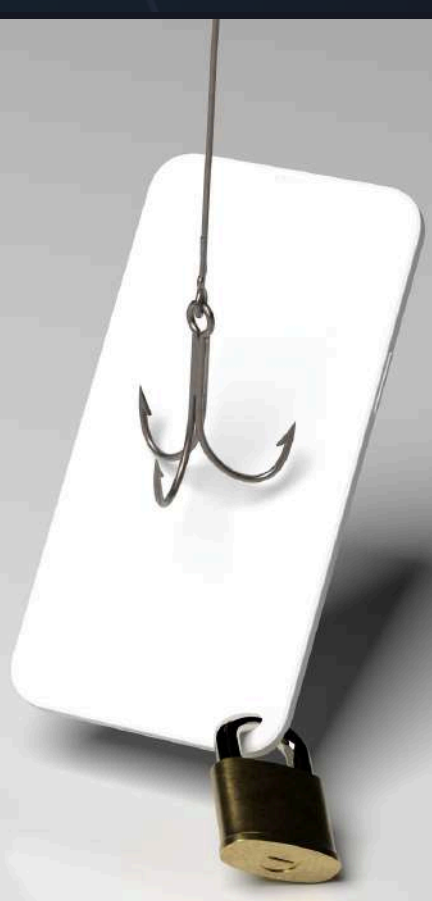
MAI 2024

Report

ANALYSE DE LA SÉCURITÉ PRIVÉE

PHISHING



Les cyberattaques sont des accès non autorisés à des systèmes ou réseaux informatiques par des tiers. Les personnes qui se livrent à ces pratiques sont appelées cybercriminels ou "hackers". Ils mènent ces actions à des fins diverses, principalement pour voler des informations, manipuler les systèmes d'entreprises ou d'organisations spécifiques et demander de l'argent en échange de la restauration de plateformes. Les cyberattaques impliquent la violation, la perte ou la manipulation de données, ce qui a un impact négatif sur la victime du délit.

En 2023, les cyberattaques ont augmenté de 87 % dans le monde, la Chine, la Russie et l'Iran étant les pays les plus touchés et l'hameçonnage étant responsable de 90 % des violations de données.

Le phishing est l'une des cyberattaques les plus courantes.

EN QUOI CONSISTE-T-IL ?

Il s'agit pour un cybercriminel d'envoyer un e-mail en se faisant passer pour une entité légitime (réseau social, banque, institution publique, etc.).

Dans le but de voler des informations privées, d'effectuer des prélèvements financiers ou d'infecter l'appareil d'un utilisateur.

Pour ce faire, le criminel joint des fichiers infectés ou des liens vers des pages frauduleuses dans le courrier électronique.

Actuellement, 3,4 milliards de courriers électroniques non sollicités sont enregistrés chaque jour, à la suite d'un hameçonnage.

En Colombie, une moyenne de quatre tentatives d'hameçonnage par minute a été signalée, et ce type d'hameçonnage figure parmi les cinq cybercrimes ayant le plus grand nombre de matérialisations.

Selon Kaspersky, une entreprise mondiale de cybersécurité et de confidentialité numérique

RECOMMANDATIONS

- Lorsque vous recevez un e-mail, assurez-vous de connaître l'expéditeur. S'il ne vous semble pas familier, méfiez-vous du message. Si ce n'est pas le cas, assurez-vous que l'e-mail que vous utilisez est correctement orthographié et qu'il correspond à celui que vous recevez habituellement.
- Ne soumettez pas de données personnelles ou d'informations financières par le biais de formulaires ou d'enquêtes envoyés par courrier. Les banques et les entreprises ne demandent pas de mots de passe, d'utilisateurs ou d'informations sensibles sur leurs produits par le biais d'aucun canal de communication.
- Évitez d'accéder aux portails bancaires via des hyperliens. Au lieu de cela, ignorez, supprimez et signalez tout message suspect à votre banque ou organisation.
  Vérifiez si l'e-mail contient des fautes de grammaire. Ces types d'attaques contiennent généralement des fautes d'orthographe et un vocabulaire inhabituel.
- Je n'ai pas fait confiance aux noms génériques des sujets de message (facture, reçu, entre autres).
  Assurez-vous que les pièces jointes ne contiennent pas l'extension « .js », car ces dernières peuvent contourner les protections antivirus.
- Activez l'option du système d'exploitation qui vous permet d'afficher les extensions de fichiers. De cette façon, vous pouvez vérifier s'il s'agit d'un exécutable, d'un document texte, d'un javascript, etc.
- Désactivez les macros Microsoft Office et faites attention aux fichiers qui vous demandent de les activer.
- Si vous pensez qu'un lien est inclus dans l'e-mail, examinez-le attentivement.
- N'oubliez pas de garder votre système d'exploitation avec antivirus et applications toujours à jour avec leur dernière version.
- Tenez-vous au courant des nouvelles tendances en matière de collecte de données, d'usurpation ou d'autres formes de criminalité découlant de l'hameçonnage afin de savoir comment agir.
- Si vous pensez avoir été victime d'hameçonnage, signalez-le aux institutions financières, organisations et groupes d'intérêt afin d'éviter la prolifération d'autres crimes comme l'escroquerie, l'externalisation, l'usurpation d'identité, etc.