MAGOO.TECH

Summary of Key

Microsoft 365 Changes

1. Requiring Multi-factor authentication for signing in

Standards: CIS, CISA, NIST CSF, Essential 8 (yeah… pretty much all cybersecurity frameworks)

Notes: This has become a "non-negotiable" for our clients because we have seen too many clients get breached due to password guessing and session hijacking. MFA can be configured to text, phone call and Authenticator App, but we highly recommend using the Authenticator app due to newly developed hacking techniques that are making it easier to bypass text and phone call MFA tokens.

2. Activity related timeouts

Standards: CIS and NIST CSF

Notes: This prevents reduces the risk that an existing session can be hijacked and used by a malicious actor.

3. Disable Guest Accounts not used in over 90 days

Standards: CIS

Notes: This is kind of a "no-brainer"… essentially "use it or lose it" for guest account that may have access to your data.

4. Disable App, Group, and Tenant creation by general users:

Standards: CIS, CISA, NIST, EIDSCA

Notes: While this one may sting a little for some of our more “hands on” organizations, it is very powerful in stopping hackers from gaining persistence in your M365 tenant.

5. Setting your password to DO NOT EXPIRE

Standards: CIS

Notes: Yes, you read that right! Users around the world are rejoicing that the era of 90, 60, or 30 day password changes have come to an end! Best business practices are now recommending that you do NOT change you password unless there is a assumed or known breach for your account. Caveat: certain regulatory bodies like PCI DSS and special account types may still require password changes at a defined interval.

6. Require admin consent for applications

Standards: CIS, CISA, EIDSCA, Essential 8, NIST CST (again, ALL the cybersecurity frameworks!)

Notes: Malicious apps (that are very good at looking legitimate) are one of the main ways that hackers are stealing your credentials and tokens. The good news is that either your tenant owner, one of your admins or one of our techs at Magoo can easily approve an app once, then it's good for all of your other employees.

7. Disable automatic forwarding to external recipients

Standards: CIS, CISA, NIST CSF

Notes: To those who never use this, you might ask "why in the world would you do that?" while those of you with a valid business process that requires this may be a bit worried. This is another common tactic for hackers to steal your data and send out malicious emails on your behalf without you even knowing.

8. Enable 'external' warning in Outlook

Standard: CIS

Notes: Yes, it might be a bit annoying for emails to have this "warning" banner attached, but many of our clients have reported that they identified phishing emails by nothing other than this "annoying" banner. This banner tends to make your users "think before they click" on links that have this at the header.