`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2023

Technology Track – Session 2

Secure Setup of Microsoft 365

Presented By:
Ben Schorr, Microsoft, Redmond, WA

About the Presenter…

Ben Schorr is a Senior Content Program Manager at Microsoft. He is also the author of several books and articles on technology including “The Lawyer’s Guide to Microsoft Outlook”, “The Lawyer’s Guide to Microsoft Word” and “OneNote in One Hour”. He was a Microsoft MVP for 20 years and involved with management and technology for more than 30, including in-house at law firms in Los Angeles and Honolulu. In his free time he’s a slow Ironman triathlete and a high school football coach. He currently lives in Martha Lake, WA with his wife Carrie, their son Keith, daughter Elena, and rescue mutt Sampson.

Securing Microsoft 365 – The essentials

Not all firms, especially small firms, have experienced IT staff available to them. Even if you retain an IT consultant, they might not be expert in the details of Microsoft 365 security.

In this paper I'm going to highlight what I think are some of the most important security settings and tools to pay attention to in Microsoft 365. Some of these settings might already be turned on for your tenant, but it's still worthwhile to check and make sure.

Note that you may not want to dig into all of these settings yourself, and that's fine. At the very least I can hopefully give you a set of things you can ask your IT support person about and make sure they've considered implementing them for you.

Multifactor authentication

The number one most important thing you can turn on in Microsoft 365 is multifactor authentication. I recommend turning it on for ALL accounts in your system.

Multifactor authentication – sometimes referred to as two-step verification – means that in addition to using a username and password to sign in the user is prompted for a second factor, such as a one-time code sent to their smartphone via SMS or generated by an authenticator app or key fob.

The first time one of your users signs in from a new device or app it will prompt them for their second factor – preferably an app on their phone. Once they successfully sign in Microsoft 365 will ask them if they trust the device they're on. If it's their personal device, as it usually will be, they can select "Yes" and Microsoft 365 won't ask for their second factor again for a period of time (default is 90 days).

Multifactor authentication is extremely important because one of the most common kinds of attacks we see are credential attacks – meaning that the bad guys somehow got your user's username and password. If you have multifactor authentication turned on, when they try to sign in from their base in Crimedanavia Microsoft 365 will ask for the second factor…which they almost certainly don't have. And you're probably now alerted to their attack.

For more information on how to enable it in Microsoft 365 see: Deployment considerations for Azure AD Multi-Factor Authentication | Microsoft Docs

Use dedicated admin accounts

It's convenient to use your own account for administering Microsoft 365 but I can give you a couple of good reasons why you shouldn't.

1. Actively used accounts are more likely to get compromised. Either by credential compromise, phishing, malware, or other attacks. If your account gets compromised the bad guys now have admin access to your Microsoft 365 tenant.
2. If you ever need somebody else, like an outside IT expert, to temporarily sign into your admin account they shouldn't sign in as you.

Create a dedicated admin account that doesn't have licenses for any of the software applications and only has permissions to carry out administrative tasks. Make sure it has a strong password, and multifactor authentication.

Tip: You should always have an admin account that you control. You may contract with an outside company to manage your Microsoft 365, and they will likely have their own admin account(s), but the account is your account, and you should have an admin account you can access if you need to. If you ever decide to change outside support companies having your own admin account can make things much easier.

The concept of **least privilege** is key here. You want to give people only as much access as they need, and only when they need it. If you have people, including yourself, signing in with an account that is also an admin account to do your daily work, you may be giving them more access than they need. And if their account, or device, is ever compromised that high level of access is then available to the attacker or the malware.

Clean up your directory

Most firms have had people come and go, and too many of those firms don't have an established exit policy for when people go that includes making sure their accounts in Active Directory have been disabled or deleted, and that any passwords they had access to are changed. Least privilege is right out the window if somebody who doesn't even still work at your firm still has an active account in your directory that they could sign into.

Cleaning up your directory isn't only about making sure only people who still work for your firm still have accounts, it's also about making sure that people who DO still work for your firm only have the permissions they need to do their jobs. If an attorney in your firm only does wills and estates, they probably don't need access to the files and folders for the business litigation part of the practice and you should make sure they don't have it.

Clean up their devices too

While you're creating your exit policy make sure it includes ensuring that no client or firm data is on the personal devices they're walking out the door with. Especially in the COVID era a lot of people were suddenly working from their dining room tables; often on personally owned computers. Confirm with the departing employee that any firm or client data has been removed from those devices too.

Block auto-forwarding

If bad guys compromise one of your users a favorite trick is to sign into their email and silently add an auto-forwarding rule that sends copies of some, or all, of their future email to an account the bad guys control. In Exchange Online you can easily set up a rule that blocks any auto-forwarding from inside your organization to addresses outside your organization. This happens at the server side, so even if one of your users gets their account compromised, the crooks won't be able to successfully auto-forward their mail.

For more information on how to set this up (it's pretty easy, really): Stop auto-forwarding emails | Microsoft Docs

Set up conditional access

Conditional access gives you more control over who (or what) can access your Microsoft 365 applications and data. You can set up policies that specify things like only users running a recent version of Windows 10 or macOS can connect or require that devices have an ant-imalware program running.

You can require that only certain applications – like Outlook, Word, or Excel – can be used to access resources in your Microsoft 365.

You can even specify certain geographical regions that are allowed or blocked for connection to your firm's regions – though keep in mind that good attackers will mask their true location with a VPN or other tool.

For more information on conditional access see: What is Conditional Access in Azure Active Directory? | Microsoft Docs

Custom banned passwords

Azure Active Directory is what Microsoft 365 uses for managing user accounts and it has a global banned password list that is automatically on. This list contains a large set of weak or common passwords, so your users shouldn't be able to use "pizza" or "123456" as their password in your Microsoft 365. However, you might want to add some custom things to that list as well – especially if you know the local sports teams are popular, or if you think your users are using the firm name as a password.

For more information see: Password protection in Azure Active Directory | Microsoft Docs

Keep devices up to date

After credential attacks most of the successful breaches we see are exploiting vulnerabilities in software or hardware – and often those vulnerabilities have already been patched by the vendor. Too often those patches were never applied by the firm that got attacked. Make sure you have a patch management policy in place to promptly apply any security fixes for your operating systems, software, browsers, and devices. PCs, Macs, servers, mobile phones, and even printers can have regular security patches that need to get installed too.

Don't forget your networking equipment like routers, switches, and firewalls; and any smart gear like security cameras, HVAC systems, or "smart" door locks as well.

Patching can be a pretty substantial task, but it's important. If you use an outside IT vendor be sure to ask them to document their patching process and service-level agreements.

Train your users

This isn't a tool or a setting, exactly, but your users are a critical line of defense in your cybersecurity. If they practice safe habits your firm is far less likely to get hit by a scam, ransomware attack, business email compromise, or many of the other common attacks we see.

Cybersecurity training doesn't have to be expensive or boring. In fact, you could just start by watching some YouTube videos on the subject and sharing the ones you find useful with your users on a regular basis. Here's a video we created to get you started: Making accounts more secure with multi-factor authentication - YouTube.

Create a positive security culture

If your firm is attacked, it may well be one of your people who spots it first. Create a culture where people are alert to suspicious activity, know who to call if they see something unsettling, and (perhaps most importantly) feel safe and empowered to do so. Especially if they made a mistake that caused a breach, some people are scared to report it in a timely fashion – fearing the consequences. Make it clear to your team that you value people who come forward to admit mistakes or report suspicious activity. Create the culture that rewards honesty more than it punishes mistakes.

Have documented policies and follow them

A lot of cyber attacks and costly scams happen because there weren't established policies on how to do things like change the way vendors are paid, or arrange for transfers of funds from one account to another. Phishing attacks often happen when staff get an email that appears to come from the boss telling them to click a link to claim a bonus, raise, or other reward.

Have well-documented policies in place and reiterate with your people that those policies will always be followed. Then have a documented escalation plan in case questions arise. It's when somebody gets an unusual request and doesn't follow the procedures that we get into situations where funds go missing or attackers gain access to our systems.

So much of effective defense is just communicating with your team.

More resources

- Microsoft security help and learning
- Microsoft 365 security documentation