Justins MKB

Bescherm jezelf tegen verdachte Microsoft 365 phishing

Er zijn nieuwe phishingaanvallen (o.a. Kali365) waarbij hackers toegang krijgen tot je account zonder wachtwoord te stelen. Dit gebeurt doordat je (onbewust) toegang geeft via een code.

Checklist tegen hackers

1. Let op deze signalen

⚠️ **Verdacht bericht** (e-mail / Teams / sms)

- Je krijgt een bericht zoals:
  - "Er staat een document voor je klaar"
  - "Je moet opnieuw inloggen"
  - "Voer deze code in om verder te gaan"
- Het lijkt van Microsoft, SharePoint, Teams of een collega

⚠️ **Je moet een code invoeren**

- Je krijgt een korte code (bijvoorbeeld: ABCD-1234)
- Je wordt gevraagd om deze in te voeren op:
  - microsoft.com/devicelogin
  - (dit is een echte Microsoft pagina!)

Het lijkt betrouwbaar, maar is dat niet

De website is echt van Microsoft, je hoeft geen wachtwoord opnieuw in te voeren en alles ziet er "normaal" uit. Maar door de code in te voeren geef je toegang aan een aanvaller.

2. Wat moet je doen als je dit ziet?

❌ Voer GEEN code in
❌ Klik niet op links in het bericht
✅ Meld het direct bij IT / Justins
✅ Verwijder het bericht

3. Wat als je toch een code hebt ingevoerd?

Geen paniek, maar handel snel:

✅ Meld dit **direct** bij IT / Justins
✅ Geef door:
- wanneer dit gebeurde
- welk bericht je kreeg

✅ Laat je account controleren

4. Zo voorkom je problemen

✅ Wees extra alert bij:
- documenten die je "moet bekijken"
- onverwachte verzoeken

✅ Controleer altijd de afzender
✅ Vertrouw je het niet? → melden

Contact Justins

Justins Klantenservice
085 - 105 41 41
klantenservice@justins.nl

Het belangrijkste advies: Voer nooit een code in die je ontvangt via e-mail, Teams of sms of telefoongesprek, TENZIJ je die net zelf hebt aangevraagd.

Versie: 1-6-2026