Newsletter

Celebrating 29 years serving Central, N.C.! October 2019

Total Computer Solutions Partners with Experts for Cybersecurity Panel- Cybersecurity for Business Owners

Greensboro-based IT support and service provider, Total Computer Solutions (TCS) together with Technology Concepts & Design, Inc. (TCDI), a pioneer in legal technology, will hold a “Cybersecurity Panel Discussion” to address business concerns related to data security October 17, 2019.

Can you stop hackers from invading your network? Would you like to know how to keep your business safe? Are you worried about ransomware, but you do not know where to start? 34% of businesses hit with malware took a week or more to regain access to their data (Kaspersky). These attacks often prove catastrophic to business owners but are just too “minor” to ever appear in national headlines.

The good news for business owners, entrepreneurs, or just those interested in cybersecurity in the Greensboro, NC area, a special “Cybersecurity Panel Discussion,” is scheduled for October 17th. The expert panel will discuss with attendees, cybersecurity, including common risk scenarios and how to respond in the event of an attack.

The panel will take a realistic look at cybercrime and how businesses can and should protect themselves. Explicitly targeted toward small to medium organizations, attendees will receive practical tips and guidelines on how to protect their data without damaging their bottom line.

“Sadly, most companies do not think they are a target for cybercriminals until they suffer an attack and real damage,” commented Barry Utesch, President, Total Computer Solutions. “Hopefully, our panel discussion will open some eyes that security needs to be a top priority. Cybercriminals are everywhere online searching for vulnerabilities within organizations for their profit and gain.”

Utesch, who has over three decades of experience in the field will be part of the panel discussion as the moderator, along with Sr. Network & Security Engineer, Steve Wujek, Data Use Privacy & Security Attorney, Joseph A. Dickinson, and Insurance Consultant, Murphy Holderness. This combination of expertise and knowledge from the cybersecurity, IT services world is well-rounded and is sure to deliver attendees a great deal of value.

The “Cybersecurity Panel Discussion” will take place at the new Hyatt Place Greensboro/Downtown, 300 N. Eugene St., Greensboro, NC 27401, on Thursday, October 17th, 2019 from 7:45 AM - 9:00 AM.

Continued on inside

Upcoming Events

Cybersecurity Panel Discussion
October 17, 2019

Webinar: Windows 7 End of Life
November 13, 2019

CIMP 2019 Conference
November 15 & 16, 2019

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

Continued...

The panel discussion is free, but registration is required. Register for tickets to this event at www.tcsusa.com/calendar/. 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 at https://www.eventbrite.com/e/cybersecurity-panel-discussion-tickets-72147847153 .

Tips on How to Create Stronger Passwords

The fact that you use passwords to protect your personal property or information does not guarantee protection against hackers. Today, websites with extra security protection are also available, but that does not suggest that you are immune to cybersecurity risks.

Individuals who can crack your password are still at large, and once they succeed in their ulterior motives, they can bypass the security protocols you have in place, and that can cost you a fortune. Identifying a strong password for sensitive information or company data is not an option.

Some of the password protection approaches that most individuals opt for include the use of numbers, special characters, and a combination of uppercase and lowercase letters. The other strategy you should consider implementing to secure your password is creating a password phrase with at least 12-14 letters as well as renewing such details once or twice a year.

Here is some insight into how you can create strong passwords:

Avoid Common Words

The temptation to use standard dictionary words when creating passwords is quite high, and that is one of the mistakes you should avoid by all means possible. For instance, there is a surge in the number of people who use the word "password" as their password and opting for a combination of such words as "Island Holidays" is not any better. Using everyday dictionary words as a password will only increase your vulnerability to hacking attacks.

Hackers use a dictionary-based system that can easily crack common words, which suggests that if this is the approach you use when creating passwords, you should stop the habit immediately as a first step towards securing your password.

Using Directly Identifiable Information Is Not An Option

Most individuals do not share details about their postal or home address, phone number, and birthday, with everyone because such information is personal. However, the fact that some individuals know more about you implies that including personal details in your password is not advisable.

Exercising caution when deciding who to trust with your personal information is essential, but using such details in your password acts as bait for hackers seeking to access your online accounts or systems within your organization.

Have Unique Passwords for Separate Accounts

Some individuals operate more than one online account, and one of their greatest fears is forgetting the login details to any of them. The obvious solution, in this case, is using the same password for all your online accounts, which means that recalling such details will not be a challenge. The problem is that when you suffer an attack, hackers will gain access to the information in every online account you own as a result of replicating your password for multiple accounts.

Creating a unique password for separate accounts is a security measure you should not overlook if you have several online accounts. Since recalling passwords for multiple accounts is a constant headache for most users, creating an idea list for strong passwords is advisable, but always remember to keep it safe.

Consider Complex and Lengthy Passwords

The strength of your password will affect the probability of suffering a hack in one way or another. For that reason, adopting long-tail passwords makes it harder for attackers to break into your online account or an organization's systems. The harder it is for hackers to guess your password the safer you are and that is why you should avoid using pet names and your personal information as your password.

Complex and lengthy passwords will require a mixture of numbers, characters, lower and uppercase letters, as well as symbols. Educating employees on the necessity of complex and lengthy password is also critical because it will not only safeguard their details, but it also acts as a safety precaution against hackers targeting company data.

Have Unique Passwords for Separate Accounts

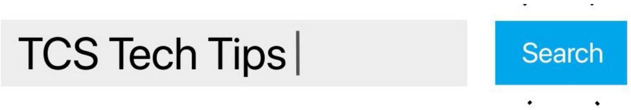
Some individuals operate more than one online account, and one of their greatest fears is forgetting the login details to any of them. The obvious solution, in this case, is using the same password for all your online accounts, which means that recalling such details will not be a challenge. The problem is that when you suffer an attack, hackers will gain access to the information in every online account you own as a result of replicating your password for multiple accounts.

Creating a unique password for separate accounts is a security measure you should not overlook if you have several online accounts. Since recalling passwords for multiple accounts is a constant headache for most users, creating an idea list for strong passwords is advisable, but always remember to keep it safe.

Consider Complex and Lengthy Passwords

The strength of your password will affect the probability of suffering a hack in one way or another. For that reason, adopting long-tail passwords makes it harder for attackers to break into your online account or an organization's systems. The harder it is for hackers to guess your password the safer you are and that is why you should avoid using pet names and your personal information as your password.

Complex and lengthy passwords will require a mixture of numbers, characters, lower and uppercase letters, as well as symbols. Educating employees on the necessity of complex and lengthy password is also critical because it will not only


TCS Tech Tips

Watch our new TCS Tech Tip videos! Visit tcsusa.com/resources/tcs-tech-tip/ to find tips and tricks to help keep you more productive.

Digital Newsletter

If you would like to receive our newsletter digitally, please visit tinyurl.com/ycqvv2r6.

Follow us on social media!

TCS Spotlight: Darren Smith & James Moore

Last month we celebrated our Customer Strategy Managers, Darren Smith and James Moore for their continued leadership at TCS. Both have been on different teams, at different levels, and with different team mates, but each time they have led from the heart with passion to make TCS a better place to work and better for our customers.

This February Smith celebrated 17 years and Moore celebrates 14 years of service with the company this month. "You both represent the core values of TCS and in this moment of change and growth of TCS, I think you have represented the core value of integrity to the n'th degree by thinking less of yourself and more for the growth of the employees and TCS" congratulated Chris Barker, Operations Manager.

Last Call for Windows 7

If you are still using Windows 7, now is an excellent time to consider an upgrade. Starting January 14, 2020, less than one year away, Microsoft will no longer support Windows 7. After that you are on your own, your operating system will no longer receive technical assistance, updates or security patches.

Older PCs can be upgraded to Windows 10 if they are meeting the minimum requirements set by Microsoft. However, we recommend that users and businesses get a new computer instead of upgrading their older machines.

Often small and medium size business owners focus on short term costs, using the end of life software and hardware can end up costing you more money than it is worth.

When you are unable to complete transactions for clients, or your computer that continually stops or stalls during presentations and video conferences eventually will hurt your reputation. A computer that loses data can cost you a fortune.

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue:

Kickoff Cybersecurity Awareness Month with a Cybersecurity Panel Discussion

Join us for our upcoming panel discussion!

Date: Thursday, October 17, 2019
Time: 7:45 am - 9:00 am
Location: Hyatt Place Greensboro/Downtown
Cost: Free

Panelists:
Steve Wujek, Sr. Network & Security Engineer, TCDI
Joseph A. Dickinson, Data Use Privacy & Security Attorney, Smith Anderson
Murphy Holderness, Insurance Consultant, Marsh & McLennan

Moderator:
Barry Utesch, President, Total Computer Solutions

To register for this event, visit www.tcsusa.com/calendar/ or call 336.804.8449. This event is free and a light breakfast will be provided.