Voici la pire menace informatique de 2023 pour votre sécurité, comment y faire face

Nassim Chentouf :

Le phishing, ou hameçonnage dans la langue de Molière, ne cesse de prendre de l'ampleur en 2023.
Une méthode vieille comme le monde que les pirates utilisent en masse.
Voici comment éviter au maximum de vous faire avoir !

© Envato

Vos données privées représentent un joli butin pour les pirates.
En ce moment, deux applications Android à supprimer d'urgence envoient vos informations sensibles en Chine.
Mais la plus grosse menace pour votre sécurité en 2023 n'est autre que le phishing ou hameçonnage dans la langue de Molière, **voici comment y faire face.**

À lire > Attention au phishing, les hackers utilisent des images pour vous faire cliquer sur des liens frauduleux

Une recrudescence des tentatives de phishing

Le phishing est une technique ancienne mais redoutable.
Les pirates envoient des courriels d'apparence légitime aux victimes avec des liens malveillants dedans.
Ces messages peuvent provenir de grandes entreprises ou du gouvernement, par exemple.

Différents procédés sont utilisés pour inciter à cliquer comme la promesse **d'une somme d'argent à récupérer ou une grosse amende à régulariser.**
Lorsque la personne ciblée clique sur le lien, elle atterrit sur un site frauduleux qui reproduit une plateforme légitime pour duper sa vigilance.
La victime entre alors les informations demandées comme son numéro de carte bancaire ou son identité et hop, **les pirates s'en emparent.**

Le phishing est tel que même Windows 11 publie un avertissement lorsque vous copiez l'un de vos mots de passe dans le presse-papier, **une mesure anti-hameçonnage déployée depuis peu pour certains utilisateurs.**

Le phishing est **en pleine recrudescence** comme en témoignent les nombreux témoignages en ligne et les SMS frauduleux que vous recevez sans doute depuis plusieurs mois.

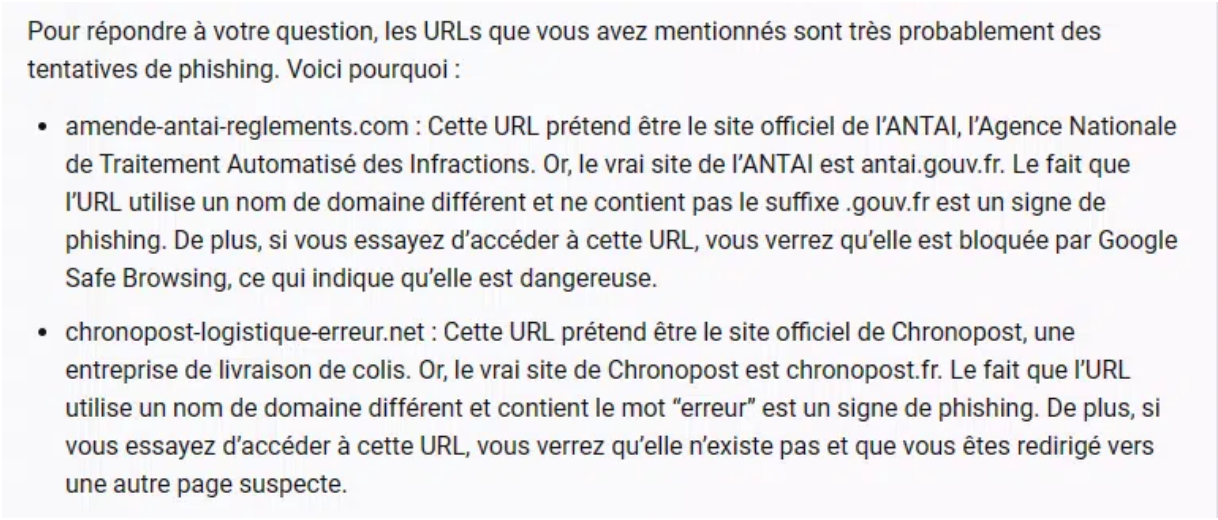
À lire > ChatGPT, Bing, Google Bard : vous risquez de vous faire piéger par les e-mails de phishing écrits par les chatbots

Si vous réalisez que vous avez entré vos données privées dans une page de phishing, **le mieux reste de changer vos mots de passe rapidement.**
Voire de faire opposition à la carte bancaire si vous avez inséré vos coordonnées bancaires.
Il est possible de le faire 24/24 et 7/7.

Il existe également **plusieurs mesures pour éviter de vous faire avoir par une page de phishing**, voici lesquelles

- Vérifiez bien l'adresse de l'expéditeur et du site.
  Les adresses contiennent des fautes, des caractères inhabituels voire des extensions… « *exotiques* ».
  Par exemple, une adresse appartenant soi-disant à Chronopost qui se présente sous la forme "*chronopost-erreur-colis.net*"
- Méfiez-vous des messages **qui ne sont pas personnalisés, mal rédigés, urgents voire menaçants.**
  Un courriel de phishing tente de vous pousser à agir sans réfléchir en vous mettant la pression
- Ne cliquez pas sur les liens ou les pièces jointes sans vérification.
  Passez la souris (ou votre doigt appuyé longuement sur cellulaire) sur le lien pour voir l'url complète.
  Sinon, utilisez un outil en ligne pour analyser le lien ou le fichier comme ScanURL**,** VirusTotal **ou** EmailVeritas
- **Ne communiquez jamais vos données personnelles par courriel.**
  Aucun organisme sérieux ne vous demandera votre code de carte bleue ou vos identifiants via un courriel.
- **Utilisez un antivirus et un navigateur mis à jour.**
  Ces outils protègent contre certaines tentatives de phishing en bloquant les sites et fichiers suspects

Contre le phishing, **votre vigilance et des outils pour vous épauler représentent la meilleure des solution.**
N'hésitez pas à demander des intelligences artificielles comme ChatGPT ou Bing IA si l'url d'une page web est suspecte.


Pour répondre à votre question, les URLs que vous avez mentionnés sont très probablement des tentatives de phishing. Voici pourquoi :

- amende-antai-reglements.com : Cette URL prétend être le site officiel de l'ANTAI, l'Agence Nationale de Traitement Automatisé des Infractions. Or, le vrai site de l'ANTAI est antai.gouv.fr. Le fait que l'URL utilise un nom de domaine différent et ne contient pas le suffixe .gouv.fr est un signe de phishing. De plus, si vous essayez d'accéder à cette URL, vous verrez qu'elle est bloquée par Google Safe Browsing, ce qui indique qu'elle est dangereuse.
- chronopost-logistique-erreur.net : Cette URL prétend être le site officiel de Chronopost, une entreprise de livraison de colis. Or, le vrai site de Chronopost est chronopost.fr. Le fait que l'URL utilise un nom de domaine différent et contient le mot "erreur" est un signe de phishing. De plus, si vous essayez d'accéder à cette URL, vous verrez qu'elle n'existe pas et que vous êtes redirigé vers une autre page suspecte.

© Tom's Guide (capture d'écran)

Par exemple, nous avons demandé à Bing IA **d'analyser deux urls reçues via des campagnes de phishing par SMS** et le résultat est sans appel !
Même si, on le précise, ne vous fiez pas totalement aux intelligences artificielles.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230726
"C'est ensemble qu'on avance"