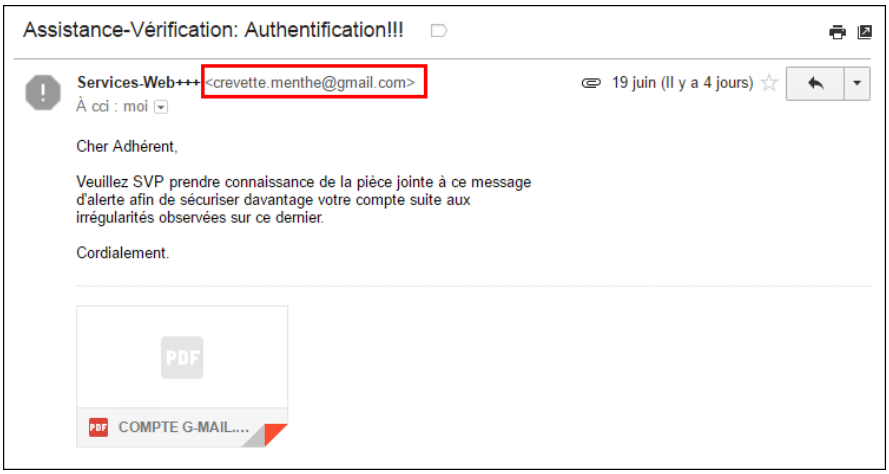
Aide pédagogique à l'utilisation des ressources numériques

Arnaque : Demande d'informations personnelles par courriel.

Depuis quelques temps, certains utilisateurs reçoivent des messages frauduleux destinés à partager des informations personnelles telles qu'un mot de passe ou un numéro de carte de paiement. Cette technique est connue sous le nom d'hameçonnage ou de phishing.
Soyez toujours très prudent avec ce genre de messages qui vous demandent des informations personnelles ou qui vous renvoient vers une page Web demandant ce type d'information. Méfiez-vous avant de cliquer sur le lien proposé !

Vous pouvez en tout cas être sûr d'une chose : Google, Gmail, Microsoft comme votre banque ne demandent jamais aux utilisateurs de fournir de telles informations par courriel. Si vous recevez un message de ce type, méfiez-vous et mieux encore, n'en tenez pas compte !
Voici quelques conseils qui devraient attirer votre attention et vous permettre de déceler l'arnaque.

1. **Vérifiez l'adresse de l'expéditeur**.
   L'adresse de l'expéditeur devrait déjà vous inviter à la prudence. Si les spammeurs utilisent des adresses qui ressemblent de plus en plus à des adresses officielles, il y a souvent moyen de trouver une différence (dans le cas ci-dessous, l'adresse crevette.menthe@gmail.com ne semble pas à première vue avoir de lien avec un service de Google).



2. **Vérifiez le lien proposé.**
   Dans le corps du message ou dans la pièce jointe souvent un lien vous est proposé pour que vous puissiez compléter vos informations ou les mettre à jour.
   Il s'agit bien sûr d'une redirection vers un site frauduleux.
   Passez la souris sur le lien, l'adresse du site apparait dans une bulle et vous permet déjà de vérifier l'exactitude du site.

3. **Lisez attentivement** le corps du message ou la pièce jointe et **décelez** les erreurs.
Souvent un ou plusieurs **indices** doivent vous inviter à la prudence.

- Le message provient d'une entreprise bien connue (Google, Microsoft, …).
- Le message est alarmiste, il y a une menace de fermeture du compte (Voir les répétitions dans le message ci-dessous).
- Il y a une promesse d'argent avec peu ou sans effort ou une proposition qui semble très alléchante.
- Une mauvaise grammaire, des fautes d'orthographe.
- Une signature anonyme.
- Une finition approximative (Dans le cas ci-dessous, le logo Gmail).

VOTRE COMPTE GMAIL VA ÊTRE SUPPRIME

Cher(e) client(e),

Gmail a récemment découvert des séries de tentatives d'activités illégales sur votre compte à partir de différents lieux et fermera votre compte tel qu'il a été marqué comme un compte émetteur de courrier indésirable.

Veuillez examiner les détails de la tentative :

Adresse IP : 419.750.283:8080

Position : Moscou, Russie.

Suite à ce problème veuillez suivre le protocole de sécurité afin d'éviter la suppression définitive de votre compte dans un délai de 24h après lecture de ce message.

Veuillez confirmer vos informations en cliquant sur le lien suivant : (Service-Enregistrement)

Nous nous engageons à traiter de façon confidentielle et à conserver les données fournies par nos utilisateurs selon les directives et lois.

Attention !!!
Le Titulaire du compte qui ne parvient pas à vérifier son compte après 24 heures de la réception de cet avertissement perdra son compte en permanence.

Nous espérons que vous apprécierez votre messagerie.
L'équipe Gmail