Boîte à outils : inspiration prévention cyber

ibz Intérieur Binnenlandse Zaken

.be

Cette nouvelle version du manuel d'inspiration en prévention cyber vous donne un aperçu des principaux types d'escroqueries en ligne. Vous y trouverez également quelques astuces de prévention, des conseils aux victimes, les coordonnées d'organisations supralocales auxquelles vous pouvez vous adresser et quelques pratiques locales de cyberprévention inspirantes.

Cette boîte à outils s'adresse en priorité aux autorités locales, qui souhaitent se familiariser davantage avec la cyberprévention car elles sont hélas de plus en plus confrontées à celle-ci. Le niveau local est stratégique dans cette forme de prévention car il permet une approche globale de la cybercriminalité.

Nous vous souhaitons beaucoup de plaisir à la lecture.

Principaux types d'escroqueries en ligne

Phishing

Le phishing est une escroquerie en ligne grâce à laquelle des cybercriminels tentent d'obtenir les données bancaires et les codes bancaires personnels de leurs victimes. À cette fin, ils utilisent de faux moyens de communication digitale comprenant un lien vers un faux site web, une pièce jointe suspecte ou une demande de téléchargement d'application.

Plus d'informations : https://campagne.safeonweb.be/fr/phishing

Fraude au service d'assistance

Forme d'escroquerie où les fraudeurs se font passer pour des employés d'un service d'assistance d'une grande entreprise informatique (banques et entreprises technologiques, par exemple). Ils prétendent qu'il y a un problème majeur sur votre PC et qu'il est urgent d'agir.

Plus d'informations : Je suis contacté par un inconnu pour un problème de pc | Safeonweb

Fraude aux comptes à sécurité renforcée

Ici, les escrocs abordent généralement les citoyens en deux étapes : ils envoient d'abord un message de phishing pour extraire les codes bancaires personnels afin d'accéder au compte bancaire. Les escrocs appellent ensuite la personne, ou se rendent au domicile de celle-ci, en se faisant passer pour un employé de banque ou de Card Stop et demandent de transférer de l'argent sur un autre compte soi-disant nouveau et sécurisé. Pour ce faire, certains escrocs vont même jusqu'à se rendre au domicile de la victime potentielle pour lui donner les instructions nécessaires

Plus d'informations : Fraude aux comptes à sécurité renforcée : nos conseils ! | Febelfin

Fraude à l'émotion : Fraude à la demande d'aide

Les fraudeurs se font passer pour une connaissance ou un être cher de la victime. Ils lui demandent une aide financière urgente par le biais de messages électroniques, de SMS ou d'applications. Pour gagner sa confiance, ils utilisent des informations personnelles sur les personnes connues/chères à la victime (également connu sous le nom d'ingénierie sociale).

Plus d'informations : Méfiez-vous de la fraude à la demande d'aide financière urgente d'un soi-disant proche | Febelfin

Fraude à l'émotion : Arnaque à l'amour ou à l'amitié

Les escrocs prennent contact avec la victime potentielle qu'ils soupçonnent d'être seule ou en recherche d'amour ou d'amitié. Les sites de rencontre sont particulièrement exposés à ce type de fraude. Contrairement à la plupart des autres formes d'escroquerie en ligne, l'auteur investit beaucoup de temps pour gagner la confiance de la victime, après quoi il lui demande de l'argent. Ainsi, un prétexte d'urgence sera souvent utilisée comme appât dans ce type d'escroquerie.

Plus d'informations : Les fraudes à l'amitié | Trop Beau Pour Être Vrai (tropbeaupouretrevrai.be)

Fraude à l'achat et à la vente

La fraude à l'achat consiste à transférer de l'argent à une personne ou à une entreprise sans recevoir le service ou le produit qui a été payé. Dans la fraude à la vente, les marchandises sont livrées mais le destinataire ne les paie pas. À cet égard, les sites web d'occasion sont un endroit propice pour commettre ces délits.

Plus d'informations : Gare aux escrocs sur les sites de ventes en ligne | Safeonweb

Fraude au CEO

La fraude au CEO est une forme d'escroquerie dans laquelle les cybercriminels contactent une entreprise (par téléphone ou par courrier électronique) pour lui demander d'effectuer un paiement important vers leur compte en banque. Les cybercriminels prennent l'identité du CEO, du directeur financier ou d'une personne de confiance et demandent à un employé des finances ou de la comptabilité d'effectuer un paiement urgent.

Plus d'informations : La fraude au CEO - Mieux vaut prévenir que payer | Centre pour la Cybersécurité Belgique (belgium.be)

Fraude à l'investissement

C'est une forme d'escroquerie où les fraudeurs vous proposent d'acheter des actions ou d'autres produits financiers fictifs ou sans valeur. Les fraudeurs vous contactent généralement sans que vous leur ayez rien demandé pour vous proposer une offre fantastique au rendement considérable et n'hésitent pas à vous mettre sous forte pression.

Plus d'info : https://febelfin.be/fr/themes/fraude-et-securite/types-de-fraudes-en-ligne/fraude-a-l-investissement

Fraude pyramidale

La fraude pyramidale est une forme de fraude où l'initiateur de la pyramide propose aux investisseurs potentiels des placements pour lesquels il promet un rendement très intéressant.

L'initiateur reçoit alors les premiers versements des investisseurs qui se laissent aveugler par les gains promis. Contrairement à ce qui est promis aux investisseurs, leur argent n'est pas réellement investi. Par contre, il leur est demandé d'apporter eux-mêmes de nouveaux investisseurs, ce qui augmenterait encore leurs gains. Les nouveaux investisseurs qui rejoignent le système apportent leur argent, qui n'est à nouveau pas investi, mais sera en partie utilisé pour rémunérer les premiers investisseurs.

Dans le cadre de cette fraude, tous les consommateurs forment ensemble une pyramide. Plus le consommateur se trouve haut dans l'organisation pyramidale, plus les chances qu'il gagne d'argent sont élevées.

Plus d'info : https://www.fsma.be/fr/fraude-pyramidale

La mule financière

Les mules financières sont des personnes qui laissent/ font transiter illégalement de l'argent par le biais de leur compte. Il s'agit souvent de personnes qui ont des difficultés financières et/ ou veulent gagner de l'argent facile. Celui ou celle qui donne suite à ce genre de "proposition

d'échange" devient une mule financière. Les criminels ont besoin de mules et de leur compte bancaire pour faire transiter ou pour retirer illégalement de l'argent. Cet argent a le plus souvent été dérobé par le biais du phishing.

En utilisant le compte et/ou la carte d'une mule financière, les criminels effacent toute trace personnelle. Agir de la sorte risque de causer bien des problèmes à la mule: des menaces physiques, la police à sa porte, le blocage ou la fermeture de son compte, un casier judiciaire, un compte pillé, avec en plus un risque de devoir indemniser les victimes.

Plus d'info : https://febelfin.be/fr/themes/fraude-et-securite/mules-financieres/qu-est-ce-qu-une-mule-financiere

Aide aux cyber-victimes

Si les cybercriminels ont pu accéder à votre compte bancaire et que vous êtes donc victime, veuillez contacter immédiatement et prioritairement les instances suivantes :

1) **Card Stop (078 170 170)**
   - Numéro gratuit accessible 24/7
   - Bloquer la carte de banque

2) **Banque**
   - Bloquer les autres moyens de paiement
   - Obtenir des preuves, en particulier des relevés de compte
   - Faire bloquer l'accès à l'application bancaire : https://cardstop.be/fr/home/Je-veux-bloquer/Bloquez-via-lemetteur.html

3) **Police locale**
   - Pour y déposer une plainte, avec des preuves, en réalisant un maximum de captures d'écrans.

Si d'autres données personnelles (par exemple, les données de la carte d'identité, du passeport, du permis de conduire) sont tombées entre les mains des escrocs, il est essentiel qu'en tant que victime vous le signaliez le plus rapidement possible à la police. Dans le cas de vol de documents d'identité, adressez-vous à Doc Stop (00800 2123 2123 ou +32 2 518 2123).

Plus d'informations : DOCSTOP - CHECKDOC

DOC STOP 24/24 00800 2123 2123 +32 2 518 2123

CARD 078 170 170 STOP 24/24

Conseils de prévention

En général

Les tentatives de fraude en ligne sont de plus en plus difficiles à repérer. Dans la plupart des formes d'escroquerie en ligne, les auteurs utilisent un modus operandi, mais il est souvent présenté de manière variable. Même au moyen de l'intelligence artificielle (IA) il est parfois difficile de discerner un message suspect.

Ces conseils de SafeOnWeb peuvent vous aider à démasquer les messages suspects :

- **Le message est-il inattendu ?**
  Vous recevez un message d'un expéditeur sans raison : vous n'avez rien acheté, vous n'avez pas eu de contact depuis longtemps, etc. Faites quelques vérifications !
- **Le message est-il urgent?**
  Gardez votre calme : connaissez-vous cet "ami dans le besoin" ? Avez-vous vraiment reçu un premier rappel de paiement ?
- **Connaissez-vous l'expéditeur ?**
  Vérifiez l'adresse e-mail, y compris les fautes d'orthographe. Mais attention : une adresse e-mail légitime n'est pas une garantie.
- **Trouvez-vous le contenu du message étrange?**
  Un organisme officiel ne vous demandera jamais votre mot de passe, vos coordonnées bancaires ou des informations personnelles par e-mail, SMS ou téléphone.
- **Où mène le lien sur lequel on vous demande de cliquer ?**
  Placez sans cliquer votre souris sur le lien. Le nom de domaine, le mot pour .be, .com, .eu, .org, … et pour le tout premier slash « / », est-il vraiment le nom de l'organisation ?
- **Le message vous-est-il adressé personnellement?**
  Les messages avec des titres généraux et vagues, doivent vous inspirer la méfiance.
- **Le message contient-il de nombreuses erreurs de langue ?**
  Même si les cybercriminels chevronnés s'expriment dans un langage correct, des erreurs de langage ou l'usage d'une langue étrangère peuvent indiquer un message suspect.
- **Le message se trouve-t-il dans votre dossier Spam/Junk ?**
  Si oui, redoublez de prudence. Vous pouvez également marquer vous-même les messages suspects comme spam ou indésirable en avertir les autres.
- **Le message tente-t-il d'aiguiser votre curiosité?**
  En prétendant : "Regarde ce que j'ai lu sur toi..." ou "Est-ce toi sur cette photo ?".

Application

Il y a aussi l'application Safeonweb**.** Cette application vous permet de recevoir des informations de manière simple et rapide concernant des cybermenaces ou escroqueries en ligne. Plus d'info: https://www.safeonweb.be/fr/safeonweb-app

Êtes-vous dans le doute? Contactez les autorités ou les organisations concernées par les voies officielles. En cas de doute, parlez-en autour de vous et reportez toujours le paiement jusqu'à ce que vous ayez une certitude totale.

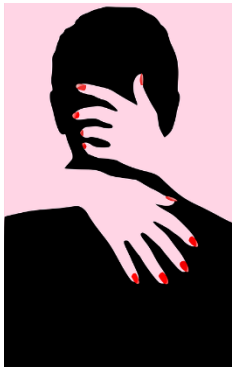
Comment réagir en cas de message suspect

De plus en plus de citoyens sont attentifs aux escroqueries en ligne et identifient les faux messages. Dans ce cas, ils peuvent être encouragés à faire ce qui suit :

- **Envoyer le message à** suspect@safeonweb.be
- Ne cliquez pas sur les liens contenus dans le courrier électronique, mais consultez le site web via un moteur de recherche.
- Ne faites pas suivre le message à vos contacts, sauf par une capture d'écran pour sensibiliser les gens.
- Ne fournissez pas de données personnelles.
- Si un escroc se fait passer pour une organisation ou une entreprise, nous vous recommandons de prévenir cette organisation. De cette façon, elle peut alerter ses clients.

Fraude à l'émotion

Contrairement à la plupart des formes d'escroquerie en ligne, la stratégie des fraudeurs de l'émotion en ligne est quelque peu différente. Elle implique une phase de recherche **:** les escrocs vont d'abord faire les recherches nécessaires notamment sur le réseau social d'une personne, afin d'obtenir suffisamment d'informations personnelles sur elle. De cette manière, ils peuvent approcher la victime de manière très crédible.



Comment reconnaître une fraude à l'amitié ?

Dans le cas de la fraude à l'amitié, les auteurs vont souvent plus loin. Ainsi, les gens investiront beaucoup plus de temps dans les messages et chats en ligne avec la victime. Ceci dans le but de créer un lien de confiance avec la victime, étant donné que ces victimes sont connues pour en avoir particulièrement besoin.

Comment reconnaître une fraude à la demande d'aide personnelle ?

En fonction du phénomène, les auteurs enquêteront sur l'environnement familial et social de la victime potentielle afin d'obtenir certains renseignements. Ces informations seront utilisées lors du contact avec la victime, pour gagner sa confiance. Par exemple : Combien a-t-elle d'enfants? Sont-ils en voyage ? Quels sont les noms des petits-enfants et des animaux domestiques ?

Conseils de prévention spécifiques contre fraude à l'émotion :

- Soyez toujours critique lorsque vous établissez des contacts en ligne et n'acceptez surtout pas de demandes de paiement sans avoir rencontré la personne dans la vie réelle (en toute sécurité).
- Si une personne proche de vous demande en ligne un transfert d'argent urgent, un appel vidéo peut être recommandé comme moyen de contrôle (si le contact physique est impossible). Pour les paiements importants, ne virez jamais rien avant d'effectuer ce contrôle, quelle que soit l'authenticité de l'appel.
- En outre, pour éviter la fraude à la demande d'aide, il peut également être recommandé de poser une question dont la réponse n'est connue que par un contact étroit. Il faut veiller à ce que ces informations ne puissent pas être trouvées sur internet. C'est souvent difficile, étant donné la quantité d'informations qui circulent sur les médias sociaux.
- Au moindre doute, ne virez aucune somme.

Pratiques locales inspirantes

Nous vous proposons quelques pratiques qui peuvent être appliquées au niveau local. Certaines de ces initiatives sont déjà lancées en Belgique.

Les cyber-volontaires ou cyber-citoyens

- Il s'agit de former et d'engager des citoyens comme volontaires pour sensibiliser d' autres citoyens vulnérables aux escroqueries en ligne. Il est souhaitable que chaque citoyen 'cyber-informé' se porte cyber-volontaire afin de partager et de communiquer les informations entre citoyens.
- La formation au cyber-volontariat peut être dispensée par les autorités locales. Une bonne coordination entre les cyber-volontaires, la zone de police et la commune est assurée, ce qui donne un point de contact et un cadre officiel aux citoyens .
- En ce qui concerne le matériel de formation, on peut se référer en premier lieu au matériel disponible et fourni par le CCB : Enseigner la cybersécurité | Centre pour la Cybersécurité Belgique (belgium.be) . En outre, vous pouvez également visiter le site web de Febelfin, votre guide . Vous pouvez également utiliser les informations fournies par la DG SP (www.besafe.be). Toutes ces informations peuvent être utilisées gratuitement lors des formations.
- Il faut encourager les jeunes à s'impliquer en tant que cyber-volontaires. Rendez cette fonction attrayante pour eux, en fonction des possibilités offertes au niveau local.
- Une fois formés, les cyber-volontaires peuvent être déployés de plusieurs façons : en étant à l'écoute des victimes, en dispensant des séances d'information dans les écoles ou associations et en exerçant une sensibilisation proactive des personnes vulnérables de la région. Cependant, il est important qu'un cadre soit établi par l'autorité locale afin de respecter certaines précautions. Ainsi, le cyber-volontaire sait quelles sont ses possibilités, mais l'autorité locale peut également agir en cas d'abus.
- Il est important que l'autorité locale puisse identifier et contacter les cyber-volontaires actifs pour sensibiliser les citoyens vulnérables.
- Il est recommandé de faire appel aux partenariats locaux de prévention (PLP) opérant dans votre commune à cet égard. Cela peut servir de base pour développer le travail avec les cyber-volontaires. Enfin il est possible de travailler avec des associations locales qui ont un intérêt à y participer.

Etablir des collaborations locales : les cyberdéfis

Chaque pouvoir local possède de nombreuses associations sur son territoire, qui peuvent bénéficier d'une cyberprévention. Tous les groupes cibles peuvent être atteints, selon l'association et l'approche.

Quelques exemples :

- une session d'infos en collaboration avec le CPAS
- sensibiliser un club de jeunes aux risques de jeux en ligne
- faire appel à un CPV (conseiller en prévention vol)
- en outre, des partenariats internes et externes peuvent être mis en place pour sensibiliser les citoyens.

Séances d'information

- Adapté aux personnes âgées et aux personnes ayant des compétences numériques limitées.
- Organisez une séance d'information sur les escroqueries en ligne dans votre collectivité locale. En même temps, cette bonne pratique assure la cohésion sociale dans la commune, car les habitants peuvent aussi apprendre à se connaître au cours de cette soirée.
- Fournir des informations accessibles qui ne nécessitent pas de connaissances techniques préalables particulières. Rendez-les accessibles à tous et aussi pratiques que possible. Ce faisant, osez également interagir avec le public. Cela vous fournira beaucoup d'informations et vous aidera à organiser les futures sessions d'information.
- En termes d'information, le matériel de formation fourni par le CCB peut être utilisé : Enseigner la cybersécurité | Centre pour la Cybersécurité Belgique (belgium.be) . En outre, vous pouvez consulter le site web de Febelfin https://www.febelfin.be/fr . Vous trouverez aussi des informations fournie par la DG SP (www.besafe.be).

Sensibilisation au marché

- Destiné aux personnes ayant des compétences numériques limitées.
- Un marché peut être une occasion idéale de toucher des personnes que les autorités locales ont du mal à atteindre par voie numérique.
- Il existe plusieurs moyens d'action pour sensibiliser les individus aux escroqueries en ligne. Dans cette optique, vous pouvez utiliser des dépliants ou brochures contenant des conseils sur la manière de reconnaître les tentatives d'escroquerie en ligne et sur ce qu'il faut faire si l'on en est victime.

Un emballage de pain ou de produits pharmaceutiques avec conseils de prévention

- Adapté aux personnes ayant des compétences numériques limitées.
- Permet d'atteindre le public cible en matière de cyberprévention en ligne. Des actions physiques, comme un sachet de pain contenant des conseils de prévention contre les escroqueries en ligne, peuvent être utiles. En s'associant avec des boulangers locaux, on peut mieux atteindre le public cible, renforcer l'économie locale et les entrepreneurs locaux peuvent également démontrer leur rôle social.
- Combinez cette action si possible avec d'autres actions afin de potentialiser la sensibilisation.

Médias éducatifs

- Adapté aux enfants et jeunes scolarisés. En effet, ils sont vulnérables et sensibles à diverses formes d'escroquerie et de violence en ligne.
- Il existe de plus en plus de jeux éducatifs sur le marché. Ces jeux peuvent également être très utiles pour sensibiliser et atteindre les jeunes, notamment en ce qui concerne les risques en ligne.
- Il est également possible de suivre des programmes à la TV éducative. Cette TV répond au style de vie des jeunes et apporte en plus un message éducatif.

Escape room

- Adapté aux jeunes et aux personnes qui sont très familiarisées avec l'internet.
- Pour aiguiser davantage leurs compétences numériques et les sensibiliser à l'impact que les risques en ligne peuvent avoir sur leur vie. Parallèlement, il convient de donner des conseils sur les points à surveiller dans le monde en ligne, sans être trop moralisateur. A cet égard, mettez toujours l'accent sur le rôle que les spectateurs (en ligne) peut jouer, faites porter la responsabilité par l'acteur et évitez de blâmer la victime.

Quiz

- Tous les groupes cibles peuvent être atteints, selon l'approche adoptée.
- Préparez un quiz permettant d'affiner les compétences numériques et de se former à la reconnaissance des e-mails frauduleux.
- Toutefois, il est également important de préciser les mesures que la personne concernée doit prendre face aux escrocs en ligne.