Newsletter

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

The New & Improved TCS Website

We are excited to finally unveil a more enhanced and functional website that will work better for you. We set out on this project to make the TCS website faster, easier-to-use, and accessible across most devices.

Quick Access to Solutions & Resources

One of the main objectives for the website redesign is to provide current and prospective clients answers and solutions for their problems quickly and efficiently. With faster loading times and a more centralized approach, visitors can now link to most of their needs from the website's home page.

Through the home page, users can learn how technology is a competitive advantage. We have also emphasized showcasing current clients and how they leveraged technology to become more productive and how future clients can partner with TCS to grow their companies.

From the homepage, you will be able to view the latest blog posts, social media activity, and industry news and from the resources tab, visitors can access case studies, e-books, and our newsletter.

Current clients can submit a service ticket or track existing service tickets quickly through the links provided at the top of the home page, as well as access remote support and support website services.

Simplified Web Design For Your Convenience

The TCS website's simplified design makes it easier for visitors to find what they need in a manner that makes sense rather than clicking through various layers of information. We have identified our services and solutions to help guide you to the resources needed to answer your questions and technology needs. The site will be updated frequently and valuable content and resources will be added; including articles, blogs, important announcements, and training videos.

Accessibility Across Most Devices

Understanding that our customers live busy lives and demand accessibility from a variety of different access points and devices, the redesigned website kept this in mind and ensures the site is a pleasant and useful experience across a multitude of devices.

A Website That Works For You

Our goal at TCS is to give organizations the time and expertise to keep up with changes in technology.

Upcoming Events

Roundtable Discussion: Life in the Cloud: Security & Backups
June 17, 2020

Webinar: Disaster Recovery- What's Your Backup Plan?
June 25, 2020

Webinar: Office 365 User Management & Administration
July 23, 2020

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

"TCS Website," Continued

We are confident that the newly designed website will enhance your experience and allow for easier access and lead to quicker IT solutions for your business.

We look forward to your web visit and any feedback you may have about the new features and designs. To send us any feedback regarding your experience on the redesigned website, please email us at info@tcsusa.com.

10 Ways to Secure Your Microsoft 365 Business Account

Securing a Microsoft 365 account requires careful attention. While Microsoft offers excellent ways to securing workstations and servers, it is ultimately up to you to put this in play.

One place to start is to check your Microsoft 365 Secure Score to identify areas that need improvement. Also, Microsoft recommends the following ten steps for improving 365 security. Some of these steps require Office 365 Advanced Threat Protection (ATP).

Multi-factor Authentication

What applications do you need to protect with multi-factor authentication?

Passwords can be guessed or stolen. Multi-factor authentication (MFA) adds a second form of identification; usually, by a code sent to the user's cell phone. Setting up MFA eliminates the intruders need to have only one password to breach your account. The Microsoft 365 administrator can enable MFA for one account or multiple accounts at once. Users will be prompted to enter their confirmation phone number the next time they log in to set up MFA.

User Training

Do your employees know what a phishing attack looks like?

If not, they may be more vulnerable to clicking on malicious links or visiting dangerous websites. Reducing human error is a crucial element of cybersecurity. Security awareness training will train them how to recognize phishing emails and other tricks. They will learn how to avoid giving out confidential information and downloading malware. Online user training is a necessary approach, more so than ever, because of the increasing sophistication these criminals use.

Dedicated Administrative Accounts

Do you have a dedicated network administrator account?

An outsider who gains control of an administrative account can do severe damage. Best practices call for using these accounts only when they are needed. Administrators should have separate accounts with limited privileges for routine tasks such as email and Web browsing. Administrators should log out of their admin accounts when they are not in use and should always have a strong password and multi-factor authentication.

Protection Against Email Malware

Does your email block malicious email attachments?

Certain kinds of attachments, such as executable files, are especially dangerous. Opening a malicious executable attachment will cause immediate damage. Microsoft 365 includes an administrative option to block these attachment types. The administrator can set a company-wide filter and customize the blocked file types from the Security & Compliance Center.

Protection Against Ransomware

Are your employees contacting your IT department as soon as they notice fishy emails in their inbox?

If ransomware is installed onto a machine, it encrypts important files and presents a demand for payment. This is usually an email with an executable attachment or an Office file that contains macros. In addition to blocking dangerous file types, the administrator can set up a warning whenever a user receives an attachment that could have macros. Users should be instructed to open these files only if they're expecting them and to disable macro execution by default.

Stop Email Auto-Fowarding

Do you allow auto-forwarding when an employees leaves or is on vacation?

Automatically forwarding all mail to a second account is sometimes useful. However, an intruder who gains access to a user's mailbox can change these settings to forward email to an unauthorized account. The user is not likely to notice. The Exchange admin center allows setting a rule to prohibit auto-forwarding to an external domain. The setting will not interfere with forwarding to another address in the same domain.

Office Message Encryption

Are you encrypting highly sensitive information?

If you would like to receive our newsletter digitally, visit www.tcsusa.com/newsletter/.

"Microsoft 365," Continued

Usually, email sends without encryption. Anyone on the Internet who intercepts a message can read it. Microsoft 365 allows encrypted mail to other users of the service, as well as to certain other services, including Gmail and Yahoo. This option is available in the Outlook mail client or Outlook.com.

Protection Against Email Phishing

Do you have a anti-phishing policy in place?

Fraudulent emails can catch anyone off guard. The best protection against phishing emails is to block them from reaching inboxes. With Office 365 Advanced Threat Protection, the admin can set up an anti-phishing policy. By using the default policy or custom rules. Anti-phishing can check for spoofed and unauthenticated sender addresses and take specific actions, including marking a message as junk or moving it to quarantine.

Advanced Threat Protection Safe Attatchments

Does your organization send and receive a lot attachments?

Dangerous email attachments are not easy to spot. Office 365 Advanced Threat Protection includes Safe Attachment protection as an option, but it has to be enabled. It covers not just email but SharePoint, OneDrive, and Teams. When enabled, it will block email attachments when it detects malware. The setting is in the Security & Compliance Center, under Threat Management.

ATP Safe Links

What security measures do you have in place to ensure those websites are linking to the intended site versus rogue websites to deliver a form of malicious software?

Email and files from disreputable sources may hold links to malicious websites. Office 365 Safe Links, another feature of ATP, guards against unintentionally opening those links. You can set options for Microsoft 365 apps to be checked against known blacklisted domains and prevent them from being opened.

The more thorough you are carrying out these tasks, the lower the chances are of a costly intrusion. Setting the priorities that will give your Microsoft 365 accounts the security you need is a complex matter. We can help you by setting up a security consultation. If you have any questions regarding your Microsoft 365 business plan or want to increase the security of your account, contact Total Computer Solutions at 336.804.8449 or visit www.tcsusa.com.

Employee Spotlight: Bill Gwaltney

Congratulations to our Analyst, Bill Gwaltney for receiving his CompTIA Security+ Certification! Security+ incorporates best practices in hands-on trouble--shooting to ensure security professionals have practical security problem-solving skills. Way to go Bill!

Roundtable Discussion: Life in the Cloud: Security & Backups

Date: Wednesday, June 17th
Time: 9:00 A.M. - 10:30 A.M. ET
Registration: Visit www.tcsusa.com/events/ or call 336.804.8449

Join industry leaders as they share their thoughts on cloud security and backups along with ways to safeguard your business from data loss.

Over the past decade, many organizations have taken advantage of cloud computing's benefits. The cloud has increased productivity and driven profit margins while providing versatility for data storage and access to business information anytime, anywhere. While these benefits boost the bottom line, cloud provider's servers and security are not enough to guard against malicious activity, nor are their "backups" enough to safeguard against data loss.

Speakers:

- *Larry Guthrie, Technical Solutions Architect, Cisco*
- *Rudy Messex, Security Solutions Consultant, SonicWall*
- *Murphy Holderness, Business Consultant, Marsh & McLennan*

Moderator:

- Andy Purcell, Business Consultant TCS

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Webinar: Disaster Recovery: What's Your Backup Plan?

Join us for our upcoming webinar!

Date: Thursday, June 25th
Time: 11:00 AM ET
Presenter: *Andy Purcell, Business Consultant, Total Computer Solutions*
Registration: Visit www.tcsusa.com/events/ or call 336.804.8449

The need for an effective backup plan is a necessity for all organizations that rely on secure data. While the disaster recovery needs vary from business to business, there are elements of a backup plan which are common and will be discussed in this webinar.

Key Topic for Discussion:

- Disasters that can interrupt your business operations
- Consequences from lack of access to data
- Potential solutions for small or medium-sized businesses
- How to develop a well designed backup plan

At this event, you will learn how to keep your data safe, available, and recoverable so that your organization can stay productive.