Éveil critique à l'usage d'internet.

A- **Delhaize** : Qu'y-a-t-il de suspect dans ce message ?

La date et l'heure du message.

Ce n'est pas suspect. Les entreprises envoient régulièrement des mails ou des messages automatisés. La date et l'heure d'envoi d'un message ne constituent donc pas une garantie d'authenticité.

Le lien renvoyant au site web (http://delhaize-be.site).

Contrôlez toujours tous les liens avant de cliquer dessus. Dans ce cas-ci, l'adresse Internet devrait être « http://www.delhaize.be ». Vous pouvez le contrôler facilement en positionnant votre curseur au-dessus du lien sans cliquer dessus. C'est suspect.

Une campagne promotionnelle pour l'anniversaire de Delhaize.

Les entreprises organisent régulièrement des campagnes promotionnelles pour des occasions spéciales. Ce n'est pas suspect.

Delhaize envoie ce message promotionnel via Instant Messaging

En cas de messages reçus via Instant Messaging, demandez-vous toujours si l'expéditeur dispose bien de votre numéro de téléphone. Par exemple, Delhaize proposera ses offres par mail ou via des dépliants déposés dans votre boîte aux lettres, mais pas via Instant Messaging. C'est suspect.

Un cœur est reproduit à la fin du message.

Les émojis sont rarement utilisés dans les communications professionnelles. L'utilisation de ces petits symboles peut indiquer une tentative de phishing. Dans ce cas-ci c'est suspect.

La promotion est trop belle pour être vraie.

Si une promotion est trop belle pour être vraie, il faut généralement se méfier. Un smartphone coûteux proposé à un prix défiant toute concurrence ou des bons d'achat d'un montant incroyable sont toujours suspects.

B- **Bpost** : Qu'y-a-t-il de suspect dans ce message ?

La communication est inattendue.

Vous n'avez pas commandé de colis ? Il y a peu de chance que vous receviez un code de suivi ou d'autres informations concernant un colis. Ne réagissez pas aux mails qui vous incitent à cliquer sur des liens. C'est suspect.

Le mail contient une photo.

Les photos contenues dans les mails ne sont pas suspectes en soi. Contrôlez la qualité de l'image et des logos utilisés : les mails de phishing n'affichent pas toujours le logo le plus récent ou contiennent des images floues.

Le domaine de l'adresse e-mail (@xyz542.be) est étrange.

Un expéditeur professionnel utilisera toujours un nom de domaine d'entreprise officiel pour envoyer des mails, par exemple @nomdelafirme.be. Vérifiez l'expéditeur si vous n'êtes pas sûr(e) de l'authenticité du mail. C'est suspect!

Activité basée du questionnaire présent sur Safeonweb

Vous êtes invité(e) à télécharger une pièce jointe.

Les pièces jointes inattendues dans un mail envoyé par une entreprise sont toujours suspectes. Il peut s'agir d'un programme ou d'un fichier zip qui, une fois ouvert, est susceptible d'endommager votre ordinateur ou vos fichiers. Attention: c'est suspect!

Le mail comporte un numéro de suivi.

Il n'y a rien d'anormal dans le fait qu'un fournisseur communique un numéro de suivi. Mais cliquer sur un lien contenu dans un mail est risqué. Il est préférable de vous rendre vous-même sur le site officiel du fournisseur pour y entrer le numéro de suivi. De cette façon, vous êtes sûr(e) de ne pas cliquer sur un lien frauduleux. Dans ce cas-ci, ce n'est pas suspect.

La date et l'heure du mail.

Les entreprises envoient régulièrement des mails ou des messages automatisés. La date et l'heure d'envoi d'un message ne constituent donc pas une garantie d'authenticité. Ce n'est pas suspect.

C- **Mail de la banque** : Qu'y-a-t-il de suspect dans ce message ?

Cathy n'est pas une cliente de cette banque.

Si vous n'êtes pas client(e) de la banque en question, vous ne devriez logiquement pas recevoir de carte bancaire. C'est suspect!

La mention « action unique ».

À l'instar d'autres entreprises, les banques organisent occasionnellement des actions : il peut s'agir de promotions ciblant des clients existants ou d'actions de recrutement de nouveaux clients. Ce n'est pas suspect.

Le domaine de l'adresse e-mail (@vnnabsbns.com).

Quel domaine bizarre. Un expéditeur professionnel utilisera toujours un nom de domaine d'entreprise officiel pour envoyer des messages. Vérifiez l'expéditeur si vous n'êtes pas sûr(e) de l'authenticité du mail. C'est suspect!

Le langage employé dans le mail est inopportun.

Une entreprise, en particulier un organisme financier, n'emploiera jamais un langage inopportun dans ses communications professionnelles. Les mails émanant d'organismes financiers contiennent généralement des informations de contact et insistent sur le fait de ne jamais transmettre ses données personnelles par mail. C'est suspect.

Interpellation par le prénom et le nom de famille.

Si vous êtes client(e) quelque part, l'entreprise dispose souvent de vos nom et prénom. Votre nom complet est alors utilisé pour apporter une touche plus personnelle au message. Toutefois, votre nom peut également être utilisé en cas de phishing. Le fait de voir votre nom ne doit donc pas vous amener à considérer immédiatement le mail comme authentique.

Le mail est défini avec une priorité « haute ».

Les mails adressés aux clients ne comportent jamais la mention « priorité haute ». Ce subterfuge est utilisé pour attirer l'attention et exercer une pression sur le destinataire qui commettra, de ce fait, plus facilement une erreur. C'est suspect.

D- Facebook – Twitter – Instagram - …

Une publication sur votre mur plutôt qu'un message privé.

Vos amis peuvent bien entendu publier des messages sur votre mur. Ce n'est pas suspect. S'il s'agit d'une question personnelle partagée publiquement, nous vous recommandons de contacter votre ami(e) pour vous assurer que c'est lui/elle qui a publié le message.

Interpellation par la formule « Bonjour à tous ».

Les profils piratés sont souvent utilisés pour atteindre de grands réseaux. Une interpellation générale de l'ensemble de votre réseau doit vous alerter. C'est suspect.

Une personne a réagi avec un émoji qui pleure.

Vous ne pouvez pas déterminer la fiabilité du message original à partir des réactions aux messages. Ce n'est pas parce que les réactions font penser que le message est correct que c'est le cas. Ce n'est pas suspect.

Vous devez d'abord vous connecter avant de pouvoir visualiser les images.

Les amis qui partagent des photos entre eux utilisent rarement des plateformes photos avec identification. Les albums privés sur les réseaux sociaux ou un dossier sur une plateforme cloud de confiance sont plus souvent utilisés. C'est pourquoi nous vous conseillons de toujours contrôler les liens avant de cliquer dessus. C'est suspect.

Vous pouvez partager le message.

Si un message est publié publiquement sur votre mur, vous pouvez également le partager. Ce n'est pas suspect. Vous trouvez qu'un message est suspect ? Ne le partagez surtout pas ! Contactez votre ami(e). S'il/elle n'a pas connaissance du message, supprimez-le immédiatement afin de limiter les dégâts au sein de votre réseau.

Le lien du site web (http://tinyurl.com/accident88).

Vous devez toujours vous montrer prudent(e) avec les liens minimisés par bit.ly, goo.gl, tinyurl ou un autre service. Vous pouvez copier le lien du site web et le contrôler en utilisant un service tel que checkshorturl.com. C'est suspect.

E- Lettre de la Police : Qu'y-a-t-il de suspect dans ce message ?

Vous n'êtes pas interpellé(e) par votre nom.

Un organisme officiel vous interpellera toujours par votre nom. C'est suspect.

L'amende a été envoyée par mail.

La police enverra toujours une amende par courrier. C'est suspect !

L'adresse e-mail de l'expéditeur (federalepolitie@hsruhaeu.com).

La police fédérale n'a pas recours aux services de messagerie gratuits ou .com ; les mails de la police sont envoyés à partir d'une adresse e-mail @police.belgium.eu ou @federalepolitie.be. C'est suspect.

Paiement sur une page Bancontact ou Mister Cash.

La police fédérale ne vous oblige pas de payer sur une plateforme de paiement en ligne. C'est suspect.

Une date et une heure concrètes sont indiquées dans le mail.

La mention d'une date et d'une heure concrètes n'est pas nécessairement le signe d'une tentative de phishing parce que ces données figurent également sur les vraies amendes. Ce n'est pas suspect.

L'objet du message est trop direct pour qu'il s'agisse d'un mail de la police.

Même si l'objet du message est très direct, ce n'est pas d'office le signe d'une tentative de phishing. En cas de doute, vérifiez l'expéditeur. Ce n'est pas suspect.

F- **Offre commerciale** : Qu'y-a-t-il de suspect dans ce message ?

Le lien reproduit dans la partie supérieure du mail, après la mention « Le mail s'affiche-t-il correctement ? ».

Ce n'est pas suspect, mais il est toujours préférable de contrôler les liens avant de cliquer dessus. La plupart des bulletins d'information sont également disponibles en passant par un navigateur Internet. Les entreprises procèdent ainsi parce que certains logiciels de messagerie n'affichent pas correctement leurs bulletins d'information.

On demande d'enregistrer des appareils.

La demande d'enregistrement peut être un piège. Mais dans ce mail, l'enregistrement ne se fait pas en suivant un lien, mais est effectué sur des appareils externes. Le mail vous explique comment procéder idéalement. Ce n'est pas suspect.

Les liens renvoyant aux réseaux sociaux dans la partie inférieure du mail.

Les liens renvoyant aux réseaux sociaux dans les mails sont très répandus. Ce n'est pas suspect, mais encore une fois, il est conseillé de contrôler d'abord le lien avant de cliquer dessus.

L'adresse e-mail de l'expéditeur (@sim.firme.be).

Le domaine principal de l'expéditeur est @firme.be. Seul la firme peut créer des sous-domaines. Nous pouvons par conséquent affirmer dans ce cas-ci que sim.firme.be est un domaine sûr. Ce n'est pas suspect.

M. Smet est interpellé par son nom de famille.

Les clients sont souvent interpellés par leur nom et prénom dans les communications directes. Étant donné qu'il s'agit d'une formule d'abonnement, l'entreprise puise ces informations dans sa base de données. Ce n'est donc pas suspect.

M. Smet utilise déjà ce produit.

Les entreprises communiquent souvent des informations relatives à leurs produits. Ce n'est pas suspect.