MENACES SUR INTERNET

RÉFLÉCHISSEZ BIEN AVANT DE CLIQUER

Vous risquez de perdre de l'argent, des données personnelles, et même les données que vous avez enregistrées si votre téléphone ne fonctionne plus. Ne vous faites pas avoir!

COMMENT EST-CE POSSIBLE?

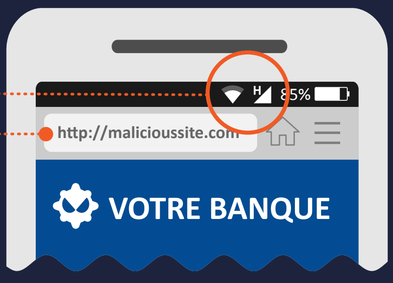
PAR PHISHING: Les utilisateurs trompés sont encouragés à fournir des informations personnelles à des entités qui se font passer pour des interlocuteurs fiables. Ce type de message est transmis par e-mail, par textos et par le biais des réseaux sociaux.

NAVIGATION SUR SITES INTERNET: Il se peut que votre smartphone soit simplement infecté suite à la visite d'un site web malveillant.

TÉLÉCHARGEMENT DE FICHIER: Les liens et pièces-jointes malveillants peuvent être intégrés à un e-mail.

POURQUOI ÇA MARCHE?

Les appareils mobiles sont **CONSTAMMENT** connectés à l'Internet.



LA TAILLE RÉDUITE DE L'ÉCRAN DE L'APPAREIL représente un risque. Les navigateurs mobiles affichent des URL sur un espace d'écran limité et cela rend difficile l'authentification du domaine.

CONFIANCE IMPLICITE DE L'UTILISATEUR en la nature personnelle de son appareil mobile.

QUE FAIRE?

Soyez méfiant en cas de SMS ou d'appel d'une entreprise requérant des informations personnelles. Vérifiez la légitimité du message/de l'appel en rappelant directement l'entreprise sur son numéro officiel.

Lorsque vous naviguez sur le web avec votre portable, assurez-vous d'une connexion sécurisée par HTTPS. Celle-ci est toujours mentionnée en début d'URL.

Ne cliquez jamais sur un lien/une pièce-jointe d'un e-mail non sollicité. Supprimez immédiatement celui-ci.

^BE:%}
W@RY
*)Z#$=

Méfiez-vous de sites contenant des erreurs de grammaire, d'orthographe ou en basse résolution.

Si possible, installez une appli de sécurité mobile qui vous avertira de toute activité suspecte.

EUROPOL EC3 European Cybercrime Centre

POLICE NATIONALE

#MobileMalware