Newsletter

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

Best Network Security Tools for Your Business

In the age of digital transformation, every business is entrusted with sensitive information from customers, suppliers, and associates. No business is too small to attract the attention of the ever-expanding world of 21st Century cyber-crime.

Whether we call them hackers, the dark web, or malicious actors, the risk of data breaches and network intrusion by any name is usually summed up by the professionals in the network security field as “not a question of if an attack will occur, but when.” With that sobering warning in mind, we will review the essential tools and practices which can prevent and deter security breaches at your business.

Antivirus Software

Antivirus software provides protection by scanning computer files and memory to detect patterns or “signatures” that indicate the presence of known malware programs. The keys to optimized antivirus protection are to scan regularly and ensure that the antivirus software is continuously updated. New and updated malware is identified by antivirus providers on a daily basis, and it is essential to keep antivirus definitions current so the software can effectively detect, block, and cleanse new forms of malware from the system.

Firewalls, Access Controls, and Privileges

Firewalls enforce access control between networks such as an organization’s LAN and the risky environment of the public Internet. The firewall functions as the front door security guard, blocking or permitting traffic and even aiding in the apprehension of offenders. The firewall protects in 3 ways:

1. It blocks incoming data which could be a cyber-attack.

2. The firewall uses NAT (Network Address Translation) to hide network information. Outgoing information appears to have originated at the firewall rather than the actual network address. A good firewall should conceal its IP address as well as IP addresses on the LAN. To launch an attack, hackers need to know the IP address of the target.

3. Limits Internet use or access to remote sites by screening outgoing traffic.

Firewalls not only block attacks, but they can alert network administrators when an attack is detected and track the data back to the malicious sender.

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

Upcoming Events

Webinar:
How to Fully Protect Your Data in the Office 365 Cloud
March 16, 2021

Webinar:
The Major Causes and Solutions for Downtime
April 20, 2021

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

The usual best practice for firewall setup is to configure it to deny access to all incoming traffic, and then open discriminating incoming traffic gates as required for operations.

Patches & Updates

By now it is obvious that updating antivirus and security software is critical, but all software updates can optimize performance as well as security. Patches plug holes and security weaknesses discovered in software and operating systems. Hackers are quick to share this information and black hat coders go to work to exploit these specific vulnerabilities. Updates also remove outdated features, fix bugs, update drivers and add the latest new improvements. The best practice for updates is to install and restart as soon as they are available. Choosing the "Remind me later" option can leave the network door open to known threats.

Strong Passwords

The most sophisticated firewalls and IDS can all be defeated by a single compromised password. The password is the key that can get a hacker inside the firewall where he can masquerade as a legitimate user and wreak havoc on the network. Any Network Use Policy should include strong passwords as a priority, following the guidelines below:

- 12 characters or longer. The longer, the better.
- Contain a combination of upper and lower case letters.
- Include at least one numeric and/or special character (&, @, etc.), punctuation, and spaces.

Using a complete sentence as a passphrase or easy to remember mi55pelling$ simplifies the use of strong passwords. All personnel should be briefed on phishing scams which entice a user to reveal a password and best practices for maintaining strong password integrity.

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.

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 ability to use 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 educate 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

“Microsoft 365” Continued

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 are 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?

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 (ATP) Safe Attachments

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.

Get a Security Consultation

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 TCS.

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

In this Issue

LIVE Webinar: How to Fully Protect Your Data in Office 365 Cloud

Date: Tuesday, March 16th
Time: 11:00 AM ET
Presenter: *Michael Brown, Technical Analyst, Total Computer Solutions*
Registration: Visit tcsusa.com/events/ or call 336.804.8449

You are invited to join us for our upcoming webinar, "**How to Fully Protect Your Data in Office 365 Cloud**".

A staggering 60% of companies that lose data close within six months of the loss. Data loss can be a significant concern for Office 365 users because Microsoft's security and backup policies cannot defend you against malware or guarantee a thorough and rapid restore of lost data. Microsoft does what they can to safeguard their customers, but they do not specifically specialize in security or data backup and recovery. Therefore, the customer is responsible for keeping their organization's data safe in the cloud.

Data loss and the concern surrounding it can be easily avoided by following and implementing security guidelines and policies and having a backup and recovery solution in place.

Key Topics for Discussion

- Ways to keep your email secure
- Advantages of third party backups
- Importance of partnering with a Managed Services Provider