Comment se protéger du smishing ?

Comment se protéger du smishing ?

Pour rappel Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Lorsque vous utilisez votre téléphone, appliquez des précautions de base, par exemple :
• Ne cliquez pas sur les liens que vous recevez sur le téléphone sauf si vous connaissez la personne qui vous les envoie.
• Même dans ce cas, si vous recevez d'un ami un SMS contenant un lien, avant de cliquer sur ce lien, assurez-vous que cet ami vous l'a bien envoyé.
• Les suites complètes de sécurité Internet ne sont pas réservées aux ordinateurs portables et aux PC. Elles trouvent également toute leur utilité sur votre téléphone mobile.
• Un VPN est également une possibilité à envisager pour vos appareils mobiles. Le VPN sécurisera et cryptera toutes les communications intervenant entre votre mobile et Internet.
• N'installez jamais d'applications à partir de SMS. Vous ne devez installer sur votre appareil que des applications en provenance directe de l'app store officiel. Ces programmes ont été testés de manière rigoureuse avant d'être autorisés sur le marché.
• Pratiquez le principe de précaution. En cas de doute sur la sécurité d'un SMS, ne l'ouvrez pas.

La quasi totalité des SMS que vous recevez est sans problèmes. Mais il suffit d'un mauvais SMS pour totalement compromettre votre sécurité. Un peu de bon sens vous évitera de vous faire dérober votre identité.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel. Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Qu'est-ce que le smishing ?*