La réception de Mails

1°) Introduction

La réception de courriels peut constituer un danger réel pour la sécurité de vos informations personnelles et professionnelles. Avec l'augmentation des menaces en ligne, il est crucial de savoir comment se protéger. Voici des conseils simples et pratiques pour reconnaître les mails suspects et éviter les pièges.

2°) Vérification de l'Expéditeur

- *Adresse e-mail :* Vérifiez que l'adresse e-mail de l'expéditeur est correcte et connue. Assurez-vous que l'orthographe de l'adresse est exacte. Les fraudeurs utilisent souvent des adresses similaires à celles de sources fiables en changeant légèrement une lettre ou en ajoutant des chiffres pour tromper les destinataires. Par exemple, "example@company.com" pourrait être modifié en "example@cornpany.com" (en changeant le "m" en "rn"). Si vous ne lisez pas attentivement l'adresse de l'expéditeur vous pourriez passer au travers d'une faute et ainsi vous faire piéger.

- *Nom de l'expéditeur :* Méfiez-vous si vous ne reconnaissez pas le nom de l'expéditeur.

3°) Analyse du Contenu

- *Liens :* Ne cliquez jamais sur des liens dans des mails suspects. Passez la souris sur les liens pour voir où ils mènent réellement.

- *Pièces jointes :* N'ouvrez jamais les pièces jointes provenant de sources inconnues ou inattendues.

- *Fautes d'orthographe :* Bien que les mails de phishing contiennent souvent des erreurs de grammaire et des fautes d'orthographe, certains peuvent sembler plus professionnels grâce à l'utilisation de l'intelligence artificielle (IA). Restez vigilant même si un courriel semble bien rédigé.

- *Informations contenues dans le mail :* Ne faites pas confiance aux informations dans le mail, comme des numéros de téléphone ou des liens vers des sites web, qui pourraient rediriger vers un complice des fraudeurs.

4°) Sécurité Technique

Importance des Mots de Passe pour la Messagerie Mail

Un mot de passe fort et unique pour votre messagerie mail est essentiel. Si un délinquant accède à votre messagerie, il pourrait :

- *Demander la réinitialisation des mots de passe* de tous vos comptes en ligne, y compris les réseaux sociaux, les services bancaires et les plateformes de shopping.

- *Accéder à vos informations personnelles* et les utiliser pour des activités frauduleuses.

- *Envoyer des courriels frauduleux* en se faisant passer pour vous, ciblant vos contacts personnels et professionnels.

- *Collecter des informations sensibles* qui peuvent être utilisées pour voler votre identité.

- *Modifier les paramètres de sécurité* de vos comptes pour rendre plus difficile la récupération de ces comptes.

- *Faire des redirections de mails* ce qui rendrait inutile le changement de mot de passe de votre boite mail après découverte du pot aux roses, puisque le délinquant aura mis une politique de redirection qui lui renverra vos mails dès réception.

Antivirus

Un antivirus est un logiciel qui détecte et élimine les logiciels malveillants. Il fonctionne en analysant les fichiers et les programmes sur votre ordinateur pour détecter des signatures de logiciels malveillants connus. Les antivirus modernes utilisent aussi l'analyse heuristique pour identifier de nouveaux types de menaces en se basant sur le comportement des fichiers.

EDR (Endpoint Detection and Response)

L'EDR est un outil de sécurité qui surveille en continu votre ordinateur pour détecter des activités suspectes. Il utilise des techniques avancées pour repérer rapidement les menaces et y répondre.

Mailinblack

C'est un service de sécurité pour les emails qui vous protège contre le spam, les phishing et d'autres menaces. Il fonctionne en filtrant les messages entrants, en bloquant ceux qui semblent suspects et en vérifiant l'authenticité des expéditeurs. Cela permet aux utilisateurs de se concentrer sur les emails importants sans être dérangés par des contenus indésirables ou dangereux. En gros, c'est un bouclier pour la boîte de réception !

5°) Signalement

- Cybermalveillance.gouv.fr : Retrouvez un maximum d'information sur le site Cybermalveillance.gouv.fr (https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-signaler-un-mail-de-phishing). Des fiches guides, des fiches reflexes, des conseils et plein d'informations libre de droits que vous pouvez donc utiliser comme bon vous semble.

- Signal Spam : Utilisez Signal Spam (https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-signaler-un-mail-de-phishing) pour signaler les messages frauduleux.

- Pharos : Signalez les contenus illégaux sur Pharos (https://www.internet-signalement.gouv.fr/PharosS1/).

- Plateforme Thésée : La plateforme Thésée (https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/plainte-en-ligne-arnaques-internet-thesee) permet aux victimes d'escroqueries en ligne de porter plainte directement en ligne sans avoir à se rendre au commissariat ou à la gendarmerie. Elle centralise les signalements et rend les enquêtes plus efficaces.

- Plateforme Perceval : La plateforme Perceval permet de signaler toute fraude à la carte bancaire, y compris une simple utilisation frauduleuse. Elle a été mise à disposition du grand public par la gendarmerie nationale en juin 2018. Les signalements sont traités rapidement et vous recevez un récépissé dans votre espace personnel.

- 33700 : Transférez et/ou signalez les SMS et appels vocaux indésirables au 33700.

6°) Application Ma Sécurité

L'application Ma Sécurité permet d'accéder à des informations de prévention et de signaler des incidents de sécurité directement depuis votre smartphone. Elle offre également des conseils personnalisés et une assistance rapide en cas de problème. Disponible sur les plateformes mobiles, cette application est un outil pratique pour rester informé et protégé.

7°) Conclusion

En suivant ces conseils, vous pouvez éviter les dangers liés à la réception de mails.

Gardez en mémoire que **94 % des cyberattaques** ont pour origine la réception d'un e-mail malveillant.

Cybersécurité, tous concernés.

Référent cybersécurité de la Gendarmerie de la Marne

Adjudant Yannick DUPONCHEL