at the bottom of your screen to see if the URL looks shortened or does not use https. Both of these are signs that something could be wrong.

"Malicious Link," Continued

It is easy to fall victim to a phishing email, a malicious link, or a video containing malware. If you need further assistance about what to do after clicking a malicious link, TCS can help. We offer free, no obligation consultations to steer you in the right direction.

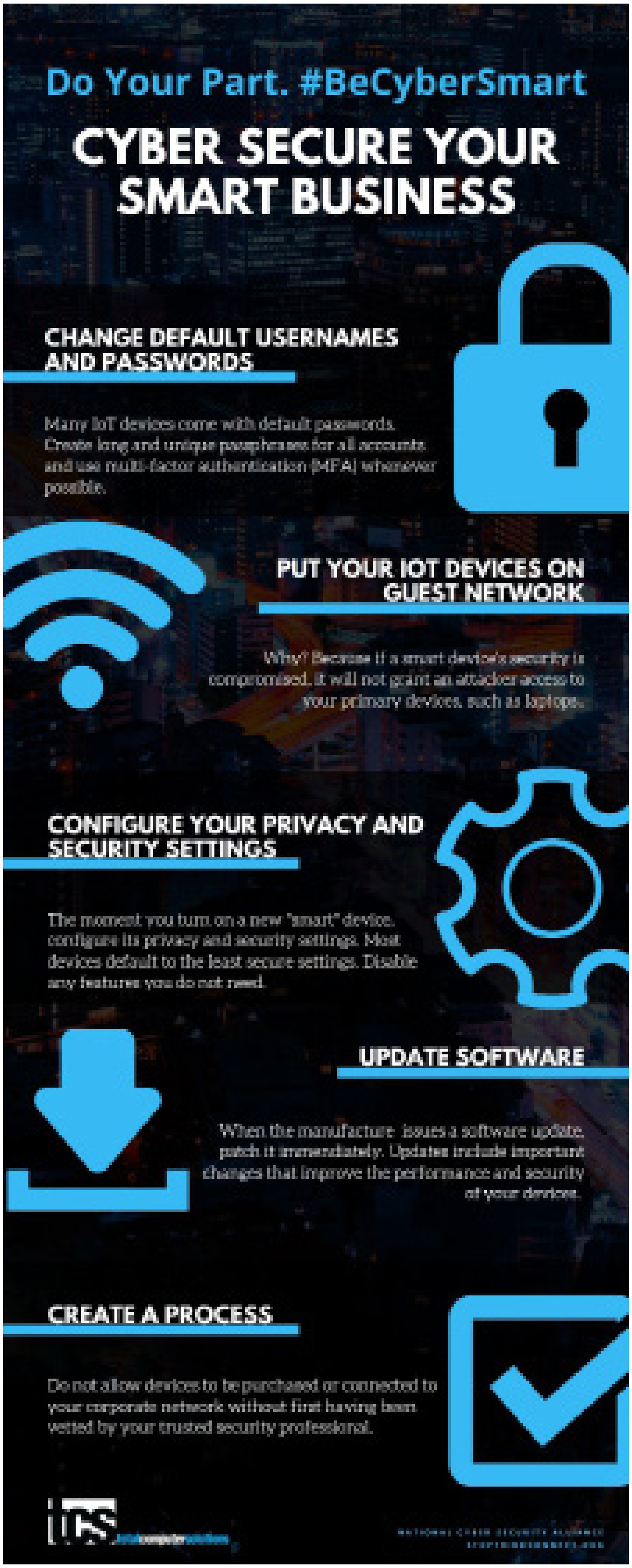
On Demand: Creating a Highly Productive Remote Environment

We had a great time at our live webinar last month, "**Creating a Highly Productive Remote Environment**," presented by *Andy Purcell, Business Consultant, TCS*. This webinar is now available on demand so that you can review important topics covered in the session. To watch the recorded webinar, please visit https://youtu.be/fhnsCyEFILU.

FREE Guide: Protect Your Company from Phishing Attacks

Computer network security is no longer just the responsibility of the IT department instead it is a company-wide effort that requires buy-in from the entire organization. While the news plays up data breaches of large national corporations, it's worth noting a few statistics that point to the truth because any size company is vulnerable. Throughout this guide, we will share how to train your team to spot phishing email, ways to protect your company with a multi-layered security approach and how you can avoid downtime, data loss, and reputation damage.

Get your FREE copy today!
Visit tcsusa.com/resources/e-books/



Do Your Part. #BeCyberSmart

CYBER SECURE YOUR SMART BUSINESS

CHANGE DEFAULT USERNAMES AND PASSWORDS

Many IoT devices come with default passwords. Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) whenever possible.

PUT YOUR IOT DEVICES ON GUEST NETWORK

Why? Because if a smart device's security is compromised, it will not grant an attacker access to your primary devices, such as laptops.

CONFIGURE YOUR PRIVACY AND SECURITY SETTINGS

The moment you turn on a new "smart" device, configure its privacy and security settings. Most devices default to the least secure settings. Disable any features you do not need.

UPDATE SOFTWARE

When the manufacture issues a software update, patch it immediately. Updates include important changes that improve the performance and security of your devices.

CREATE A PROCESS

Do not allow devices to be purchased or connected to your corporate network without first having been vetted by your trusted security professional.

tcs totalcomputersolutions

NATIONAL CYBER SECURITY ALLIANCE
STAYSAFEONLINE.ORG

tcs totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Webinar: How to Protect Your Business from Cyber Attacks

Join us for our upcoming webinar!

Date: Tuesday, October 6, 2020
Time: 10:30 AM ET
Presenter: *Andy Purcell, Business Consultant, Total Computer Solutions*
Registration: Visit www.tcsusa.com/events/ or call 336.804.8449

It is important to protect your data proactively by effectively educating your workforce about the security threats you and they face every day, and ensuring they understand how to protect their computers, and your company, from those threats.

Key Takeaways

- Who is at risk?
- How do cybercriminals get information?
- What can minimize the risk of data breaches?

Attend this webinar to learn what industry leaders are doing to create a layered approach to securing their networks.