ISSUE 55 AUGUST 2022

Newsletter

What's Inside:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

Cyber Threats and How They Impact You!

In the past few decades, our society has grown to depend on technology, which has been a remarkable progression for us all. However, there will still be people out there looking to take advantage of you in some way, shape, or form. Online threats vary and show no discrimination between individuals, small businesses, large corporations, or even the government itself. No matter what, you want to have a layer of protection in place before you're targeted for an attack.

Leading into 2022, cyber-attacks have become and continue to be a growing concern for small to medium-sized businesses. The cost of cybercrimes reached $2.7 billion in 2020 alone according to FBI's Internet Crime Report. The workload that small business owners already have on their plate was enough, let alone trying to survive through the pandemic. It is difficult to process when a cyber-attack is taking place, and following that, all the things that go into reporting it. It's a lot to handle. Your best option is to have protections put in place to avoid an intrusion of any sort. Prevention is possible. Let's explore why small to medium-sized businesses are prime targets for cybercriminals, the common attacks used, and what protection options will best serve your needs.

Why Small To Medium-Sized Businesses Are The Ideal Targets

One main reason that small to medium-sized businesses are appealing targets to cybercriminals is that they typically lack the security infrastructure that large businesses and corporations have in place. Many companies have limited time to devote to any cybersecurity and simply can't afford professional IT solutions. With their gates wide open, cybercriminals jump at the opportunity to infiltrate and retrieve personal information or a desired amount of money to transfer.

The shift in remote and hybrid offices has created new opportunities for hackers to take advantage of new vulnerabilities and gaps in security. This doesn't mean that you should get rid of remote workers or hybrid offices altogether. It simply means that you should become more aware of the cracks that can give way to attacks. What is astounding is that more companies have a higher concern about ransomware, data breaches, and major IT outages than supply chain disruptions, natural disasters, or even the COVID-19 pandemic. The impact of any of these circumstances can vary from minimal to catastrophic.

Continued on page 2.

CONTINUED...

One of the best things you can do as a business owner is be prepared and have preventative measures in place. Before you get to that step, you need to know as much information about cyberattacks and cybersecurity as possible. The more you know, the better you will feel putting preventative measures in place. Plus, if an attack does take place, being well versed in what is taking place will help you solve the issues more efficiently and proficiently.

Common Types Of Attacks On Small To Medium-Sized Businesses

A cybercriminal can penetrate 93% of your company's networks. With such a high number at risk, it's surprising that more small to medium-sized businesses don't invest in cybersecurity. In addition to that statistic, cybercrime has gone up 600% since the COVID-19 pandemic. We completely understand the financial strains at play with small businesses; however, being passive on cybercrime activity and failing to implement solutions to protect your business can lead to catastrophic events.

What are the most common ways for cybercriminals to ruin your business? While cyberattacks are constantly evolving, there are 4 common types that owners of small to medium-sized businesses should be aware of: malware, viruses, ransomware, and phishing. Here are the definitions of each one:

1. **Malware** (i.e., malicious software) is known as an umbrella term referring to software intentionally signed to cause damage to a client, computer, server, or computer network. This can include ransomware and viruses.
2. **Viruses** are programs that are harmful and intended to spread from one computer to the next (as well as other connected devices). They are used by cybercriminals to gain access to your system.
3. **Ransomware** is a specific type of malware. It infects and restricts access to a computer or device until a ransom is paid. This will typically happen through phishing emails and exploiting unpatched vulnerabilities in your software.
4. **Phishing** is a type of cyberattack that everyone in your office who utilizes a work email should be trained on. It uses email or a malicious website to infect your machine with malware or it can collect your sensitive information.

Now that you know what type of attacks can likely happen to your business, what can you do about it?

Preventative And Protection Options For Your Needs

Every business is different. Their needs will vary, especially when it comes to any IT-related services. If small to medium-sized businesses are looking for preventative and protective options, the best place to start is finding a managed service provider. What does your company gain from this option? You will now have access to dedicated security professionals that have the proper expertise needed to improve your unique cybersecurity. They will provide expert-level configuration of security solutions, which is exactly what you need.

A managed service provider tailors your needs to the proper services for protection. This means that you won't be guessing whether certain applications or devices in place will be beneficial. You will most likely end up saving money if you hire the right provider that is looking out for not only your needs but also your wallet. They will deliver services such as network, application, infrastructure, and security with ongoing and regular support alongside active administration. As every business has its varying needs, your managed service provider will customize their services to provide the ultimate preventative measures and protection for you.

If you want more information regarding the impact of cybercrime on small to medium-sized businesses and service options with a managed service provider that will benefit you and your organization, contact us today. Regardless of your business size, the benefits of a long-term relationship with a knowledgeable and reliable provider are essential for creating a thriving company. RJ2 Technologies can provide you those resources and will work as an extension of your team to implement timely and quality solutions.

RJ2 SPOTLIGHT

Kevin Dann

Dispatch Engineer

Kevin Dann has been in the professional field since 2012. He started his career in the telecommunications field working as a project designer for Fullerton Engineering. Kevin joined RJ2 as an intern from 2010-2012 working onsite with engineers and as a recruiter. In 2019 he became a full-time employee at RJ2 as a Dispatcher Engineer.

Fun Fact: Kevin once met Zachary Levi out in downtown Chicago.

Where's your favorite place in the world?
- Vail, Colorado

What do you like to do when you aren't working?
- Catching up on my Netflix series

What is the best career lesson you've learned so far?
- You miss 100% of the shots you don't take

If you could meet anyone in the world, dead or alive, who would it be and why?
- Walter Payton, he was my childhood athlete I'd always looked up to

What is your favorite part of working at RJ2?
- Working alongside my colleagues

Mitigating Microsoft 365 Security Risks:

Choosing the right software and services is critical to your business's success. And when it comes to cloud-based tools and services, Microsoft 365 is one of the best, as it offers powerful features and cost-saving benefits. But as with any technology, Microsoft 365 comes with security challenges. In this article, we will discuss some of the most common security risks associated with the productivity suite and how you can mitigate them.

Infected File Synchronization

Like most cloud services, Microsoft 365 allows users to automatically sync files stored on their devices to the cloud, such as in OneDrive. However, this useful feature is not without security risks. If a locally stored file is infected with malware, OneDrive will view the file as changed/updated and trigger a sync to the OneDrive cloud, with the infection going undetected.

Microsoft Defender for Cloud Apps is a great tool against malware infection. Part of Microsoft 365 Defender, this app is designed to enhance protections for Office 365 apps. It also provides great visibility into user activity to improve incident response efforts. Make sure your organization's security administrators set this up on your systems so you can detect and mitigate cyber risks as soon as they arise.

Security Risks in Dormant Applications

Some organizations using Microsoft 365 often don't use all the tools and services included in the productivity suite. For instance, your organization might use programs like Word, Excel, and SharePoint every day, but rarely use OneDrive. Unfortunately, dormant applications may be prone to attack. To counter this, it's ... crucial to identify unused apps and have an administrator tweak user settings to restrict availability on these apps.

Unprotected Communication Channels

Phishing attacks and malware are two of the most common ways cybercriminals infiltrate a system, but there are other paths of attack that you may not be aware of. Microsoft 365 applications like Microsoft Teams, which can connect to external networks, may serve as a medium for ransomware and other types of cyberattacks.

To fight against such threats, train your staff in identifying potentially malicious files and links. You can also offer guidelines on how to handle and route sensitive files and communications to safe locations.

Vulnerabilities in SharePoint

Businesses typically use SharePoint to store sensitive information like personally identifiable data, so failing to secure SharePoint content against unauthorized users is one way to expose data and your business to cyberthreats. This can be disastrous for companies that are required to comply with stringent data privacy and protection regulations. Failure to comply may result in serious consequences not only for businesses but their customers as well.

To prevent this, limit administrator-level privileges and enable encryption. Additionally, set the necessary security restrictions per user for every application. This ensures that users and hackers who get a hold of user credentials cannot exploit or misuse privileges.

Microsoft 365 provides a powerful and convenient tool for businesses. However, as long as cybercriminals exist, there are always security risks to be aware of.

If you have any questions about Microsoft 365 security or would like help in implementing these tips, our team of experts would be happy to assist you.

Featured Partner:

datto

Datto Inc. is an award-winning vendor of backup, disaster recovery (BDR) and Intelligent Business Continuity (IBC) solutions, providing best-in-class technology and support to its 5,000+ channel partners throughout North America and Europe. Datto is the only hybrid-cloud BDR/IBC vendor that provides instant on and off-site virtualization and screenshot backup verification, serving the needs of small to medium-sized businesses.

These Windows 11 Keyboard Shortcuts Will Make Your Life Easier:

Windows 11 has been around for almost a year now, and many Windows 10 users have upgraded to the latest operating system from Microsoft. There are many Windows 11 Keyboard shortcuts to help you perform your tasks faster and more efficiently. Keep reading to find out how these shortcuts can make your life easier.

General Windows 11 Keyboard Shortcuts:

These shortcuts are for general functions, such as copy, cut, paste, and more.

Command	Function
Ctrl + A	Highlights all items in the active window
Ctrl + C	Copies the highlighted items
Ctrl + V	Pastes the cut or copied items
Ctrl + Z	Undoes recent changes
Ctrl + Y	Redoes recent changes
Ctrl + Shift + Drag an icon	Creates a shortcut
Shift + Left mouse click	Selects multiple items
Ctrl + O	Open a file
Ctrl + S	Saves a file or folder
Ctrl + Shift + S	Opens the Save As dialog box
Ctrl + N	Opens a new window
Alt + Tab	Switches between active tabs or windows
Alt + F4	Closes an active window
Shift + Delete	Deletes a file or folder without going through the recycle bin
Shift + Delete	Deletes a file or folder without going through the recycle bin
F5	Refreshes the active window

Windows 11 Command Prompt Shortcuts:

These shortcuts will help you navigate the Command Prompt terminal faster.

Command	Function
Ctrl + A	Selects all items
Ctrl + M	Activates Mark mode
Ctrl + F	Opens the Find dialog box
Esc	Deletes everything you typed
Up and Down arrow keys	Cycles through the command history
Page Up/Down	Moves the cursor up or down a whole page
Shift + Home	Repositions the cursor at the start of the current line

Windows 11 File Explorer Shortcuts:

Use these File Explorer shortcuts to manage your files and folders more efficiently.

Command	Function
Win + E	Opens File Explorer
Ctrl + N	Opens another File Explorer window while you're in File Explorer
Ctrl + E	Goes to the Quick access search bar
Ctrl + W	Closes File Explorer
Ctrl + Mouse scroll	Changes how files and folders can be viewed
F4	Goes to the File Explorer address bar
F5	Refreshes the current File Explorer window
F6	Toggles between the left and right pane
Ctrl + Shift + N	Creates a new folder
Alt + P	Shows/Hides the preview panel
Alt + Enter	Shows the Properties window of the selected item
Alt + Left or Right arrow keys	Toggles between the next and previous folders
Alt + Up arrow key	Goes to the parent folder or directory
Num Lock + Plus (+) key	Expands the selected folder
Num Lock + Minus (-) key	Collapses the selected folder

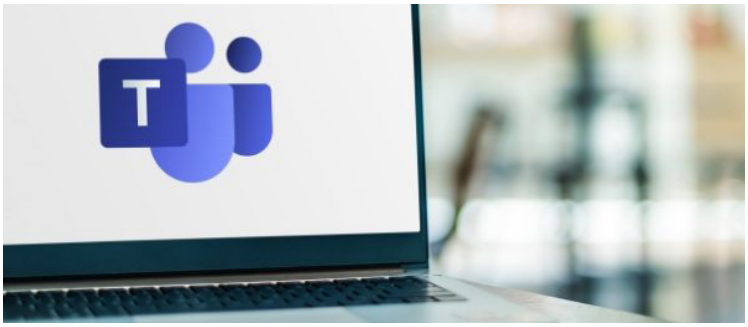
New Windows 11 Keyboard Shortcuts:

Here are keyboard shortcuts you'll find only in Windows 11.

Command	Function
Win + C	Opens the Microsoft Teams chat app
Win + H	Opens Voice Typing
Win + A	Launches the Quick Settings flyout
Win + N	Opens the Notification Center
Win + W	Brings up the Widgets pane
Win + Z	Launches the Snap Layouts flyout

Remembering all these keyboard shortcuts can be difficult but learning them can save you significant time and effort while working on tasks on a Windows 11 computer.

How to Secure Microsoft Teams:



Microsoft Teams is a powerful tool that can help your workplace run more smoothly. However, with great power comes great potential security risks. In this blog post, we will discuss the three best tips on how to secure Microsoft Teams.

Utilize Built-In Security Features

The most dependable approach to securing Microsoft Teams is through governance restrictions. These are rules that set the parameters for how the platform will be used, who can establish Teams accounts, and what information people may provide. Appointing a Teams administrator will be critical in ensuring that Teams security policies are followed by users throughout the company.

Administrators should also set up Teams' data loss prevention (DLP) feature to prevent accidental exposure of critical information and reduce the risk of data breaches. For instance, administrators can use sensitivity labels as a condition in DLP policies to instantly block guests or unauthorized users from accessing or sharing data in a Teams channel or a private chat.

Limit External Access

Speaking of guest users, you should also use Teams' Lobby feature when meeting with external users or teams. This feature redirects guests to a virtual lobby where they will wait before being admitted into the meeting. This can be useful when you want to talk with your team first before officially starting the meeting with a client.

Another way to control Teams access is by creating security groups. By default, a user with an Exchange Online mailbox can create a Team and become a Team owner. Creating a security group will help prevent unwanted and unverified users from creating and joining any group, extension, and Team.

Enable MFA (Multi-Factor Authentication)

Multifactor authentication (MFA) is a practical way to enforce security when using Teams. In 2020, more than 99.9% of compromised Microsoft enterprise accounts didn't use MFA. This is highly concerning because if an attacker compromises a Microsoft account and is able to get into Teams, they will gain access to valuable information the account's owner works with through the platform as well as other integrated apps.

MFA can be used in conjunction with a password, PIN, or biometric data such as a fingerprint or an iris scan. In the case of Microsoft Teams, requiring multiple factors for authentication ensures that only authorized users will be able to access their accounts. And when someone else tries to gain access, they will be alerted of suspicious activity so they can take steps to further safeguard their accounts. This can discourage malicious actors and, more importantly, instill better security habits among users.

Following these tips can help ensure a seamless and secure collaboration environment for your workplace. Contact our IT experts today to learn more about Microsoft Teams and how to better secure it against attacks.

Tech Tips of the Month:

- Don't use public Wi-Fi without a VPN
- Backup all your data to the cloud to protect your company in the event of a disaster
- Double check the URL or Web Address on a link. Often times, phishing links are almost identical to the legitimate sites but contain a small spelling change.