

Attic BOUNCER

Microsoft 365 beveiliging tegen valse inlogpagina's en verdachte inlogpogingen

Hackers breken niet in, ze loggen gewoon in!

Cybercriminelen slaan op twee manieren toe om in te loggen op jouw Microsoft 365 account. Ten eerste via nep-inlogpagina's die niet van echt te onderscheiden zijn. Log je hierop in? Dan onderscheppen ze al je gegevens inclusief tweestapsverificatie.

Ten tweede door gewoon te blijven proberen: ze testen gestolen wachtwoorden uit eerdere datalekken, populaire combinaties of gaan systematisch door tot ze binnenkomen.

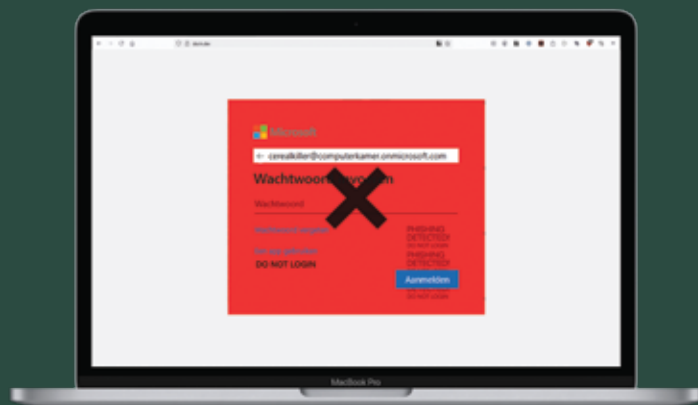


Een sterk wachtwoord en tweestapsverificatie bieden géén bescherming tegen inlogfraude.

Als cybercriminelen eenmaal ingelogd zijn, kunnen ze razendsnel enorme financiële en reputatieschade aanrichten.

- 🚨 Klanten krijgen nep-facturen "van jou"
- 🚨 Je systeem wordt gegijzeld met ransomware
- 🚨 Je klantendatabase verdwijnt naar de hoogste bieder
- 🚨 Je goede naam ligt aan diggelen

Gelukkig hoeft dit niet te gebeuren als je inlog-beveiliging op orde is.



Attic BOUNCER houdt hackers buiten de deur

Attic BOUNCER herkent nep-inlogpagina's en slaat direct alarm als je op zo'n phishing-pagina belandt. Je ziet dan een groot rood alarmscherm, zodat je weet dat je moet wegwezen.

Daarnaast ben je met BOUNCER ook beschermd tegen inlogpogingen van hackers, doordat we automatisch monitoren wie inlogt, hoe vaak en vanaf welke locatie. Zien we hierin onregelmatigheden? Dan rapporteren we dit direct, zodat je zelf het account in kwestie kunt blokkeren.

Welke beveiliging zit in Attic BOUNCER?

Bescherming tegen phishing

- ✓ Realtime detectie van fake Microsoft 365 inlogpagina's
- ✓ Waarschuwing met rood alarmscherm bij nep-pagina's
- ✓ Echtheidszegel op officiële Microsoft 365 inlogpagina's
- ✓ E-mail aan de beheerder wanneer een collega een valse pagina bezoekt
- ✓ Inzicht welke collega een fake inlogpagina heeft bezocht

Bescherming tegen inlogpogingen van hackers

- ✓ Monitoring van alle Microsoft 365 inlogactiviteiten
- ✓ Detectie van verdachte inlogpogingen (wie, waar, hoe vaak)
- ✓ E-mail aan de beheerder bij verdachte inlogactiviteiten

Online security awareness training

- ✓ Gericht op het herkennen van risico's

WIJ ZIJN ATTIC SECURITY

Een productgedreven beveiligingsbedrijf voor de praktijk van het mkb. Opgericht door hackers en engineers.

Geen jargon, geen ballast, alleen slimme en schaalbare bescherming waar dat het hardst nodig is.

€ 30 /maand

Incl. 20 gebruikers, +€1 per extra



Cybersecurity made in Europe

Dataproductie, naleving van regelgeving en culturele aansluiting.



Betaalbare beveiliging door automatisering

Efficiëntie en schaal zonder hoge kosten.



Attic LAB

Ontwikkeld door hackers en engineers, gericht op automatisering en onderzoek.



Gericht op Microsoft 365

Maximale bescherming van het platform tegen BEC, datalekken en afpersing.

Voor wie is Attic BOUNCER geschikt?

- Mkb'ers met een Microsoft 365 omgeving
- Mkb'ers zonder eigen IT-afdeling
- Mkb'ers die zich zorgen maken over hackers, phishing, betaalfraude en ransomware
- Mkb'ers die inzicht willen in wie wanneer inlogt
- Mkb'ers die verdachte inlogpogingen willen detecteren



atticsecurity.com/bouncer



support@atticsecurity.com