Newsletter

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

Total Computer Solutions Presents 5th Annual Cybersecurity Panel Discussion

Do you know how to protect your organization against cybercrime? Would you like to hear from industry experts on how to make your business safe? Are you worried about data breaches but do not know where to start? Small and medium sized businesses are the victim of over 60% of cyberattacks.

The good news for business owners, entrepreneurs, or just those interested in cybersecurity in the extended Greensboro, NC area, a special "Cybersecurity Panel Discussion" is scheduled for October 7. The expert panel will discuss with attendees, cybersecurity, including shared risk scenarios and how to respond in the event of a data breach. The panel will take a realistic look at cybercrime and how businesses can and should protect themselves. Attendees will receive practical tips and guidelines on how to secure their data without damaging their bottom line.

"Many companies don't realize the threat that is posed to them in the cybersecurity domain," commented Ian Collins, Information Security Manager, Total Computer Solutions. "Cyberspace does not have nationally guarded borders like the physical domain. Cyber threats are simultaneously thousands of miles away, and at your doorstep. This panel discussion will help illuminate the threats, responsibilities, and strategies businesses can use to defend themselves."

Collins, who has over five years of experience in the field, will be part of the panel discussion, along with FBI Agent Adam Scholtz, Attorney, Robert Young, Carruthers & Roth, Cyber Insurance Specialist, Ryan Forrester, Coalition, Managing Partner, and Lance Cancro, Home Front Enterprises. This combination of in-depth knowledge and experience from the cybersecurity, IT services world is quite balanced and is sure to deliver attendees a great breadth of knowledge.

The "5th Annual Cybersecurity Panel Discussion" will occur at The Colonnade at Revolution Mill, 900 Revolution Mill Drive, Greensboro, NC 27405, on Thursday, October 7, 2021, from 9:00 AM – 11:00 AM.

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

For more information, be sure to visit www.tcsusa.com and the event's Event page.

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

Upcoming Events

5th Annual Cybersecurity Panel Discussion
October 7, 2021

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

Lunch & Learn: Disaster Recovery: Solutions for a Successful Backup Strategy
November 9, 2021

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

"Panel" Continued

3 Best Practices for Dealing with Phishing Threats

From ransomware to SolarWinds, the cybersecurity space has been as hectic as it has ever been over the last 12-24 months. However, for all the emerging threats and news that are cropping up on the horizon, phishing -- one of the oldest pain points in cybersecurity -- continues to wreak havoc quietly and is as big of a threat as it has ever been.

Despite often being overlooked in the hype, phishing has been a mainstay in the cybersecurity threat landscape nearly ten years. Forty-three percent of cyberattacks in 2020 featured phishing or pre-texting, while 74 percent of US organizations experienced a successful phishing attack last year alone. That means that phishing is one of the most dangerous "action varieties" to an organization's cybersecurity health. As a result, the need for proper anti-phishing hygiene and best practices is an absolute must.

With that in mind, here are a few quick best practices and tips for dealing with phishing threats.

Know the Red Flags

Phishers are masters of making their content and interactions appealing. However, from content design to language, it can be difficult to discern whether the content is genuine or a potential threat, which is why it is so important to know the red flags. Awkward and unusual formatting, overly explicit callouts to click a hyperlink or open an attachment and subject lines that create a sense of urgency are all hallmarks that the content you received could be potentially from bad actors and that it should be handled with caution.

Verify the Source

Phishing content comes in various ways; however, many phishers will try to impersonate someone you may already know -- such as a colleague, service provider, or friend -- to trick you into believing their malicious content is trustworthy. Please do not fall for it. If you sense any red flags that something may be out of place or unusual, reach out directly to the individual to confirm whether the content is authentic and safe. If not, break off communication immediately and flag the incident through the proper channels.

Be Aware of Vishing and Other Phishing Offshoots

As more digital natives have come online and greater awareness has spread about phishing, bad actors have begun to diversify their phishing efforts beyond traditional email. For example, voice phishing -- or vishing -- has become an alternative for bad actors looking to gain sensitive information from unsuspecting individuals. Like conventional phishing, individuals posing as a legitimate organization, such as a healthcare provider or insurer. The call from a native language individual seems perfectly legitimate and they ask for sensitive information. Simply put, individuals must be wary of any communication that asks for personal information, whether via email, phone, or chat -- especially if the communication is unexpected. If anything seems suspicious, break off the interaction immediately and contact the company directly to confirm the integrity of the communications.

Phishing may be "one of the oldest tricks in the book," but it is still incredibly effective. And although it may be hard to spot when your busy at work it is important that you exercise caution and deploy these few fundamentals. Individuals and organizations can reduce the chances of falling victim to a phishing attack.

TCS can help train you staff on the red flags and what to look out for. If you are interested in our cybersecurity awareness training call us today.

5 Cybersecurity Tools to Protect Your Business

When we are more connected than ever, being "cyber smart" is of the utmost importance. This year has already seen more than a fair share of attacks and breaches, including the SolarWinds and Kaseya breaches, as well as high-profile attacks on the Colonial Pipeline and other critical infrastructure. Furthermore, as has been underlined by these recent breaches, cyberattacks are becoming more sophisticated, with more evolved bad actors cropping up each day. Luckily, there are several steps that we can take daily to mitigate risks and stay one step ahead of malefactors.

Here are a few quick tips:

Enable MFA

Multi-factor authentication (MFA) adds that necessary second check to verify your identity when logging in to one of your accounts. In addition, by requiring multiple authentication methods, your account is further protected from being compromised, even if a bad actor hijacks your password. In this way, MFAs make it more difficult for password cracking tools to enable attackers to break into accounts.

Use Solid Passphrases/Password Manager

Using a password manager may seem obvious but securing strong passphrases/password managers is often overlooked. For example, spending more time online during the pandemic

has undoubtedly contributed to more bad actors prowling for accounts to attack. Using long, complex, and unique passwords is a good way to stop your account from being hacked, and an easy way of keeping track and remembering your passwords is by using a password manager.

Perform Software Updates

When a device prompts that it is time to update the software, it may be tempting to click postpone and ignore the message. However, having the latest security software, web browser, and operating system on devices is one of the best defenses against online threats. So, do not wait - update.

Do Your Research

Common sense is a crucial part of maintaining good online hygiene, and an intuitive step to stay safe online is to do some research before downloading anything new, such as a new app. For example, before downloading a new app make sure that it is legitimate by checking who created the app and what the user reviews say. Also, any articles published online about the app's privacy and security features.

Check Your Settings

Be diligent in double-checking your privacy and security settings and be aware of who can access your documents. This extends from Google docs to Zoom calls and beyond. For meetings on Zoom, for example, create passwords so only those invited to the session can attend and restrict who can share their screen or files with the rest of the attendees.

Keeping your business protected from cyber-attacks is critical. If you would like help deciding what procedures or tools are best to keep your business safe.

Employee Spotlight: Adam Spivey

Congratulations to our Analyst, Adam Spivey for recieving his CompTIA A+ certification. Certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. Way to go Adam!!

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.

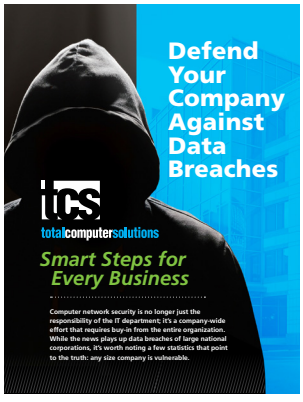
Key Topics for Discussion

- 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.

FREE Guide: Defend Your Company Against Data Breaches

Malware protection software is not enough to defend against today's data breaches. Learn about the number one threat to your network and how cyber criminals may be using your employees to access sensitive company information.



Learn how to train your team to spot a phishing emails, protect your company with multi-layered security, and advoid downtime, data loss, and reputation damage

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

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Upcoming Events!

Total Computer Solutions Presents 5th Annual Cybersecurity Panel Discussion

3 Best Practices for Dealing with Phishing Threats

5 Cybersecurity Tools to Protect Your Business

Employee Spotlight

Safeguard Your Organization from Growing Cyber Threats