PHISHING : QUAND L'IA S'EN MÊLE !

L'intelligence artificielle permet aujourd'hui de créer des attaques de phishing **plus crédibles, rapides et personnalisées**. Elle rédige des messages **sans faute**, dans le **ton de l'entreprise**, et peut même interagir **en temps réel** via des chatbots ou des réponses par mail instantanées.

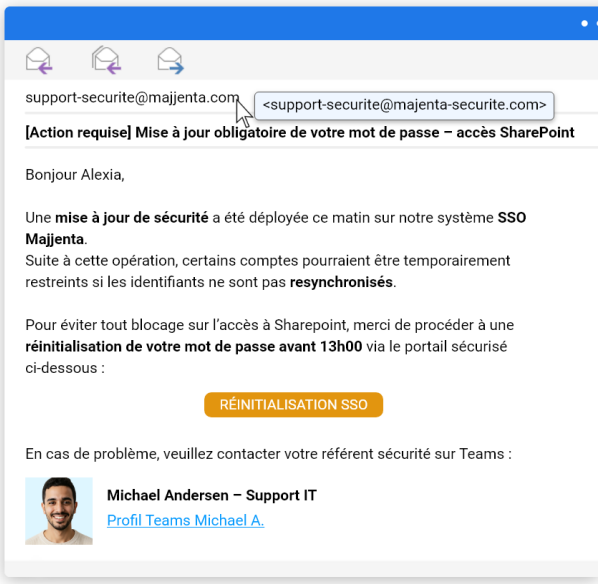
Et demain ?

Les IA continueront à s'améliorer : elles pourront **simuler des échanges prolongés**, s'adapter en direct à vos réponses et même se **connecter à des bases de données publiques** pour rendre les messages encore plus réalistes et ciblés.

LE "CONTEXTING", C'EST QUOI ?

Le **contexting**, c'est l'art de créer un message qui colle à votre environnement professionnel (vocabulaire interne, outils, habitudes, collègues, services utilisés…).

L'IA excelle dans cet exercice :
elle peut en quelques secondes analyser vos **réseaux sociaux**, **signatures mail, organigrammes, outils collaboratifs** pour rendre l'attaque **parfaitement crédible**.



COMMENT L'IA AMÉLIORE LES TENTATIVES DE PHISHING :

MESSAGE SANS FAUTE

L'IA rédige des mails en français impeccable, sans fautes ni tournures maladroites. Elle adapte le ton (formel, amical, pro) selon le destinataire : RH, DSI, fournisseur…

CHATBOT INTELLIGENT

Un faux chatbot animé par l'IA peut simuler un vrai support IT. Il comprend vos réponses et s'adapte pour récupérer des infos (mots de passe, codes…). Les attaques sont décuplées, une même IA pouvant parler à des milliers de cibles en même temps.

FAUX PROFIL SUR LES RÉSEAUX

L'IA sert à alimenter des profils LinkedIn ou WhatsApp réalistes (photo, texte, parcours) et peuvent être scriptées pour discuter, gagner votre confiance, et vous pousser vers un lien piégé.

CHATBOT AUDIO

Une IA vocale vous appelle et répond comme un assistant réel pour obtenir des infos confidentielles.

COMMENT SE PROTÉGER ?

Appliquez les mêmes réflexes qu'avec des mails de phishing et redoublez de vigilance :

- **Ne vous fiez pas à la qualité du message** : une orthographe parfaite n'est plus une garantie.
- **Vérifiez toujours la source** : lien, adresse mail, page web, nom de domaine.
- **Méfiez-vous des interactions en direct inattendues** : pop-up, chatbot ou appel "automatisé" surtout quand vous n'êtes pas l'émetteur de la demande.
- **Ne donnez jamais d'informations sensibles** via un canal non vérifié (identifiants, RIB, etc.).
- En cas de doute : coupez la communication et **signalez immédiatement à la DSI**.

© Dæsign - Ces contenus sont protégés par le droit d'auteur. Leur reproduction est interdite sans l'accord préalable de Dæsign. La reproduction sur un support papier demeure autorisée aux conditions suivantes : usage non commercial, respect de l'intégrité des documents reproduits (ni modifications, ni altérations), citation claire et lisible du copyright Dæsign.