Multi-factor Autenticatie (MFA)

Als het mogelijk is schakel de Multi-Factor Authenticatie (MFA) in.
Dit is een beveiligingsmethode die vereist dat gebruikers meerdere vormen van verificatie doorlopen voordat ze toegang krijgen tot een systeem, account of applicatie.
Veel bedrijven en online diensten, zoals banken, e-mailproviders en cloudplatforms, maken er al gebruik van. In plaats van alleen een wachtwoord te gebruiken, combineert MFA verschillende identificatiemethoden om de kans op ongeautoriseerde toegang te verkleinen. Het combineren van een wachtwoord of een pincode met een of meerdere mails, code naar een sms-bericht van een mobiele telefoon, beveiligingstoken of smartcard, biometrische gegevens zoals een vingerafdruk of gezichtsherkenning. Iets wat je weet, hebt en/of bent. Zelfs als phishers uw wachtwoord bemachtigen, moeten ze extra verificatiestappen omzeilen om toegang te krijgen tot uw account.

Je kan ook Multi-Factor Authenticatie (MFA) zelf instellen door het Download van een authenticator-app zoals Microsoft Authenticator of Google Authenticator op je telefoon. Ga naar de beveiligingsinstellingen van het platform waarvoor je MFA wilt inschakelen (bijvoorbeeld Microsoft 365, Google, of je bank). Selecteer MFA of tweestapsverificatie en kies een verificatiemethode (zoals een app, sms-code of hardware-token). Scan de QR-code die wordt gegenereerd door het platform met je authenticator-app. Bevestig de verificatie door de gegenereerde code in te voeren. Test de MFA-instelling door uit te loggen en opnieuw in te loggen met de extra verificatiestap.

Wanneer je gebruik kunt maken van multifactor authenticatie, doe dit dan! Zeker ook bij de beveiliging van jouw wachtwoordmanager. *Meer informatie over tweestaps authenticatie kun je lezen in* dit artikel *van de* Consumentenbond*. En als je een ANWB Inboedelverzekering met cyberdekking hebt, helpt de* Cyberhelpdesk *jou gratis met het instellen ervan.*

Alex Hol