How to improve your Office 365 Security - Checklist

What's the Problem?

There has been a significant increase in Office 365 accounts (including email) compromises over the last few weeks, notably since people moved to working from home. Getting into your email is the first step for cyber criminals to start their scams and frauds. This is because they can:

1. Get access to information
2. Allow them to authentically impersonate the real user

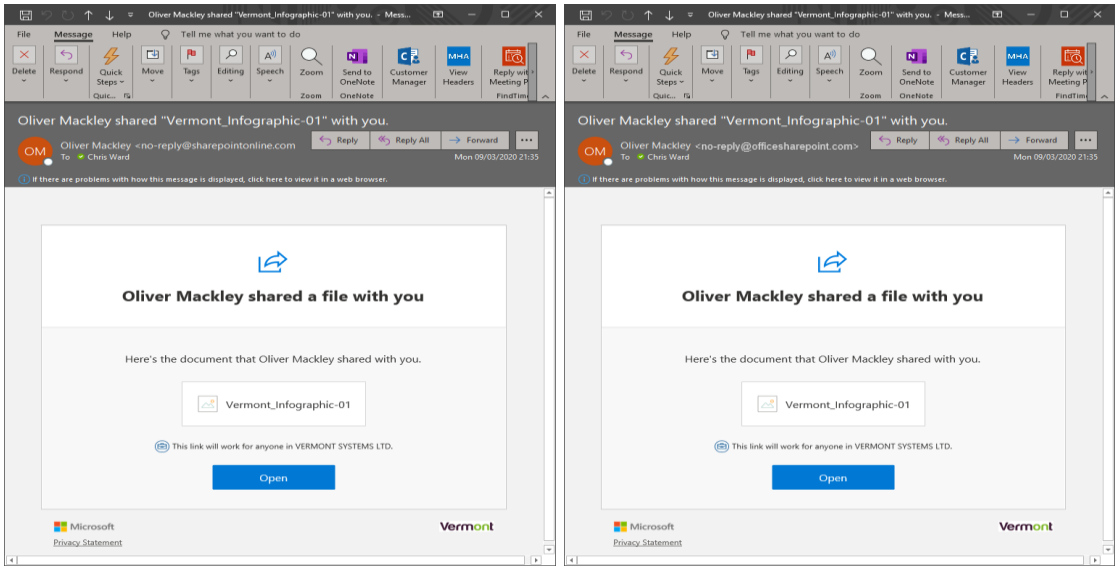
These two things combined give the criminals the tools to commit further frauds against the company and its employees, suppliers, and customers.

Why is It Increasing?

Two reasons:

1. People using more online "cloud" services. Previously when we received a fake service notification we discarded it. The email might have pretended to be from a colleague and that they had shared a file, or Microsoft telling us our storage was filling up. We discarded it because we didn't use those services. Now we do, and it is hard to spot the fake ones because Microsoft keep changing what the real ones look like!

   Which is real? One of these is fake. Would you know the difference?



2. Many of us are in a state of flux and under pressure – working hard and fast to adapt our businesses to the new reality. This is when mistakes can be made.

The cyber criminals know this and are merciless. They do not subscribe to the "we are all in this together" attitude and they are working to take full advantage of us, to make as much revenue as they can.

Office 365 Security Check List

By following all, or most of, the below you can eliminate a large amount of risk

1. **Is multi-factor authentication turned on?**

   Why is this important? This is where you need to approve the login via a code on your phone or via an app. It means that even if your password is compromised a hacker still needs to access your phone making you way harder to breach. Microsoft says 99.9% of Office 365 compromises would be prevented by MFA.

2. **Are all your users accounts "standard users"?**

   Why is this important? And administrator account has full access to the whole system – they can change other people's passwords, delete data, give themselves access to other mailboxes, create new accounts. The last thing you want is a hacker getting in on an administrator account. No one needs to use one for day to day use so make sure all admin accounts are separate from day to day working accounts.

3. **Has Activity Auditing been turned on?**

   Why is this important? This feature creates logs of when different users login, and from where. So if an account gets compromised you can trace back to see how long the hacker has been accessing your system. However you will probably be surprised to learn this feature is turned off by default.

4. **Has Mobile Device Management (MDM) features been enabled?**

   Why is this important? If you let employees access your company system from their phone or device, you want the ability to delete you data if you need to. Crucially, under standard configurations, your only way to do this is by wiping their whole phone, which could land you in hot water. MDM allows you to just delete the Office 365 data.

5. **Has someone recently checked that all old accounts disabled or deleted?**

   Why is this important? This should of course happen when people leave the company. However it is almost always the case that when we check there is one or two that were missed. At least. Even if that employee wouldn't do anything bad, they might have used the same password elsewhere, which leaves a key to your front door lying around. And don't forget to check the admin accounts!

6. **Are external emails marked "External"?**

   Why is this important? It helps people to spot a fraudulent email pretending to be from you asking for money to be transferred. But as importantly, it helps your people to identify a real Microsoft notification from a fraudulent ones which are aimed at capturing your password. Adding the "External" tag to anything from outside means you can spot the fake ones easily.

7. **Has email forwarding been blocked?**

   Why is this important? Once a hacker has access to your account, they will usually create forwarding rules so that interesting emails containing words like "invoice", "bank", "payment" are automatically forwarded themselves. They can then sit waiting and jump in

quickly to act to try and divert a payment to their account using timely pertinent information. Forwarding is rarely used these days and so tuning it off prevents this tactic.

8. **Has "Legacy Authentication" been disabled?**

Why is this important? Legacy Authentication is old and insecure. However it is turned on by default as older versions of Outlook (2013 and earlier) and old phones and tablets need it turned on. But because it is turned on, hackers will use it to try and gain access. So make sure all your versions of Outlook are 2016 or newer (we suggest making your Office 365 subscriptions "Business Premium" which includes latest version of Office) and turn off Legacy Authentication.