Exemple d'arnaque d'une vente en ligne :

Achat d'un article qui est mis en vente via Marketplace (Facebook) ou 2ememain.be :

Le suspect montre son intérêt pour l'article en vente et donne une excuse pour un envoi via DPD. A la suite de cela, un mail est envoyé du soi-disant DPD et la victime doit remplir des données personnelles et bancaires. Ensuite, une personne contacte la victime pour lui donner la procédure à suivre et lui demande d'utiliser son digipass. A ce moment-là, le suspect a accès au compte bancaire de la victime et réalise des transactions.

Digipass →

Exemple d'arnaque via SMS :

Sms frauduleux :

La victime reçoit un sms disant qu'elle a payé une facture en double ou qu'elle a droit à un remboursement, elle est invitée à cliquer sur un lien. Ensuite elle reçoit un appel d'une personne qui prétend être de la société dudit sms.

Lors de la communication téléphonique le suspect demande à la victime de faire des codes sur son digipass. Celle-ci s'exécute … A partir de ce moment-là, le suspect a accès au compte bancaire de la victime et réalise des transactions.

Vous avez été escroqué ?

À partir du moment où vous avez perdu de l'argent ou que vous êtes victime d'une extorsion, contactez votre banque et/ou Cardstop au 070 344 344 si vous avez transmis des informations bancaires, si de l'argent disparaît de votre compte bancaire ou si vous avez transféré de l'argent à un fraudeur. De cette façon, les éventuelles transactions frauduleuses pourraient être bloquées.

Ensuite nous vous conseillons de faire une déclaration à la police. Vous pouvez le signaler à la police locale de votre lieu de résidence ou via https://www.police-on-web.be/

Si vous voulez signaler une fraude, vous pouvez surfer sur https://pointdecontact.belgique.be/meldpunt/fr/bienvenue. Le SPF Economie lance un point de contact unique pour les victimes de fraudes, tromperies, arnaques et escroqueries.

Ne Tombez pas dans le piège !

Sur le site **www.safeonweb.be/fr**, apprenez à reconnaître les messages frauduleux, faites le test du phishing et apprenez à ne plus vous faire avoir.

Le site **safeonweb.be** vous explique comment (ré)agir correctement.

SafeOnWeb est un projet du service public 'Centre pour la Cybersécurité'

Editeur responsable : Vanhaeren Stephane
Avenue albert 1er à 1420 Braine L'Alleud

Escroquerie avec internet / Fraude informatique

Les instances officielles ne vous demanderont JAMAIS de fournir vos codes personnels ou les résultats de votre digipass par mail, SMS ou téléphone.

ZONE DE POLICE 5273 BRAINE - L'ALLEUD

Les modes opératoires les plus courants dans le cadre de ces faits :

Envois d'e-mails/SMS, création de faux sites internet ou de fausses nouvelles.
Ex. :

- Faux messages qui semblent provenir de la Police Fédérale / EUROPOL **(objet : votre convocation)**

- Faux messages provenant de la Commission Européenne **(objet : remboursement)**

- Faux messages de son opérateur télécom **(objet : facture impayée)**

- Faux messages de sa mutuelle **(objet :remboursement)**

- Faux messages de DHL **(objet : commande ou avis de livraison)**

- Faux messages de Microsoft **(objet : Mise à jour)**

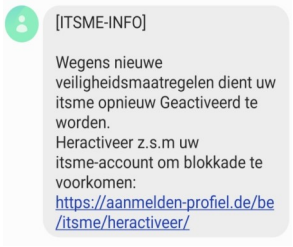
- Faux messages de Itsme **(objet : (ré)activation du compte/ connexion suspecte)**

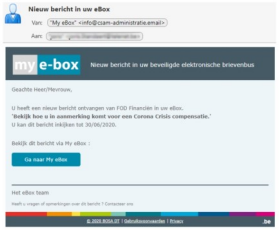
- Faux messages de My e-box **(objet : Informations importantes concernant votre vaccin COVID-19 ou des informations concernant une indemnisation COVID-19)**

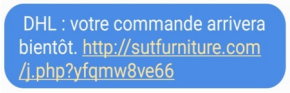
- Faux messages : Paypal **(objet : une action de votre part est nécessaire)**

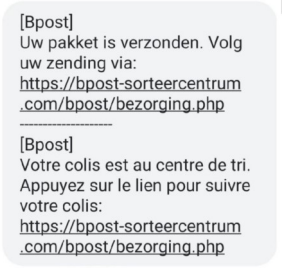
- Faux messages de Bpost **(objet : votre colis est en route, suivez-le ici)**

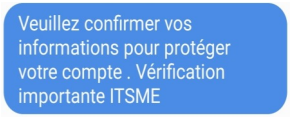
Méfiez-vous !

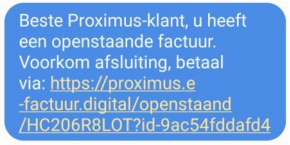


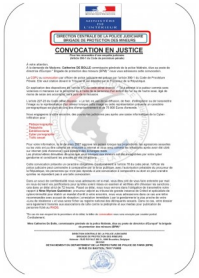












Mesure de prudence :

- Ne cliquez pas sur un lien suspect et n'ouvrez pas les pièces jointes.

- Ne répondez jamais à un mail/SMS qui semble étrange, suspect. Ne répondez jamais à un appel téléphonique à une personne insistante et menaçante afin d'effectuer des paiements d'urgence.

- Attention à un mail/SMS qui contient beaucoup de fautes d'orthographe et de langage.

- Recherchez, via votre navigateur, le site officiel du supposé expéditeur du message afin de comparer l'adresse et vérifiez sur le site officiel de l'émetteur si une action est réellement requise.

- Ne communiquez **JAMAIS** vos données personnelles ou bancaires via téléphone, SMS ou mail à la demande d'un tiers.

- N'utilisez pas votre digipass via un mail, un sms ou une demande téléphonique.

Vous avez cliqué sur un lien suspect ?

- Si vous avez cliqué, ne remplissez pas les champs et annulez toute interaction.

- Si vous avez fourni un mot de passe que vous utilisez ailleurs, changez-le immédiatement.

- Si vous avez cliqué sur un lien qui ouvre un site web où vous devez soumettre vos coordonnées bancaires, vérifiez d'abord qu'il s'agit bien du site web de votre banque (ouvrez le site de votre banque et comparez). Si vous avez le moindre doute, n'effectuez pas le paiement.