Six conseils pour éviter d’être victimes de phishing

Six conseils pour éviter d’être victimes de phishing

Le phishing (e-mails frauduleux se faisant passer pour des marques de commerce ou de service avec l'intention de tromper le destinataire) est l'une des attaques les plus anciennes, mais aussi des plus rentable pour les cybercriminels.

Sur la base de « plus des gens le reçoivent, meilleure est la probabilité que quelqu'un tombe dans le piège » ces campagnes frauduleuses dont le seul but est le vol de données personnelles et financières, ont beaucoup évolué dans les dernières années. Et, en plus, **au cours du premier trimestre de 2016 les cas de spam avec des pièces jointes malveillantes, ils n'ont pas cessé d'augmenter**.
Il y a quelques années, il était facile de distinguer ces e-mails entrant dans la boîte de réception car ils avaient des fautes d'orthographe, des conceptions plutôt anciens… qui nous fassent au moins nous méfier. D'autres viennent directement comme spam, ou comme un courrier indésirable. Mais maintenant, **ils ont évolué**. Bon nombre de ces campagnes utilisent des courriels parfaitement conçus: avec le logo, les couleurs et l'apparence de la marque qui sont en train de supplanter.

Mais le fait que, heureusement, ils ne donnent pas des coups au dictionnaire, signifie que ces emails sont beaucoup plus difficiles à détecter comme frauduleux. Cependant, **il y a un certain nombre de précautions que nous pouvons prendre pour éviter de devenir une victime de ces e-mails malveillants.** Check Point propose ces conseils que nous devons mettre en pratique pour les détecter au début, ou presque:
1. **Surveillez les e-mails qui viennent de marques célèbres.** Le site OpenPhish rassemble les marques les plus utilisées par les cybercriminels pour mener à bien leurs attaques de phishing. **Parmi eux, Apple, Google et Paypal figurent dans le top dix des plus touchés par ce type de campagne**. Les raisons sont évidentes: ils sont extrêmement populaires, il est donc plus susceptible de réussir à usurper l'identité des victimes potentielles.
2. **Vérifiez l'expéditeur du message. Les emails officiels sont toujours envoyés avec le domaine de la marque, par exemple @paypal.com.** Les cybercriminels peuvent mettre le nom de marque, mais ils ne peuvent jamais utiliser le domaine réel.
3. **Fautes d'orthographe.** Nous venons de dire que les cybercriminelles ont beaucoup amélioré en ce sens mais **ils restent toujours quelques erreurs de basse**, souvent en raison de mauvaises traductions.
4. **Hyperliens.** Les liens qui sont envoyés par le biais de ces e-mails sont clairement frauduleux. Une fois que vous y accédez normalement **ils conduisent à des formes où ils volent les données**. Donc, lorsque vous accédez à un site Web qui n'a pas le protocole HTTPS, vous devenez une victime.
5. « **Cher utilisateur** ». Il faut tenir en compte que **les entreprises traitent leurs clients par leur nom et prénom** mais les cybercriminels envoient des e-mails en masse, impersonnelles.
6. **Urgence.** Dans de nombreux e-mails de ce type, **il y a généralement un sentiment d'urgence pour donner nos données personnelles**: le compte est fermé, vous perdrez de l'argent, votre colis sera envoyé sont des exemples.
7. **Attention aux pièces jointes.** Des entreprises n'envoient jamais des pièces jointes dans leurs e-mails. **Évitez d'ouvrir ces documents**, sauf si vous êtes très sûr de l'expéditeur.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Six conseils pour éviter d’être victimes de phishing – Globb Security FR