



# Newsletter

Celebrating 29 years serving Central, N.C.!

April 2019

## Total Computer Solutions Receives “Best Christian Workplace Certification”



Total Computer Solutions (TCS) is proud to announce that it has been awarded two years in a row the “Best Christian Workplace” certification by The Best Christian Workplaces Institute (BCWI). This award makes TCS, the only Managed Service Provider in North Carolina to have received this award.

“It makes me so happy that we have received this award twice,” said Mrs. Shaun Floyd, Service Manager for TCS. “TCS is a strong company built on a Christian foundation and I am very glad to be a part of it.”

Christian-owned and biblically-focused, Total Computer Solutions’ mission statement reads “Our Mission is to glorify God as we provide exceptional IT services focused on building relationships with our clients and employees.”

This serves as a reflection of how the company desires a culture of not only exceptional professional services but a company that actively promotes strong values and positive actions that have an impact within the office and throughout the community and world.

Total Computer Solutions has decades of experience providing managed technology solutions to meet the specific needs of businesses, giving them the time and expertise necessary to keep technology from disrupting productivity.

“We have used this survey for the past three years, each year we have taken the employee’s feedback and improved multiple issues that were a concern of the employees,” said Chris Barker, Operations Manager. “The employees appreciate an opportunity to provide feedback to the company and we are grateful for their input in order to improve their work environment.”

“Our leaders are proud members of C12 and cultivate a company culture that promotes Biblical values and positive actions, which not only affect the TCS family but the community,” said Floyd.

Total Computer Solutions has been partnering with companies throughout Central, North Carolina for more than 29 years for everything from consultation to outsourcing. Those interested in learning more about Total Computer Solutions can read the company’s services profile at [www.tcsusa.com](http://www.tcsusa.com).

## Upcoming Events

**Cybersecurity Panel Discussion**  
*April 11, 2019*

**Backup & Disaster Recovery Lunch & Learn**  
*May 9, 2019*

**Night at the Hoppers**  
*May 17, 2019*

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

## Next Steps After Clicking a 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 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. The page that uploads is not the one you were expecting. 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?

Whether you know this feeling or not, this scenario has a chance of happening to you at home or work. There are a few steps that you should be aware 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 only 'sign off' and do not press 'restart.' At this point, if you have an IT company, 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. What you don't want to do is go on as if nothing happened, because later on, you might question why your computer is running slow or why files are starting to disappear.

If you are not familiar with how to run a check then call a professional for extra support. Have the tech 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.

### Step 3: Backup Your Data

Small businesses should be backing up their data, but if you were not, then do not panic, check your files - see if everything you need is there. Begin to backup your data through one of the plethora of 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 you cannot dismiss is changing 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 perfect time to create new and strong passwords, it is after you fall for a phishing scam.

### Tips If You Are Thinking About Clicking

There are a few other important things to remember:

- First, breaking news topics that become big are picked up by hackers because they know you will click on the website or link for more information. This also happens to popular videos and articles that seem benign at first, but are only a disguise. You should continuously be wary because they often can be at the top of a Google search list or shared through a social media site.
- Secondly, if an unknown source send the email and it seems very urgent, you should be wary. Hackers tend to use urgency and fear of loss to make people click the email's link. Just remember, if there is a major issue, then the sender will use various mediums to contact you, such as by 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.

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.

## Total Computer Solutions Teams Up with Experts for Cybersecurity Panel



Managed IT leader, Total Computer Solutions together with FBI Special Agent, Adam Scholtz, and Certified Ethical Hacker Garrett Baltezegar will hold a “Cybersecurity Panel Discussion” to address business concerns related to data security on April 11, 2019.

Does cybersecurity concern you? Would you like to know how to make your business safe? Are you worried about data security breaches, but you do not know where to start? Over 94% of data breaches involve small and medium-sized businesses (WFLA). These breaches 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 extended Greensboro, NC area, a special “Cybersecurity Panel Discussion,” is scheduled for April 11th. The expert panel will discuss with attendees, cybersecurity, including common 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. Targeted specifically toward small to medium businesses, attendees will receive practical tips and guidelines on how to secure their data without damaging their bottom line.

“Sadly, 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 around everywhere online searching for cybersecurity vulnerabilities they can use for their profit and gain.”

Utesch, who has over three decades of experience in the field will be part of the panel discussion, along with FBI Special Agent Adam Scholtz, Certified Ethical Hacker, Garrett Baltezegar, and HIPAA Privacy and Security expert Karen McKeithen Schaede, Attorney, Connors Morgan, PLLC. 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 deal of value.

The “Cybersecurity Panel Discussion” will take place in the Revolution Mill Gallery Room, 1250 Revolution Mill Drive Suite 123, Greensboro, NC 27405, on Thursday, April 11th, 2019 from 8:00 AM - 9:00 AM.

The panel discussion is free, but registration is required. Register for tickets to this event at [www.tcsusa.com/calendar/](http://www.tcsusa.com/calendar/). If you have any questions, please call 336.804.8449.

For more information be sure to visit [www.tcsusa.com](http://www.tcsusa.com) and the event’s Event page at <https://www.eventbrite.com/event/cybersecurity-panel-discussion-tickets-54663739717>.

## 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.

If you would like more information or help to assess the age of your workstations, call today for a no-obligation consultation at 336-804-8449.

TCS Tech Tips |

Search

Watch our new TCS Tech Tip videos! Visit [tcsusa.com/resources/tcs-tech-tip/](http://tcsusa.com/resources/tcs-tech-tip/) to find tips and trips to help keep you more productive.

## Digital Newsletter

If you would like to receive our newsletter digitally, please visit [tinyurl.com/ycqv2r6](http://tinyurl.com/ycqv2r6).



168 Thatcher Road  
Greensboro, NC 27409

### In this Issue:

- Total Computer Solutions Receives “Best Christian Workplace Certification”
- Next Steps After Clicking a Malicious Link
- Total Computer Solutions Teams Up with Experts for Cybersecurity Panel
- Last Call for Windows 7
- TCS Tech Tips
- Panel Discussion

## Cybersecurity Panel Discussion

Join us for our upcoming panel discussion!

**Date:** Thursday, April 11, 2019

**Time:** 8:00 am - 9:00 am

**Location:** Revolution Mill Gallery Room, Greensboro, NC

**Cost:** Free

### Panelists:

*Adam Scholtz, Special Agent, FBI*

*Garrett Baltezegar, IS Security Manager, Liberty Healthcare Management*

*Karen McKeithen Schaede, Attorney, Connors Morgan, PLLC*

*Barry Utesch, President, Total Computer Solutions*

To register for this event, visit [www.tcsusa.com/calendar/](http://www.tcsusa.com/calendar/) or call 336.804.8449. This event is free and a continental breakfast will be provided.

