La minute du PSIR

19 mars 2025 - # 71

Smishing

NIVEAU DE DIFFICULTÉ

CYBERSÉCURITÉ

PERSONNES CONCERNÉES

De plus en plus de personnes sont victimes de phishing, de ce fait, nous sommes plus sensibilisés à cette cyberattaque. Cependant, les personnes malveillantes ont inventé une nouvelle forme d'attaque : le smishing.

Le smishing est une forme d'attaque de phishing qui se déroule via SMS. Les cybercriminels envoient des messages trompeurs, souvent prétendant provenir d'organisations légitimes, pour inciter les destinataires à révéler des informations personnelles ou à cliquer sur des liens malveillants. L'objectif est de voler des données sensibles, comme des mots de passe, des informations bancaires, ou d'installer ou à installer des logiciels malveillants sur leurs appareils.

Il existe plusieurs types de messages plus ou moins similaires pour créer une pression :

- **Usurpation d'identité** : Les messages prétendent provenir de banques ou d'autres institutions financières, alertant les victimes de problèmes avec leurs comptes bancaires et les incitant à fournir des informations de connexion ou des numéros de carte bancaire.

- **Notification de livraison** : Les SMS simulent des notifications de livraison de colis, demandant aux destinataires de cliquer sur des liens pour suivre ou reprogrammer une livraison, liens qui mènent à des sites web malveillants.

- **Alertes de sécurité** : Les messages avertissent les utilisateurs de prétendues violations de sécurité sur leurs comptes en ligne ou leur messagerie, les incitant à cliquer sur des liens frauduleux pour récupérer leurs mots de passe.

- **Usurpation d'identité de services gouvernementaux** : les malfaiteurs se font passer pour des organismes gouvernementaux, afin de soutirer de l'argent ou des informations aux victimes.

- En savoir plus