Securing Office 365 Email

Description

Microsoft Office 365 is a great product that many title agents are using. Depending on the license purchased agents have access to email, encrypted email, free office software, one drive, file sharing, and many other features. However, as with most technology there are security risks introduced by using Office 365 for email. Many of the security features available in Office 365 by default are *not enabled* . We continue to see a rise in attacks within the title industry, mostly in the form of phishing emails. One scenario we see repeatedly are phishing emails when clicked on require the end user to put in their Office 365 credentials. These credentials go back to the attacker and they can login to the Office 365 account as if they are the end user. Once the attacker is in the Office 365 account, not only can they see all the emails in the account, but they also set up forwarding rules to allow all the end users email to be sent to the attackerâ??s email account. We all know the scenario that follows, emails are sent to your clients in an attempt to have your clients wire money to a fraudulent account. The good news is that there are security controls that can be put in place to add extra layers of security to minimize your exposure within your Office 365 account.

The controls listed below must be implemented in the Administrator account in your Office 365 account.

1. Check your Office 365 Secure Score
2. Use strong passwords
3. Implement password expiration policy
4. Check box to have security alerts sent, make sure appropriate email address is listed to receive the security alerts
5. Turn on audit data recording
6. Turn on mailbox auditing for all users
7. Implement rule not allowing forwarding
8. Implement rule protecting against ransomware
9. Implement mobile device management
10. Implement two-factor authentication on all accounts

The above security controls are at minimum what should be implemented within Office 365. Implementing the above security controls will increase your security posture while using Office 365, however do not guarantee that you will not fall victim to an attack. Agents that follow the Best Practices for securing nonpublic personal information laid out by ALTA stand the best chance of mitigating the risks of being the victim of a malicious attack.

If you have any questions on implementing the security controls listed here or any other security related issues, please feel free to reach out to me at 703-378-4110 or melissa.ellis@smeinc.net.

By: Melissa Ellis
VP/CFO
SME, Inc.

Category

1. Cybersecurity

Date Created
2019/03/26
Author
vltaexaminer