campagnes de phishing OAuth visant les entreprises

Le 03/03/2026, Microsoft a alerté sur de nouvelles campagnes de phishing exploitant le protocole OAuth pour cibler les entreprises utilisant Microsoft 365 et Microsoft Entra ID.

Qu'est-ce que cette attaque ?

Il s'agit d'une technique de phishing utilisant les mécanismes légitimes d'OAuth pour contourner les protections de sécurité.
Les attaquants envoient des emails frauduleux (réunions Teams, documents, notifications) contenant des liens piégés.
Ces attaques fonctionnent via : emails de phishing, redirections OAuth, pages malveillantes imitant des services Microsoft.

Pourquoi ces attaques augmentent ?
Cette technique est efficace car elle exploite un fonctionnement normal d'OAuth et non une faille technique.
Les cybercriminels ciblent particulièrement les entreprises car : elles utilisent massivement Microsoft 365, une seule compromission permet d'accéder à plusieurs services et données internes.

Conséquences pour les entreprises
Vol d'accès aux comptes, compromission des systèmes internes, installation de malware, propagation de l'attaque dans l'entreprise, non-respect du RGPD.

Conclusion
Les attaques par phishing évoluent et exploitent désormais des services légitimes comme OAuth, les rendant plus difficiles à détecter. Les entreprises doivent renforcer l'authentification et surveiller les accès pour limiter les risques.

Sources :
https://www.bleepingcomputer.com/news/security/microsoft-hackers-abuse-oauth-error-flows-to-spread-malware/
https://thehackernews.com/2026/03/microsoft-warns-oauth-redirect-abuse.html