POLICE MUNICIPALE
DE
SAINTE-SOULLE

LA CYBERCRIMINALITÉ

Un hacker met en moyenne **10 minutes à « cracker » un mot de passe composé de 6 lettres, 3 ans pour un mot de passe de 7 lettres minuscules et majuscules**. Et, **s'il le pouvait, il mettrait 463 ans pour un mot de passe de 8 caractères contenant lettres majuscules et minuscules, chiffres et symboles**.
source : frenchweb.fr

ESCROQUERIES LES PLUS FREQUENTES SUR INTERNET

- Achats effectués en ligne sur des sites de ventes aux enchères, sans retour de biens.
- Utilisation frauduleuse de numéros de carte bancaire sur Internet.
- Le phishing_("hameçonnage") : Faux mail de banque. L'émetteur se fait passer pour votre banque et veut connaître vos coordonnées bancaires afin de prélever de l'argent sur votre compte.
-

EN CAS DE TRANSACTION EN LIGNE

- Si vous achetez un bien très onéreux, organisez une rencontre avant la transaction,
- Si vous vendez un bien, attendez d'avoir matériellement reçu l'argent, avant de livrer le bien.
- Dans la mesure du possible, privilégiez les **sites reconnus**.
- Vérifiez systématiquement l'adresse du site sur lequel vous vous trouvez. Soyez attentifs aux avis des internautes qui ont déjà passé commande sur ce site.
- Si vous ne connaissez pas le site sur lequel vous vous trouvez, **soyez attentifs aux avis des internautes qui ont déjà passé commande sur ce site**.
- Au moment de rentrer les coordonnées de votre carte bancaire, vérifiez que l'adresse de la page débute par ***https://*** et que votre navigateur internet affiche un **cadenas** près de la barre d'adresse. La présence de ces deux éléments indique que vos informations seront cryptées pour plus de sécurité et ne pourront être interceptées par un tiers malveillant.

Internet Explorer	Firefox	Chrome	Safari
	https:	https:	https

HTTPS = *HyperText Transfer Protocol Secure.*
Littéralement : "Protocole de transfert hypertexte sécurisé"

EN CAS D'UTILISATION FRAUDULEUSE DE VOTRE CARTE DE PAIEMENT

- Si vous êtes victime d'une escroquerie sur Internet, vous devez en premier lieu le signaler à votre banque.
- Déposez plainte à la gendarmerie
- Suite à ce dépôt de plainte, une enquête pourra être ouverte et transmise au procureur de la République

LE « PHISHING » OU HAMEÇONNAGE

- Ne répondez jamais à un mail vous demandant de transmettre vos coordonnées bancaires.
- Votre banque ou toute autre institution bancaire ne vous demandera jamais vos coordonnées bancaires par mail.
- En cas de doute, appelez immédiatement votre banque.

oooOOOooo