SOCIAL ENGINEERING / PHISHING / HACKING

(comprendre et s'en prémunir.)

version 20 Avril 2024

Le social engineering est une technique utilisée pour manipuler les gens afin d'obtenir des informations confidentielles ou d'accéder à des systèmes informatiques.

Ces méthodes sont employées par les hackers, les brouteurs, et les escrocs.

Voici quelques-unes des bases de cette pratique :

- **L'ingénierie sociale repose sur la manipulation psychologique** : Elle exploite les faiblesses humaines et les failles psychologiques telles que la curiosité, la peur, la sympathie ou la cupidité pour obtenir ce que l'attaquant désire.
- **La collecte d'informations (recherche)** : Avant de lancer une attaque, l'attaquant doit recueillir autant d'informations que possible sur la cible, y compris les détails personnels, les relations professionnelles et les habitudes en ligne.
- **La création de l'apparence de légitimité** : L'attaquant se fait passer pour quelqu'un de confiance, comme un employé, un technicien informatique ou un membre du service client, pour gagner la confiance de la victime.
- **L'utilisation de la persuasion et de la manipulation** : L'attaquant utilise des techniques de persuasion pour convaincre la victime de divulguer des informations confidentielles ou de prendre une certaine action.
- **L'utilisation de scénarios crédibles** : Les attaquants élaborent des histoires ou des scénarios crédibles pour convaincre les victimes de coopérer, en utilisant par exemple des urgences, des menaces imminentes ou des opportunités attrayantes.
- **La récolte des fruits de l'interaction** : Une fois que la victime est manipulée avec succès, l'attaquant obtient les informations ou l'accès désiré et peut les exploiter à des fins malveillantes.

LA MANIPULATION PSYCHOLOGIQUE

L'exploitation des failles humaines est au cœur de l'ingénierie sociale, car elle repose sur la manipulation des émotions, des instincts et des comportements humains pour obtenir ce que l'attaquant désire.

- **Autorité et légitimité** : Un attaquant peut se faire passer pour un employé d'une entreprise ou un représentant d'une organisation légitime. Par exemple, il peut prétendre être un technicien informatique de votre fournisseur d'accès Internet et vous contacter pour prétendre qu'il y a un problème de sécurité sur votre compte, vous demandant de fournir votre mot de passe pour "vérifier" votre compte.
- **Urgence** : L'attaquant peut créer un sentiment d'urgence pour inciter la victime à agir rapidement sans réfléchir. Par exemple, un e-mail ou un appel téléphonique peut prétendre qu'il y a eu une fraude sur le compte bancaire de la victime et qu'elle doit immédiatement fournir des informations personnelles pour éviter des conséquences graves.
- **Peur** : L'attaquant peut exploiter la peur pour inciter la victime à agir contre son intérêt. Par exemple, un e-mail pourrait prétendre que le compte en ligne de la victime a été piraté et que des photos compromettantes seront publiées en ligne si elle ne fournit pas des informations de connexion.
- **Curiosité** : Les attaquants peuvent utiliser la curiosité humaine pour inciter les gens à cliquer sur des liens malveillants ou à ouvrir des pièces jointes infectées. Par exemple, un e-mail pourrait prétendre contenir des informations "top secrètes" ou des photos compromettantes d'une célébrité pour inciter la victime à cliquer.
- **Sympathie** : L'attaquant peut se faire passer pour une personne en détresse ou dans le besoin pour susciter la sympathie de la victime et lui faire divulguer des informations ou lui fournir de l'aide. Par exemple, un e-mail pourrait prétendre être d'une organisation caritative demandant des dons pour aider les victimes d'une catastrophe naturelle, mais en réalité, il s'agit d'une arnaque pour collecter des informations financières.
- **La cupidité** : Les attaquants peuvent également exploiter la cupidité humaine en offrant des récompenses attractives ou des opportunités financières alléchantes en échange d'informations sensibles ou d'actions spécifiques. Par exemple, un e-mail frauduleux peut prétendre offrir une opportunité d'investissement lucrative, incitant ainsi la victime à divulguer des informations financières ou à effectuer un paiement.

En comprenant comment les attaquants exploitent ces émotions humaines, il devient plus facile pour les individus de reconnaître et de se protéger contre les tentatives d'ingénierie sociale.

L’autorité et la légitimité

Exemple concret d'e-mail exploitant l'autorité et la légitimité :

Objet : Notification de sécurité importante pour les utilisateurs

Cher(e) [Nom du destinataire],

Je suis [Nom de l'expéditeur], le responsable de la sécurité informatique au sein de [Nom de l'entreprise]. Je vous écris pour vous informer d'une récente mise à jour de sécurité concernant votre compte utilisateur.

Suite à une évaluation de nos systèmes de sécurité, nous avons identifié des activités suspectes potentielles liées à votre compte. Pour garantir la sécurité de nos utilisateurs et de nos systèmes, nous vous prions de bien vouloir suivre les instructions ci-dessous pour vérifier votre compte et prendre les mesures nécessaires pour protéger vos informations :

1. Connectez-vous à votre compte en utilisant le lien sécurisé fourni ci-dessous :
   [Lien vers site de phishing]
2. Vérifiez vos informations de connexion et modifiez votre mot de passe si nécessaire.
3. Assurez-vous également de mettre à jour vos informations de sécurité, telles que les questions de sécurité et les informations de récupération de compte.

Nous prenons cette mesure de précaution pour garantir la sécurité de votre compte et éviter tout accès non autorisé.

Si vous avez des questions ou des préoccupations, n'hésitez pas à me contacter directement à [adresse e-mail de l'expéditeur] ou par téléphone au [numéro de téléphone de l'expéditeur].

Je vous remercie de votre coopération.

Cordialement, [Nom de l'expéditeur] Responsable de la sécurité informatique [Nom de l'entreprise]

Dans cet exemple, l'attaquant se présente comme le responsable de la sécurité informatique d'une entreprise légitime pour établir son autorité et sa légitimité.

L'e-mail utilise un ton professionnel et des termes techniques pour renforcer cette impression d'autorité. L'attaquant demande à la victime de suivre des instructions spécifiques pour vérifier son compte, ce qui peut sembler légitime et rassurant pour la victime.

En réalité, le lien fourni redirige vers un site Web frauduleux conçu pour voler les informations d'identification de la victime.

L'urgence

Exemple concret d'e-mail exploitant l'urgence :

Objet : Action immédiate requise : Problème de sécurité critique

Cher(e) utilisateur/trice,

Nous avons détecté une activité suspecte sur votre compte. Il semble qu'une tentative d'accès non autorisé ait été effectuée récemment.

Pour protéger vos informations personnelles et sécuriser votre compte, nous vous demandons de prendre des mesures immédiates :

1. Changez immédiatement votre mot de passe en cliquant sur le lien ci-dessous :
   [Lien vers site de phishing]
2. Vérifiez vos dernières activités et signalez tout comportement inhabituel ou non autorisé.
3. Contactez notre service d'assistance si vous avez des questions ou si vous avez besoin d'aide supplémentaire.

Nous vous recommandons également de vérifier votre compte bancaire et tout autre compte en ligne lié à cette adresse e-mail pour vous assurer qu'aucune activité suspecte n'a eu lieu.

Nous prenons cette mesure d'urgence pour garantir la sécurité de votre compte et éviter tout accès non autorisé.

Nous vous remercions de votre compréhension et de votre coopération.

Cordialement, L'équipe de sécurité de [Nom de l'entreprise]

Dans cet exemple, l'e-mail utilise un ton urgent et alarmant pour inciter la victime à agir rapidement. Il prétend qu'une activité suspecte a été détectée sur le compte de la victime et l'invite à prendre des mesures immédiates pour sécuriser son compte.

Le lien fourni mène généralement vers un site Web frauduleux où les informations d'identification de la victime sont volées.

L'urgence perçue dans l'e-mail incite souvent la victime à agir impulsivement, sans prendre le temps de vérifier l'authenticité de la demande.

La peur

Voici un exemple concret d'e-mail exploitant la peur :

Objet : Urgent : Action requise pour éviter la suspension de votre compte

Cher(e) client(e),

Nous avons détecté des activités suspectes sur votre compte. Pour protéger votre sécurité et vos informations personnelles, nous sommes contraints de suspendre temporairement votre compte si aucune action n'est entreprise immédiatement.

Pour éviter la suspension de votre compte, veuillez cliquer sur le lien ci-dessous pour confirmer votre identité et restaurer l'accès à votre compte : **[Lien vers site de phishing]**

Si aucune action n'est entreprise dans les 24 heures, votre compte sera suspendu et toutes les informations associées seront supprimées de manière permanente.

Nous vous remercions de votre coopération et de votre compréhension.

Cordialement, L'équipe de sécurité de [Nom de l'entreprise]

Dans cet exemple, l'e-mail joue sur la peur de la victime en lui indiquant qu'il y a eu des activités suspectes sur son compte et que des mesures drastiques seront prises si elle ne prend pas immédiatement des mesures.

L'e-mail incite ainsi la victime à agir rapidement, sans réfléchir, par peur de perdre l'accès à son compte ou de voir ses informations personnelles compromises.

Le lien fourni redirige en réalité vers un site Web frauduleux conçu pour voler les informations d'identification de la victime.

La curiosité

Exemple concret d'e-mail exploitant la curiosité :

Objet : Invitation à une présentation exclusive sur les tendances du marché

Cher(e) [Nom de la victime],

Nous avons le plaisir de vous inviter à une présentation exclusive sur les tendances actuelles du marché dans votre secteur d'activité. Cette présentation sera animée par des experts de l'industrie et fournira des insights précieux sur les dernières évolutions, les opportunités émergentes et les défis à venir.

En tant que leader dans votre domaine, votre expertise et votre perspective sont précieuses, et nous serions honorés de compter sur votre participation à cet événement exclusif. Cette présentation vous offrira une occasion unique d'enrichir vos connaissances, d'échanger des idées avec vos pairs et de découvrir des stratégies innovantes pour stimuler la croissance de votre entreprise.

La présentation aura lieu le [date] à [heure] et se déroulera en ligne via une plateforme sécurisée. Pour confirmer votre participation et recevoir les détails de connexion, veuillez cliquer sur ce lien de réservation avant le [date] **[Lien vers site de phishing]**

Nous sommes impatients de vous accueillir à cet événement exceptionnel et de partager des informations précieuses qui pourraient avoir un impact significatif sur votre entreprise.

Cordialement,

[L'expéditeur]

Cet e-mail exploite la curiosité professionnelle en offrant à la victime l'opportunité d'assister à une présentation exclusive sur les tendances du marché dans son secteur d'activité.

En mettant en avant l'expertise et la perspective de la victime et en soulignant les bénéfices potentiels de sa participation, l'e-mail incite la victime à répondre pour confirmer sa présence et à s'engager dans cet événement professionnel.

La sympathie

Exemple concret d'e-mail exploitant la sympathie :

Objet : Demande de soutien pour une cause importante

Cher(e) [Nom du destinataire],

Je m'adresse à vous aujourd'hui avec le cœur lourd, mais rempli d'espoir pour un avenir meilleur. En tant que membre de notre communauté, je voudrais attirer votre attention sur une situation critique qui touche de nombreuses familles dans le besoin.

Récemment, j'ai eu l'occasion de visiter un centre d'accueil pour les sans-abri dans notre ville. Ce que j'ai vu là-bas m'a profondément touché. Des hommes, des femmes et même des enfants luttaient pour leur survie, confrontés au froid glacial de l'hiver sans abri ni nourriture suffisante.

C'est dans ce contexte que je me permets de solliciter votre aide. Ensemble, nous pouvons faire une différence significative dans la vie de ces personnes vulnérables. Votre contribution, qu'elle soit financière, en nature ou sous forme de bénévolat, peut apporter un peu de chaleur et d'espoir à ceux qui en ont le plus besoin.

Je comprends que nous traversons tous des périodes difficiles, mais même la plus petite contribution peut avoir un impact énorme sur la vie de quelqu'un. Si vous souhaitez en savoir plus sur la manière dont vous pouvez aider ou si vous avez des questions, n'hésitez pas à cliquer sur le lien suivant : **[Lien vers site de phishing]**

Merci d'avance pour votre générosité et votre compassion. Ensemble, nous pouvons faire une différence.

Avec gratitude, [Votre nom]

Dans cet exemple, l'e-mail exploite la sympathie en évoquant une cause noble et en encourageant le destinataire à contribuer à une solution. L'appel à l'action est centré sur le bien-être des personnes dans le besoin, ce qui vise à susciter de l'empathie et à inciter le destinataire à agir pour aider.

Ce type d'e-mail est souvent utilisé dans le cadre de campagnes de collecte de fonds légitimes pour des organisations caritatives ou des initiatives communautaires mais également en vue d’un phishing.

La cupidité

Exemple concret d'e-mail exploitant la cupidité :

Objet : Opportunité d'investissement lucrative

Cher(e) [Nom de la victime],

Je me permets de vous contacter car j'ai récemment découvert une opportunité d'investissement exceptionnelle qui pourrait vous intéresser.

Il s'agit d'un projet novateur dans le domaine de la technologie financière qui promet des rendements extrêmement élevés en un laps de temps très court. Nos investisseurs initiaux ont déjà réalisé des bénéfices impressionnants et nous cherchons à étendre nos activités en accueillant de nouveaux partenaires.

En tant que destinataire de cet e-mail, vous avez été spécifiquement sélectionné(e) pour participer à cette opportunité exclusive. Nous offrons des conditions spéciales aux premiers investisseurs, y compris des bonus de parrainage pour chaque nouvel investisseur que vous référez à notre programme.

Pour en savoir plus sur cette opportunité et commencer à investir dès maintenant, veuillez répondre à cet e-mail ou me contacter directement au **[numéro de téléphone]** ou en suivant ce lien :

[Lien vers site de phishing]

N'attendez pas trop longtemps, car les places sont limitées et cette offre pourrait ne pas durer longtemps.

Je suis impatient(e) de vous accueillir dans notre communauté d'investisseurs.

Cordialement,

[Prénom] [Nom]

[Poste]

[Entreprise]

Cet e-mail exploite la cupidité en offrant à la victime une opportunité d'investissement très lucrative avec des rendements élevés et des conditions spéciales réservées aux premiers investisseurs.

En incitant la victime à agir rapidement pour ne pas rater cette "opportunité exclusive", l'attaquant espère exploiter le désir de profit de la victime pour obtenir une réponse rapide et éventuellement des fonds d'investissement.

LA COLLECTE D'INFORMATIONS

La collecte d'informations est une étape cruciale de l'ingénierie sociale, car elle permet à l'attaquant de personnaliser son approche et d'augmenter ses chances de succès. Voici quelques exemples concrets de la manière dont les attaquants peuvent collecter des informations sur leurs cibles :

1. **Sur les réseaux sociaux** : Les réseaux sociaux sont une mine d'informations pour les attaquants. En consultant les profils publics des individus sur des plateformes comme Facebook, LinkedIn ou Twitter, un attaquant peut recueillir des informations telles que le lieu de travail, les relations, les centres d'intérêt, les dates importantes (comme les anniversaires), etc. Ces informations peuvent être utilisées pour personnaliser des attaques, telles que des e-mails d'hameçonnage.
2. **Par l'intermédiaire de sites Web publics** : Les attaquants peuvent rechercher des informations sur les sites Web publics tels que les annuaires d'entreprises, les forums de discussion ou les blogs. Ces sources peuvent fournir des détails sur les employés d'une entreprise, leurs fonctions, leurs adresses e-mail et parfois même des informations sensibles telles que des identifiants d'accès ou des mots de passe mal protégés.
3. **À travers l'ingénierie sociale indirecte** : Les attaquants peuvent également collecter des informations en se faisant passer pour quelqu'un d'autre. Par exemple, un attaquant pourrait appeler le service client d'une entreprise en se faisant passer pour un employé légitime et poser des questions sur les politiques internes ou les procédures de sécurité, tout en obtenant subtilement des informations sur la manière dont l'entreprise fonctionne.
4. **Par le biais de techniques d'ingénierie sociale directe** : Les attaquants peuvent contacter directement les individus sous divers prétextes pour obtenir des informations. Par exemple, un appel téléphonique ou un e-mail prétendant être un sondage d'opinion ou une enquête de satisfaction peut être utilisé pour obtenir des détails personnels ou professionnels.
5. **En utilisant des techniques de phishing** : Les attaquants peuvent envoyer des e-mails ou des messages texte frauduleux contenant des liens malveillants ou des pièces jointes infectées. Lorsque la victime interagit avec ces éléments, l'attaquant peut recueillir des informations sensibles, tels que des identifiants de connexion ou des informations financières.

En combinant ces différentes méthodes, les attaquants peuvent rassembler une quantité significative d'informations sur leurs cibles, ce qui leur permet de personnaliser leurs attaques et d'augmenter leurs chances de succès lors de la phase d'exécution.

C'est pourquoi il est crucial pour les individus et les organisations de limiter la quantité d'informations personnelles accessibles publiquement et de sensibiliser les utilisateurs aux risques potentiels de divulgation d'informations en ligne.

LA CRÉATION DE L'APPARENCE DE LÉGITIMITÉ

La création de l'apparence de légitimité est une stratégie clé en ingénierie sociale. Elle consiste à donner l'impression que l'attaque ou la demande est légitime et provient d'une source fiable ou autorisée. Voici quelques exemples concrets de cette stratégie :

1. **Faux sites Web ou e-mails de phishing** : Les attaquants créent souvent des sites Web ou envoient des e-mails qui imitent parfaitement l'apparence et le langage des sites légitimes, tels que des banques, des plateformes de médias sociaux ou des fournisseurs de services en ligne. Par exemple, un e-mail de phishing prétendant provenir de votre banque peut contenir un lien vers une page de connexion frauduleuse qui ressemble exactement à celle de votre banque, mais qui est contrôlée par l'attaquant.
2. **Utilisation de noms et de titres professionnels crédibles** : Les attaquants se présentent souvent avec des noms et des titres professionnels qui semblent crédibles et légitimes. Par exemple, lors d'un appel téléphonique, un attaquant peut prétendre être un responsable du service client ou un agent de police pour gagner la confiance de la victime.
3. **Manipulation de la confiance** : Les attaquants exploitent parfois les relations de confiance existantes pour tromper les victimes. Par exemple, un attaquant peut se faire passer pour un collègue, un ami ou un membre de la famille de la victime et prétendre avoir besoin d'informations confidentielles pour une raison légitime.
4. **Faux documents et identifiants** : Les attaquants peuvent créer de faux documents ou des identifiants qui semblent officiels pour renforcer leur crédibilité. Par exemple, un attaquant peut fournir une fausse carte d'identification ou un badge d'employé lors d'une visite en personne pour donner l'impression d'être un membre autorisé du personnel.
5. **Utilisation de logos et de marques familières** : Les attaquants utilisent souvent des logos et des marques bien connus pour donner l'impression de légitimité. Par exemple, un e-mail de phishing peut contenir des logos d'entreprises célèbres pour induire en erreur les destinataires et les inciter à fournir des informations sensibles.

En utilisant ces tactiques, les attaquants peuvent créer une apparence de légitimité qui trompe souvent les victimes et les incite à coopérer involontairement.

C'est pourquoi il est important pour les individus et les organisations de rester vigilants et de vérifier attentivement l'authenticité des demandes d'information ou d'accès avant de partager des informations sensibles.

L’UTILISATION

DE SCÉNARIOS CRÉDIBLES

La création de scénarios crédibles est une stratégie essentielle en ingénierie sociale, car elle implique de concevoir des histoires ou des situations qui semblent plausibles et convaincantes pour les victimes ciblées. (voir en annexes quelques scénarios développés point par point)

Voici quelques exemples concrets de cette stratégie :

1. **Faux appels de support technique** : Un attaquant peut appeler une victime en se faisant passer pour un technicien du support technique d'une entreprise bien connue, prétendant qu'il y a un problème avec l'ordinateur ou le compte de la victime. L'attaquant peut alors guider la victime à travers des étapes pour donner accès à distance à l'ordinateur ou pour divulguer des informations d'identification sensibles.
2. **Scénarios de fraude financière** : Un attaquant peut appeler ou envoyer un e-mail à une victime en se faisant passer pour un représentant de la banque de la victime, prétendant qu'il y a eu des activités suspectes sur le compte bancaire de la victime et demandant des informations d'identification ou de carte bancaire pour "vérifier" le compte.
3. **Faux concours ou offres spéciales** : Un attaquant peut envoyer un e-mail à une victime prétendant qu'elle a gagné un prix dans un concours auquel elle n'a jamais participé. Pour réclamer le prix, la victime doit fournir des informations personnelles telles que son nom, son adresse et son numéro de téléphone, ce qui peut ensuite être utilisé à des fins frauduleuses.
4. **Scénarios d'urgence médicale ou familiale** : Un attaquant peut envoyer un e-mail ou un message texte à une victime prétendant être un ami ou un membre de la famille en difficulté. L'attaquant peut prétendre avoir eu un accident ou être tombé malade à l'étranger et demander de l'argent pour l'aide médicale ou pour rentrer chez lui.
5. **Faux messages d'alerte de sécurité** : Un attaquant peut envoyer un e-mail ou un message texte à une victime prétendant être une entreprise ou une organisation gouvernementale, prétendant qu'il y a une urgence de sécurité, comme une violation de données ou une menace terroriste imminente. La victime peut alors être incitée à cliquer sur un lien malveillant ou à fournir des informations personnelles pour "vérifier" son identité.
6. **Faux appels de recrutement professionnel** : Un attaquant peut appeler une victime en se faisant passer pour un recruteur d'une entreprise renommée, prétendant avoir trouvé le CV de la victime en ligne et lui offrant une opportunité d'emploi irrésistible. L'attaquant peut ensuite demander des informations personnelles telles que l'historique de travail ou les références.
7. **Messages de vérification de compte** : Un attaquant peut envoyer un e-mail ou un message texte à une victime prétendant être d'une plateforme en ligne populaire, comme un service de messagerie ou un réseau social, affirmant qu'il y a eu une activité suspecte sur le compte de la victime et demandant de vérifier son identité en cliquant sur un lien fourni.

8. **Faux appels de soutien technique pour les appareils électroniques** : Un attaquant peut appeler une victime en se faisant passer pour un représentant du fabricant d'appareils électroniques, prétendant qu'il y a un problème avec l'appareil de la victime et offrant une assistance technique gratuite. L'attaquant peut ensuite guider la victime à travers des étapes pour obtenir un accès à distance à l'appareil.
9. **Scénarios de fausse détresse financière** : Un attaquant peut envoyer un e-mail ou un message à une victime prétendant être un ami ou un membre de la famille en difficulté financière, demandant de l'argent pour payer des factures médicales ou des frais d'urgence. L'attaquant peut utiliser des détails personnels pour rendre le scénario plus crédible.
10. **Faux appels de service client pour les services en ligne** : Un attaquant peut appeler une victime en se faisant passer pour un représentant du service client d'un fournisseur de services en ligne, comme une plateforme de streaming vidéo ou un service de messagerie, prétendant qu'il y a un problème avec le compte de la victime et demandant des informations d'identification pour résoudre le problème.
11. **Faux appels de réclamation de loterie ou de prix** : Un attaquant peut appeler une victime prétendant être un représentant d'une société de loterie ou d'un concours, affirmant que la victime a gagné un prix important. L'attaquant peut demander à la victime de payer des frais de traitement ou de fournir des informations personnelles pour recevoir le prix.
12. **Scénarios de fausse identité pour la livraison de colis** : Un attaquant peut envoyer un e-mail ou un message texte à une victime prétendant être une société de livraison bien connue, comme UPS ou FedEx, affirmant qu'il y a un problème avec la livraison d'un colis à la victime. L'attaquant peut demander des informations d'identification ou de paiement pour résoudre le prétendu problème de livraison.
13. **Faux appels de collecte de fonds pour des causes humanitaires** : Un attaquant peut appeler une victime prétendant être un représentant d'une organisation caritative réputée, affirmant qu'elle collecte des fonds pour une cause humanitaire urgente, comme l'aide aux victimes d'une catastrophe naturelle. L'attaquant peut alors demander à la victime de faire un don par téléphone ou en ligne.
14. **Scénarios de fausse enquête de satisfaction client** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise avec laquelle la victime a récemment fait des affaires, affirmant qu'elle mène une enquête de satisfaction client et offrant un cadeau ou un bon de réduction en échange de la participation à l'enquête. L'attaquant peut ensuite demander des informations personnelles ou de compte sous prétexte de traitement de l'enquête.
15. **Faux appels de support technique pour les logiciels malveillants** : Un attaquant peut appeler une victime prétendant être un technicien informatique du service de sécurité de l'ordinateur de la victime, affirmant que l'ordinateur de la victime est infecté par des logiciels malveillants et offrant une assistance pour nettoyer l'ordinateur. L'attaquant peut ensuite demander à la victime de télécharger un logiciel malveillant sous prétexte de protection contre les menaces.

16. **Scénarios de fausse offre d'emploi à domicile** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise offrant une opportunité d'emploi à domicile, affirmant que la victime peut gagner de l'argent en travaillant à distance. L'attaquant peut demander à la victime de fournir des informations personnelles ou bancaires sous prétexte de traitement de la candidature.

17. **Faux appels de prétendus membres de la famille en détresse** : Un attaquant peut appeler une victime prétendant être un membre de la famille en voyage à l'étranger, affirmant qu'il a été victime d'un accident ou d'un vol et demandant de l'argent pour l'aide médicale ou pour rentrer chez lui. L'attaquant peut utiliser des détails personnels pour rendre le scénario plus crédible.

18. **Scénarios de fausse vérification d'identité pour les services financiers** : Un attaquant peut envoyer un e-mail à une victime prétendant être une institution financière, affirmant qu'il y a eu une activité suspecte sur le compte de la victime et demandant de vérifier son identité en fournissant des informations d'identification ou en cliquant sur un lien fourni.

19. **Faux appels de prétexte de vérification de la propriété** : Un attaquant peut appeler une victime prétendant être un agent immobilier ou un représentant d'une agence de location, affirmant qu'il y a un problème avec la propriété de la victime et demandant des informations personnelles ou financières pour vérifier la propriété.

20. **Scénarios de fausse menace de poursuites judiciaires** : Un attaquant peut envoyer un e-mail à une victime prétendant être un avocat représentant une entreprise ou une organisation, affirmant qu'il y a eu une violation du contrat ou une infraction à la loi et menaçant des poursuites judiciaires à moins que la victime ne paie des frais ou ne fournisse des informations pour régler le problème.:

21. **Faux appels de support technique pour les réseaux sociaux** : Un attaquant peut appeler une victime prétendant être un représentant du support technique d'une plateforme de médias sociaux populaire, affirmant qu'il y a un problème avec le compte de la victime et demandant des informations d'identification ou de connexion pour résoudre le problème.

22. **Scénarios de fausse demande d'assistance technique en ligne** : Un attaquant peut envoyer un e-mail à une victime prétendant être un utilisateur rencontrant des problèmes avec un logiciel ou un service en ligne, affirmant que la victime peut aider en fournissant un accès à distance à son ordinateur pour résoudre les problèmes.

23. **Faux appels de soutien technique pour les services de télécommunications** : Un attaquant peut appeler une victime prétendant être un technicien d'une société de télécommunications, affirmant qu'il y a un problème avec le service Internet ou téléphonique de la victime et demandant des informations d'identification ou de paiement pour résoudre le problème.

24. **Scénarios de fausse demande de mise à jour de logiciel** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise de logiciels, affirmant qu'une mise à jour critique est disponible pour un logiciel utilisé par la victime et demandant à celle-ci de télécharger un fichier malveillant sous prétexte de sécurité.

25. **Faux appels de réclamation de remboursement d'impôt** : Un attaquant peut appeler une victime prétendant être un représentant de l'IRS ou d'une autre autorité fiscale, affirmant qu'il y a une erreur dans le remboursement d'impôt de la victime et demandant des informations d'identification ou de compte pour corriger le problème.

26. **Scénarios de fausse demande de vérification de compte bancaire** : Un attaquant peut envoyer un e-mail à une victime prétendant être sa banque, affirmant qu'il y a eu une activité suspecte sur le compte de la victime et demandant de vérifier son identité en fournissant des informations d'identification ou en cliquant sur un lien fourni.

27. **Faux appels de demande de confirmation de commande** : Un attaquant peut appeler une victime prétendant être un représentant d'une entreprise de vente en ligne, affirmant qu'il y a une erreur dans une commande récente de la victime et demandant des informations de paiement ou de livraison pour corriger le problème.

28. **Scénarios de fausse demande de sondage en ligne** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise offrant des récompenses pour la participation à un sondage en ligne, affirmant que la victime peut gagner des prix attractifs en répondant à quelques questions simples et demandant des informations personnelles ou financières pour participer au sondage.

29. **Faux appels de demande de soutien pour une fausse cause caritative** : Un attaquant peut appeler une victime prétendant être un représentant d'une organisation caritative, affirmant qu'elle collecte des fonds pour une cause humanitaire ou environnementale urgente et demandant des dons par téléphone ou en ligne.

30. **Scénarios de fausse demande de vérification d'identité pour un concours en ligne** : Un attaquant peut envoyer un e-mail à une victime prétendant être un organisateur d'un concours en ligne, affirmant que la victime a gagné un prix et demandant de vérifier son identité en fournissant des informations d'identification ou en téléchargeant des documents personnels.

31. **Faux appels de demande de confirmation de données personnelles pour des services gouvernementaux** : Un attaquant peut appeler une victime prétendant être un représentant d'une agence gouvernementale, affirmant qu'il y a un problème avec les données personnelles de la victime et demandant des informations d'identification pour mettre à jour les dossiers gouvernementaux.

32. **Scénarios de fausse demande de soutien pour une campagne politique** : Un attaquant peut envoyer un e-mail à une victime prétendant être un représentant d'un parti politique, affirmant qu'il collecte des fonds pour une campagne électorale importante et demandant des dons par téléphone ou en ligne.Bien sûr, voici 20 autres exemples de création de scénarios crédibles en ingénierie sociale :

33. **Faux appels de vérification de données pour des enquêtes de marché** : Un attaquant peut appeler une victime prétendant être un enquêteur pour une société de recherche en marketing, affirmant qu'il mène une enquête sur les habitudes de consommation et demandant des informations personnelles ou financières pour la recherche.

34. **Scénarios de fausse offre d'assistance technique pour les services de streaming** : Un attaquant peut envoyer un e-mail à une victime prétendant être un représentant d'une plateforme de streaming vidéo populaire, affirmant qu'il y a un problème avec le compte de la victime et demandant des informations d'identification ou de paiement pour résoudre le problème.

35. **Faux appels de demande de confirmation de réservation d'hôtel** : Un attaquant peut appeler une victime prétendant être un employé d'un hôtel, affirmant qu'il y a un problème avec la réservation de la victime et demandant des informations de carte de crédit ou de confirmation pour corriger le problème.

36. **Scénarios de fausse demande de participation à un programme de récompenses** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise offrant des récompenses pour la participation à un programme de fidélité, affirmant que la victime peut gagner des points ou des cadeaux en s'inscrivant au programme et demandant des informations personnelles pour l'inscription.

37. **Faux appels de demande de mise à jour de données d'inscription** : Un attaquant peut appeler une victime prétendant être un représentant d'une association professionnelle ou d'un club, affirmant qu'il y a un problème avec les données d'inscription de la victime et demandant des informations personnelles pour mettre à jour les dossiers.

38. **Scénarios de fausse demande de vérification de compte pour des services de voyage** : Un attaquant peut envoyer un e-mail à une victime prétendant être une agence de voyage en ligne, affirmant qu'il y a eu une activité suspecte sur le compte de la victime et demandant de vérifier son identité en fournissant des informations d'identification ou en cliquant sur un lien fourni.

39. **Faux appels de demande de confirmation de participation à un événement** : Un attaquant peut appeler une victime prétendant être un organisateur d'un événement, affirmant que la victime est inscrite à l'événement et demandant des informations de paiement ou de confirmation pour confirmer la participation.

40. **Scénarios de fausse offre de partenariat commercial** : Un attaquant peut envoyer un e-mail à une victime prétendant être un entrepreneur ou un investisseur, affirmant qu'il est intéressé par un partenariat commercial avec la victime et demandant des informations financières ou commerciales pour discuter des détails du partenariat.

41. **Faux appels de demande de vérification d'identité pour des services de crédit** : Un attaquant peut appeler une victime prétendant être un représentant d'une agence de crédit, affirmant qu'il y a un problème avec le dossier de crédit de la victime et demandant des informations d'identification pour vérifier son identité.

42. **Scénarios de fausse demande de confirmation de commande en ligne** : Un attaquant peut envoyer un e-mail à une victime prétendant être un vendeur en ligne, affirmant qu'il y a une erreur dans une commande récente de la victime et demandant des informations de paiement ou de livraison pour corriger le problème.

43. **Faux appels de demande de confirmation de rendez-vous médical** : Un attaquant peut appeler une victime prétendant être un représentant d'un cabinet médical, affirmant qu'il y a un problème avec le rendez-vous de la victime et demandant des informations d'identification ou de confirmation pour résoudre le problème.

44. **Scénarios de fausse demande de participation à un programme de test de produit** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise de produits de consommation, affirmant qu'elle offre la possibilité de tester gratuitement un nouveau produit et demandant des informations personnelles pour l'inscription au programme de test.

45. **Faux appels de demande de confirmation de participation à un sondage politique** : Un attaquant peut appeler une victime prétendant être un représentant d'un institut de sondage, affirmant qu'il mène une enquête politique et demandant des informations personnelles ou politiques pour la participation au sondage.

46. **Scénarios de fausse offre d'adhésion à un club exclusif** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise offrant une adhésion gratuite à un club exclusif, affirmant que la victime a été sélectionnée pour bénéficier d'avantages spéciaux et demandant des informations personnelles pour l'inscription au club.

47. **Faux appels de demande de confirmation de commande de produits pharmaceutiques** : Un attaquant peut appeler une victime prétendant être un représentant d'une pharmacie en ligne, affirmant qu'il y a une erreur dans une commande de médicaments de la victime et demandant des informations de paiement ou de livraison pour corriger le problème.

48. **Scénarios de fausse demande de participation à un programme de parrainage** : Un attaquant peut envoyer un e-mail à une victime prétendant être une entreprise offrant des récompenses pour la participation à un programme de parrainage, affirmant que la victime peut gagner des récompenses en recommandant des amis ou des collègues et demandant des informations personnelles pour l'inscription au programme.

49. **Faux appels de demande de confirmation de réservation de vol** : Un attaquant peut appeler une victime prétendant être un employé d'une compagnie aérienne, affirmant qu'il y a un problème avec la réservation de vol de la victime et demandant des informations de carte de crédit.

50.… l’imagination des brouteurs et des hackers est infinie.

LA RÉCOLTE
DES FRUITS DE L'INTERACTION

La récolte des fruits de l'interaction fait référence à la phase où l'attaquant exploite les informations et la confiance gagnées au cours de l'interaction avec la victime pour atteindre ses objectifs, que ce soit en recueillant des données sensibles, en incitant la victime à prendre des mesures indésirables ou en poursuivant d'autres formes d'exploitation.

Voici quelques exemples concrets de cette stratégie :

1. **Vol d'informations d'identification** : Après avoir établi une relation de confiance avec la victime, l'attaquant peut demander des informations d'identification sous prétexte de vérifier un compte ou de résoudre un problème. Ces informations peuvent inclure des noms d'utilisateur, des mots de passe, des numéros de carte de crédit ou d'autres données sensibles.

2. **Installation de logiciels malveillants** : En utilisant des techniques de persuasion, l'attaquant peut convaincre la victime de télécharger et d'exécuter un logiciel malveillant sous prétexte de résoudre un problème technique ou d'accéder à une offre spéciale. Une fois installé, le logiciel malveillant peut être utilisé pour voler des informations, prendre le contrôle de l'ordinateur de la victime ou mener d'autres activités nuisibles.

3. **Fraude financière** : Après avoir gagné la confiance de la victime, l'attaquant peut l'inciter à effectuer des transactions financières indésirables, telles que des paiements pour des produits ou des services fictifs, des dons à des organisations frauduleuses ou des transferts d'argent vers des comptes contrôlés par l'attaquant.

4. **Phishing continu** : En utilisant les informations collectées lors des interactions précédentes, l'attaquant peut personnaliser davantage ses attaques de phishing pour sembler plus crédibles et persuader la victime de fournir encore plus d'informations sensibles ou de prendre des mesures indésirables.

5. **Escroqueries basées sur la confiance** : Ayant établi une relation de confiance avec la victime, l'attaquant peut exploiter cette confiance pour proposer des offres d'investissement frauduleuses, des opportunités commerciales douteuses ou d'autres arnaques qui incitent la victime à perdre de l'argent ou à divulguer des informations sensibles.

6. **Chantage et extorsion** : En utilisant les informations sensibles recueillies auparavant, l'attaquant peut menacer de divulguer des données compromettantes ou de nuire à la réputation de la victime à moins qu'elle ne paie une rançon ou ne se soumette à d'autres demandes.

7. **Ingénierie sociale ciblée** : En se basant sur les interactions précédentes, l'attaquant peut ajuster sa stratégie d'ingénierie sociale pour cibler des objectifs spécifiques, tels que d'autres employés d'une organisation, des membres de la famille de la victime ou des contacts professionnels.

8. **Propagation de la désinformation** : En utilisant les informations recueillies sur les préférences, les opinions ou les habitudes de la victime, l'attaquant peut diffuser de fausses informations via des réseaux sociaux, des forums en ligne ou d'autres plateformes pour semer la confusion, influencer les perceptions ou manipuler les comportements.

QUOI FAIRE POUR SE PRÉMUNIR ?

Pour éviter le phishing téléphonique et par e-mail, voici quelques bonnes pratiques et choses à vérifier :

Phishing par téléphone :

1. **Soyez méfiant envers les appels non sollicités** : Ne donnez jamais d'informations personnelles ou confidentielles lors d'un appel téléphonique non sollicité, même si l'appelant prétend être d'une entreprise légitime.
2. **Vérifiez l'identité de l'appelant** : Si quelqu'un vous demande des informations sensibles au téléphone, demandez-lui des détails sur son identité et l'entreprise qu'il représente. Vérifiez ensuite cette information en contactant directement l'entreprise via un numéro de téléphone vérifié.
3. **Ne cédez pas à la pression** : Méfiez-vous des appelants qui tentent de vous presser de prendre des décisions rapides ou qui vous menacent de conséquences négatives si vous refusez de coopérer. Prenez le temps de vérifier les informations avant de prendre toute action.

Phishing par e-mail :

1. **Vérifiez l'adresse de l'expéditeur** : Vérifiez attentivement l'adresse e-mail de l'expéditeur pour vous assurer qu'elle correspond exactement à celle d'une entreprise légitime. Méfiez-vous des adresses e-mail avec des orthographes incorrectes ou des extensions de domaine inhabituelles.
2. **Méfiez-vous des liens et des pièces jointes** : Ne cliquez jamais sur des liens ou ne téléchargez pas de pièces jointes provenant d'e-mails suspects ou non sollicités. Si vous devez vérifier un lien, survolez-le avec votre souris pour afficher l'URL réelle avant de cliquer.
3. **Vérifiez la qualité du contenu** : Méfiez-vous des e-mails contenant des erreurs grammaticales ou typographiques, une formulation peu professionnelle ou des demandes inhabituelles, telles que la fourniture d'informations personnelles ou le transfert d'argent.
4. **Vérifiez les demandes d'urgence** : Soyez prudent avec les e-mails qui vous pressent de prendre des mesures immédiates, en particulier ceux qui prétendent être des urgences financières ou des menaces de suspension de compte. Prenez le temps de vérifier l'authenticité de la demande.
5. **Utilisez des solutions de sécurité** : Utilisez un logiciel antivirus et un filtre anti-spam pour détecter et bloquer les e-mails de phishing avant qu'ils n'atteignent votre boîte de réception. Mettez régulièrement à jour vos logiciels de sécurité pour bénéficier des dernières protections.

En suivant ces bonnes pratiques et en restant vigilants face aux tentatives de phishing téléphonique et par e-mail, vous pouvez réduire considérablement votre risque de devenir une victime d'ingénierie sociale.

GLOSSAIRE :

1. **Autorité et légitimité** : L'utilisation de noms, titres ou logos de personnes ou d'organisations légitimes pour donner l'apparence de validité à une demande ou à une communication, souvent utilisée dans les attaques de phishing.
2. **Brouteur :** Un "brouteur" est un terme utilisé pour désigner une personne ou un groupe de personnes qui pratique l'arnaque sur internet, généralement dans le but de tromper des individus pour obtenir de l'argent ou des informations personnelles. Le terme "brouteur" est souvent associé aux fraudes nigérianes ou à d'autres formes d'escroqueries en ligne, mais il peut également faire référence à d'autres types d'activités frauduleuses sur internet.
3. **Curiosité** : L'intérêt naturel pour la découverte ou la connaissance, souvent exploité dans les attaques d'ingénierie sociale pour inciter les victimes à répondre à des e-mails ou à cliquer sur des liens malveillants.
4. **Cupidité** : L'avidité ou le désir excessif de gains matériels ou financiers, souvent exploité dans les attaques d'ingénierie sociale pour inciter les victimes à prendre des mesures indésirables.
5. **Ingénierie sociale ou social engineering** : La manipulation psychologique des individus pour les inciter à divulguer des informations confidentielles ou à effectuer des actions indésirables.
6. **Manipulation** : L'utilisation de techniques trompeuses ou manipulatrices pour influencer les pensées, les émotions ou les comportements des individus dans le but d'obtenir un avantage personnel.
7. **Persuasion** : L'utilisation de tactiques de communication et d'influence pour convaincre les individus d'adopter une opinion, de prendre une décision ou d'agir d'une certaine manière.
8. **Peur** : L'exploitation des émotions négatives, telles que la peur ou l'anxiété, pour inciter les victimes à agir impulsivement ou à divulguer des informations par crainte de conséquences négatives.
9. **Phishing** : Une forme d'attaque par e-mail où les fraudeurs se font passer pour des entités légitimes afin de tromper les utilisateurs et de leur soutirer des informations personnelles ou financières.
10. **Récolte des fruits de l'interaction** : La phase où l'attaquant exploite les informations et la confiance gagnées au cours de l'interaction avec la victime pour atteindre ses objectifs, dans le cadre d'une attaque d'ingénierie sociale.
11. **Scénarios crédibles** : Des récits ou des situations plausibles qui donnent l'apparence de légitimité à une demande ou à une communication dans le cadre d'une attaque d'ingénierie sociale.
12. **Sympathie** : L'exploitation des émotions positives, telles que la sympathie ou la compassion, pour inciter les victimes à coopérer ou à fournir des informations sensibles.
13. **Urgence** : L'utilisation de délais serrés ou de menaces de conséquences négatives imminentes pour inciter les victimes à agir rapidement sans réfléchir, souvent utilisée dans les attaques d'ingénierie sociale.

Annexes Scénarios :

Scénario "Le faux recrutement"

Description du scénario : *Dans ce scénario, un individu malveillant se fait passer pour un recruteur d'une entreprise réputée. Il cible des professionnels sur des plateformes professionnelles telles que LinkedIn, où il peut accéder à des informations détaillées sur leur expérience, leurs compétences et leur historique professionnel. L'attaquant utilise ces informations pour personnaliser ses approches et rendre ses offres d'emploi plus convaincantes.*

1. **L'approche initiale** : L'attaquant envoie des messages privés aux professionnels ciblés, se présentant comme un recruteur travaillant pour une entreprise prestigieuse. Il complimente souvent le profil de la victime et exprime son intérêt pour ses compétences spécifiques. Cette approche amicale vise à établir une relation de confiance dès le début.
2. **La proposition d'opportunités d'emploi attrayantes** : Une fois qu'une conversation est établie, l'attaquant propose des opportunités d'emploi très attrayantes, telles que des postes de direction ou des missions stimulantes avec des salaires compétitifs. Il met en avant des avantages supplémentaires tels que des avantages sociaux généreux, des opportunités de croissance professionnelle et des horaires de travail flexibles pour rendre l'offre encore plus alléchante.
3. **L'organisation d'entretiens téléphoniques ou vidéo** : Pour donner plus de crédibilité à ses offres, l'attaquant organise des entretiens téléphoniques ou vidéo avec les victimes potentielles. Pendant ces entretiens, il se fait passer pour un professionnel expérimenté et pose des questions détaillées sur l'expérience et les compétences de la victime pour paraître légitime.
4. **La demande d'informations sensibles** : Pendant l'entretien, l'attaquant peut demander des informations sensibles telles que des numéros de sécurité sociale, des références professionnelles ou des informations bancaires sous prétexte de vérifications d'antécédents ou de traitement des candidatures. Ces demandes semblent légitimes dans le contexte d'un processus de recrutement, mais en réalité, elles sont utilisées à des fins de fraude ou de vol d'identité.
5. **L'utilisation des informations obtenues** : Une fois que l'attaquant a obtenu les informations souhaitées, il peut les utiliser pour commettre diverses fraudes, telles que l'usurpation d'identité, le vol d'identifiants financiers ou la fraude à la carte de crédit. Ces informations peuvent également être vendues sur le marché noir pour être utilisées par d'autres criminels.

Ce scénario démontre comment les attaquants peuvent exploiter la confiance des individus dans les processus de recrutement pour obtenir des informations sensibles à des fins frauduleuses.

Il met en lumière l'importance pour les professionnels d'être vigilants lorsqu'ils interagissent avec des recruteurs en ligne et de vérifier soigneusement l'authenticité des offres d'emploi avant de fournir des informations personnelles ou financières.

Scénario, "L'attaque par le biais d'un fournisseur tiers"

***Description du scénario** : Dans ce scénario, un attaquant cible une entreprise en se faisant passer pour un fournisseur tiers légitime, tel qu'un prestataire de services informatiques ou un partenaire commercial. L'objectif est de tromper les employés de l'entreprise pour qu'ils effectuent des paiements frauduleux ou divulguent des informations confidentielles.*

1. **Recherche sur la cible** : Avant de lancer l'attaque, l'attaquant effectue des recherches approfondies sur l'entreprise ciblée pour identifier ses fournisseurs tiers légitimes. Il recueille des informations sur les partenariats existants, les processus d'approvisionnement et les contacts clés au sein de l'entreprise.
2. **Création d'un faux e-mail ou d'un faux site web** : L'attaquant crée un e-mail ou un site web contrefait qui imite étroitement la marque et l'identité visuelle du fournisseur légitime. Il utilise des techniques d'ingénierie sociale pour rendre l'e-mail ou le site web aussi convaincant et authentique que possible.
3. **Envoi de demandes de paiement frauduleuses** : L'attaquant envoie des e-mails contrefaits à des employés de l'entreprise, prétendant être un représentant du fournisseur tiers légitime. Dans ces e-mails, il demande des paiements pour des services prétendument rendus ou des produits livrés. Les e-mails peuvent contenir des instructions détaillées sur la manière d'effectuer le paiement, y compris des coordonnées bancaires frauduleuses.
4. **Utilisation de techniques de persuasion** : Pour inciter les employés à agir rapidement, l'attaquant peut utiliser des techniques de persuasion telles que l'urgence (ex: "Ce paiement doit être effectué immédiatement pour éviter des retards dans nos services") ou l'autorité (ex: "Cette demande de paiement a été approuvée par notre département financier").
5. **Réception des paiements frauduleux** : Si les employés de l'entreprise tombent dans le piège et effectuent les paiements demandés, l'argent est transféré sur les comptes contrôlés par l'attaquant. Ce dernier peut ensuite retirer les fonds ou les transférer vers d'autres comptes pour dissimuler leur origine.
6. **Divulgation d'informations confidentielles** : En plus des demandes de paiement frauduleuses, l'attaquant peut également utiliser cette tactique pour obtenir des informations confidentielles telles que des informations sur les systèmes informatiques de l'entreprise, des identifiants de connexion ou des données sensibles sur les clients ou les employés.

Ce scénario met en lumière l'importance pour les entreprises de mettre en place des processus de validation rigoureux pour les demandes de paiement et de sensibiliser les employés aux tactiques utilisées dans les attaques d'ingénierie sociale.

Il souligne également l'importance de vérifier l'authenticité des communications provenant de fournisseurs tiers et de mettre en place des mesures de sécurité robustes pour protéger les actifs financiers et les informations sensibles de l'entreprise.

Scénario, "La fraude au support technique"

***Description du scénario** : Dans ce scénario, un individu malveillant se fait passer pour un technicien informatique légitime et contacte sa victime, prétendant avoir détecté des problèmes sur son ordinateur. L'objectif est de convaincre la victime de fournir un accès à distance à son ordinateur, ce qui permettra à l'attaquant d'installer des logiciels malveillants ou de voler des informations sensibles.*

1. **L'appel ou l'e-mail initial** : L'attaque commence par un appel téléphonique ou un e-mail envoyé à la victime. L'attaquant peut prétendre être un représentant d'une grande entreprise technologique ou d'un service de support technique tiers réputé. Il informe la victime qu'il a détecté des problèmes sur son ordinateur et qu'il est là pour l'aider à les résoudre.
2. **La création d'un sentiment d'urgence** : Pour inciter la victime à agir rapidement, l'attaquant crée un sentiment d'urgence en prétendant que les problèmes détectés sur l'ordinateur de la victime sont graves et nécessitent une action immédiate pour éviter des dommages irréparables. Il peut également menacer la victime en disant que son ordinateur sera bloqué ou qu'elle risque de perdre des données si elle ne coopère pas.
3. **La demande d'accès à distance** : Une fois qu'il a établi un certain niveau de confiance avec la victime, l'attaquant demande l'autorisation d'accéder à distance à l'ordinateur de la victime. Il utilise souvent des logiciels de prise de contrôle à distance légitimes pour établir une connexion avec l'ordinateur de la victime, ce qui lui permet de voir l'écran et de contrôler le clavier et la souris à distance.
4. **L'installation de logiciels malveillants ou la demande de paiement** : Une fois qu'il a accès à l'ordinateur de la victime, l'attaquant peut installer des logiciels malveillants tels que des ransomwares, des enregistreurs de frappe ou des chevaux de Troie. Il peut également afficher de fausses alertes de sécurité ou de faux résultats d'analyse pour convaincre la victime d'acheter des logiciels inutiles ou de souscrire à des services coûteux.
5. **L'exploitation des informations volées** : Une fois que l'attaquant a obtenu ce qu'il veut, il peut utiliser les informations volées à des fins frauduleuses, telles que le vol d'identité, la fraude à la carte de crédit ou la vente sur le marché noir. Dans certains cas, les informations volées peuvent également être utilisées pour cibler d'autres victimes dans des attaques ultérieures.

Ce scénario met en lumière l'importance pour les particuliers d'être sceptiques face aux appels ou aux e-mails non sollicités prétendant provenir de services de support technique.

Il est essentiel de ne jamais partager d'informations personnelles ou d'accorder un accès à distance à son ordinateur à moins d'être absolument certain de l'identité et de la légitimité de la personne ou de l'entreprise avec laquelle vous communiquez.

Scénario, "Le faux profil de rencontre en ligne"

Description du scénario *: Dans ce scénario, un individu malveillant crée un faux profil sur un site de rencontre en ligne dans le but d'établir une relation virtuelle avec sa victime. Une fois qu'il a gagné sa confiance, l'attaquant utilise différentes tactiques pour extorquer de l'argent ou obtenir des informations personnelles de sa victime.*

1. **La création du faux profil** : L'attaquant crée un faux profil sur un site de rencontre en ligne en utilisant des photos attrayantes et des informations fictives sur sa personnalité, ses intérêts et son style de vie. Le profil est conçu pour attirer l'attention et susciter l'intérêt des autres membres du site.
2. **L'établissement d'une relation virtuelle** : Une fois que le faux profil est créé, l'attaquant commence à interagir avec les membres du site, y compris sa future victime. Il engage des conversations et établit une connexion émotionnelle en utilisant des compliments, des flatteries et des messages séduisants pour gagner la confiance de sa victime.
3. **La demande d'argent ou d'autres faveurs** : Après avoir établi une relation de confiance avec sa victime, l'attaquant commence à demander de l'argent ou d'autres faveurs sous prétexte de situations d'urgence ou de besoins financiers. Il peut prétendre avoir des problèmes médicaux, des difficultés financières ou des obstacles à surmonter pour se rencontrer en personne.
4. **La manipulation des émotions** : Pour inciter sa victime à répondre favorablement à ses demandes, l'attaquant manipule ses émotions en jouant sur la sympathie, la culpabilité ou la compassion. Il peut raconter des histoires tristes ou dramatiques pour susciter la pitié et encourager sa victime à lui venir en aide.
5. **La disparition une fois les fonds obtenus** : Une fois que l'attaquant a obtenu ce qu'il veut, il peut disparaître subitement et cesser toute communication avec sa victime. Il peut également continuer à solliciter des fonds en inventant de nouveaux prétextes ou en utilisant des identités différentes sur d'autres sites de rencontre.
6. **L'utilisation des informations personnelles** : En plus de l'extorsion d'argent, l'attaquant peut également utiliser les informations personnelles obtenues pendant la relation pour commettre d'autres formes de fraude ou de vol d'identité, telles que l'usurpation d'identité ou le piratage de comptes en ligne.

Ce scénario met en lumière l'importance pour les utilisateurs de sites de rencontre en ligne d'être vigilants et sceptiques face aux personnes qu'ils rencontrent en ligne.

Il est essentiel de ne jamais partager d'informations personnelles ou financières avec des personnes rencontrées en ligne et de signaler tout comportement suspect ou toute demande inhabituelle aux administrateurs du site.

Scénario, "L'escroquerie aux faux héritages"

***Description du scénario** : Dans ce scénario, un individu malveillant contacte sa victime en prétendant qu'elle est l'héritière d'une fortune importante d'un parent éloigné décédé. L'attaquant utilise différents moyens de communication, tels que des e-mails ou des lettres, pour inciter la victime à croire en la légitimité de l'héritage et à coopérer pour débloquer les fonds prétendument hérités.*

1. **L'approche initiale** : L'attaquant envoie un e-mail ou une lettre à sa victime, prétendant être un avocat, un notaire ou un représentant d'une banque ou d'un cabinet de gestion de patrimoine. Il informe la victime qu'elle est l'héritière d'une fortune importante laissée par un parent éloigné décédé et lui offre son aide pour récupérer les fonds.
2. **La création de documents falsifiés** : Pour donner l'apparence de légitimité à la demande, l'attaquant peut envoyer de faux documents officiels, tels que des testaments, des certificats de décès ou des lettres d'administration successorale. Ces documents sont falsifiés pour inclure le nom de la victime en tant qu'héritière légitime et pour démontrer l'existence des fonds à débloquer.
3. **La demande de frais ou de dépôts initiaux** : Une fois que la victime a exprimé son intérêt pour l'héritage, l'attaquant commence à demander des frais ou des dépôts initiaux pour couvrir les frais administratifs, les taxes successorales ou d'autres dépenses prétendument nécessaires pour débloquer les fonds. Ces frais peuvent être présentés comme temporaires et remboursables une fois que les fonds sont libérés.
4. **La manipulation des émotions** : Pour inciter la victime à coopérer, l'attaquant peut utiliser des tactiques de manipulation émotionnelle telles que la pitié, la sympathie ou l'excitation. Il peut prétendre que l'héritage est une bénédiction inattendue qui changera la vie de la victime pour le mieux et lui offrira des opportunités financières illimitées.
5. **La disparition une fois les fonds obtenus** : Une fois que la victime a versé les frais demandés, l'attaquant peut disparaître subitement et cesser toute communication. Les fonds versés sont généralement irrécupérables, et la victime se rend compte qu'elle a été victime d'une escroquerie aux faux héritages.
6. **L'utilisation des informations personnelles** : En plus de l'extorsion d'argent, l'attaquant peut également utiliser les informations personnelles obtenues pendant la communication pour commettre d'autres formes de fraude ou de vol d'identité, telles que l'usurpation d'identité ou le piratage de comptes en ligne.

Ce scénario souligne l'importance pour les individus d'être prudents lorsqu'ils reçoivent des communications inattendues concernant des héritages ou des fortunes inattendus.

Il est essentiel de vérifier l'authenticité de toute demande et de ne jamais verser d'argent ou fournir des informations personnelles sans une confirmation indépendante de la légitimité de la demande.

Scénario, "Faux services d'assistance sociale"

Description du scénario *: Dans ce scénario, un individu malveillant se fait passer pour un représentant d'un service d'assistance sociale ou d'une organisation caritative et contacte sa victime pour lui proposer de l'aide financière ou des services d'assistance en échange de frais initiaux ou de dons. L'objectif est de convaincre la victime de verser de l'argent ou de fournir des informations personnelles sous de faux prétextes.*

1. **L'approche initiale** : L'attaquant contacte sa victime par téléphone, e-mail ou par le biais de publicités en ligne prétendant représenter un organisme d'assistance sociale, une organisation caritative ou un fonds d'aide d'urgence. Il prétend offrir de l'aide financière ou des services d'assistance pour des situations telles que des difficultés financières, des problèmes de logement ou des besoins médicaux.
2. **La demande de frais initiaux ou de dons** : Une fois qu'il a établi un contact avec sa victime, l'attaquant commence à demander des frais initiaux ou des dons pour couvrir les coûts administratifs, les frais de traitement ou les dépenses prétendument nécessaires pour fournir l'aide ou les services promis. Ces frais peuvent être présentés comme temporaires et remboursables une fois que l'aide est accordée.
3. **La manipulation des émotions** : Pour inciter la victime à verser de l'argent ou à fournir des informations personnelles, l'attaquant peut utiliser des tactiques de manipulation émotionnelle telles que la pitié, la sympathie ou l'urgence. Il peut raconter des histoires tristes ou dramatiques pour susciter la compassion de sa victime et la convaincre d'agir rapidement.
4. **La promesse de résultats rapides ou miraculeux** : Pour rendre l'offre plus attrayante, l'attaquant peut promettre des résultats rapides ou miraculeux, tels que la résolution immédiate des problèmes financiers, le traitement rapide des demandes d'aide ou l'obtention de subventions ou d'allocations importantes.
5. **La disparition une fois les fonds obtenus** : Une fois que la victime a versé les frais demandés ou effectué les dons, l'attaquant peut disparaître subitement et cesser toute communication. Les fonds versés sont généralement irrécupérables, et la victime se rend compte qu'elle a été victime d'une escroquerie aux faux services d'assistance sociale.
6. **L'utilisation des informations personnelles** : En plus de l'extorsion d'argent, l'attaquant peut également utiliser les informations personnelles obtenues pendant la communication pour commettre d'autres formes de fraude ou de vol d'identité, telles que l'usurpation d'identité ou le piratage de comptes en ligne.

Ce scénario souligne l'importance pour les individus d'être prudents lorsqu'ils reçoivent des offres d'aide financière ou d'assistance sociale inattendues.

Il est essentiel de vérifier l'authenticité de toute demande et de ne jamais verser d'argent ou fournir des informations personnelles sans une confirmation indépendante de la légitimité de l'organisation ou de l'organisme d'assistance.

Scénario, "Fausse campagne de sécurité"

Description du scénario *: Dans ce scénario, un attaquant lance une fausse campagne de sensibilisation à la sécurité au sein d'une entreprise, prétendant être une initiative officielle de l'entreprise pour sensibiliser les employés aux menaces de sécurité informatique. L'objectif est d'inciter les employés à participer à des formations en ligne ou à fournir des informations personnelles sous prétexte de renforcer la sécurité de l'entreprise.*

1. **Création de la fausse campagne** : L'attaquant crée une fausse campagne de sensibilisation à la sécurité en utilisant des e-mails, des affiches dans les locaux de l'entreprise ou des messages sur le réseau interne de l'entreprise. Les communications semblent provenir de sources officielles de l'entreprise, avec des logos et des signatures de messagerie falsifiés pour donner l'apparence de légitimité.
2. **Incitation à participer à des formations en ligne** : Les employés sont encouragés à participer à des formations en ligne sur la sécurité informatique en cliquant sur des liens inclus dans les e-mails ou les messages de la campagne. Ces liens dirigent les employés vers de faux sites web qui imitent les plateformes de formation légitimes, mais en réalité, ils sont contrôlés par l'attaquant.
3. **Demande d'informations personnelles** : Pendant les formations en ligne, les employés sont souvent invités à fournir des informations personnelles telles que leur nom, leur adresse e-mail, leur numéro de téléphone ou d'autres données sensibles. Ces informations sont prétendument collectées à des fins de suivi ou de certification, mais en réalité, elles sont utilisées à des fins de phishing ou de vol d'identité.
4. **Installation de logiciels malveillants** : Dans certains cas, les liens inclus dans les e-mails de la campagne peuvent également être utilisés pour distribuer des logiciels malveillants, tels que des chevaux de Troie ou des ransomwares, sur les ordinateurs des employés. Ces logiciels malveillants peuvent être utilisés pour voler des informations sensibles ou compromettre la sécurité du réseau de l'entreprise.
5. **Exploitation de la confiance des employés** : L'attaquant exploite la confiance des employés envers les communications internes de l'entreprise pour inciter leur participation à la fausse campagne de sensibilisation à la sécurité. Les employés sont moins susceptibles de remettre en question l'authenticité de la campagne lorsqu'elle semble provenir de sources internes et de confiance au sein de l'entreprise.
6. **Conséquences pour la sécurité de l'entreprise** : En participant à la fausse campagne, les employés peuvent involontairement compromettre la sécurité de l'entreprise en fournissant des informations sensibles ou en installant des logiciels malveillants sur leurs ordinateurs. Cela peut entraîner des violations de données, des pertes financières ou des dommages à la réputation de l'entreprise.

Ce scénario met en lumière l'importance pour les entreprises de sensibiliser leurs employés aux techniques d'ingénierie sociale et de mettre en place des processus de validation rigoureux pour toute communication interne ou externe concernant la sécurité de l'entreprise.

Il souligne également l'importance pour les employés d'être vigilants et de vérifier l'authenticité des communications avant de fournir des informations personnelles ou de cliquer sur des liens.

Scénario, "Faux service de réparation d'urgence"

Description du scénario *: Dans ce scénario, un individu malveillant se fait passer pour un technicien ou un plombier d'urgence et contacte les résidents par téléphone, par e-mail ou par le biais de publicités en ligne pour leur annoncer qu'une réparation urgente est nécessaire dans leur maison. L'objectif est d'inciter les victimes à fournir des informations personnelles ou à effectuer des paiements en ligne pour planifier la réparation, mais en réalité, il n'y a aucun problème à résoudre et l'attaquant vole les informations fournies.*

1. **L'appel ou l'e-mail initial** : L'attaque commence par un appel téléphonique, un e-mail ou une publicité en ligne envoyée aux résidents, prétendant être un technicien ou un plombier d'urgence travaillant pour une entreprise réputée. L'attaquant informe les victimes qu'une réparation urgente est nécessaire dans leur maison et les incite à agir rapidement pour éviter des dommages graves.
2. **La création d'un sentiment d'urgence** : Pour inciter les victimes à agir rapidement, l'attaquant crée un sentiment d'urgence en prétendant que le problème à résoudre est critique et nécessite une intervention immédiate. Il peut également menacer les victimes en leur disant que leur maison risque d'être endommagée ou que leur sécurité est en danger si la réparation n'est pas effectuée rapidement.
3. **La demande d'informations personnelles ou de paiement** : Une fois qu'il a établi un certain niveau de panique chez les victimes, l'attaquant demande des informations personnelles telles que leur nom, leur adresse, leur numéro de téléphone ou leurs coordonnées bancaires pour planifier la réparation. Il peut également demander des paiements en ligne pour réserver un rendez-vous ou couvrir les frais de service prétendument nécessaires pour la réparation.
4. **L'exploitation de la confiance des victimes** : L'attaquant exploite la confiance des victimes envers les professionnels de la réparation d'urgence pour les convaincre de fournir des informations personnelles ou d'effectuer des paiements en ligne. Les victimes sont moins susceptibles de remettre en question l'authenticité de l'appel ou de l'e-mail lorsqu'elles croient qu'elles sont confrontées à une situation d'urgence réelle.
5. **La disparition une fois les informations ou les paiements obtenus** : Une fois que les victimes ont fourni les informations demandées ou effectué les paiements en ligne, l'attaquant peut disparaître subitement et cesser toute communication. Les informations fournies sont souvent utilisées à des fins de vol d'identité ou de fraude, tandis que les paiements effectués sont irrécupérables.
6. **Les conséquences pour les victimes** : Les victimes peuvent subir des pertes financières importantes en fournissant des informations personnelles ou en effectuant des paiements en ligne à l'attaquant. De plus, leurs informations personnelles peuvent être utilisées à des fins de fraude ou de vol d'identité, ce qui peut entraîner des conséquences à long terme sur leur sécurité financière et leur réputation.

Ce scénario souligne l'importance pour les individus d'être vigilants et sceptiques face aux appels ou aux e-mails non sollicités prétendant provenir de services de réparation d'urgence.

Scénario, "L'arnaque aux faux concours en ligne"

***Description du scénario** : Dans ce scénario, un individu malveillant crée un faux concours en ligne sur les réseaux sociaux ou les sites web populaires, prétendant offrir des prix attrayants tels que des voyages, des produits électroniques ou de l'argent. Les participants sont incités à partager des informations personnelles telles que leur nom, leur adresse e-mail et parfois même leurs coordonnées bancaires pour prétendument participer au concours.*

1. **Création du faux concours** : L'attaquant crée une annonce ou une publication sur les réseaux sociaux ou les sites web, prétendant offrir des prix attrayants dans le cadre d'un concours en ligne. L'annonce est conçue pour attirer l'attention des utilisateurs et les inciter à participer en fournissant leurs informations personnelles pour prétendument avoir une chance de gagner.
2. **Incitation à partager des informations personnelles** : Les utilisateurs sont incités à partager des informations personnelles telles que leur nom, leur adresse e-mail, leur numéro de téléphone et parfois même leurs coordonnées bancaires pour prétendument participer au concours et avoir une chance de gagner les prix annoncés. Ces informations sont souvent collectées via un formulaire en ligne ou une page web dédiée au concours.
3. **Promesses de gains attractifs** : L'attaquant promet des gains attractifs, tels que des vacances de luxe, des produits électroniques haut de gamme ou de l'argent en espèces, pour inciter les utilisateurs à participer au concours. Ces promesses de gains peuvent sembler trop belles pour être vraies, mais elles incitent néanmoins de nombreux utilisateurs à partager leurs informations personnelles dans l'espoir de gagner.
4. **Demande de coordonnées bancaires ou de paiements** : Dans certains cas, les utilisateurs sont également invités à fournir leurs coordonnées bancaires ou à effectuer des paiements pour prétendument augmenter leurs chances de gagner ou pour couvrir les frais de participation au concours. Ces demandes de paiement sont souvent présentées comme temporaires et remboursables une fois que les prix sont attribués.
5. **Disparition une fois les informations obtenues** : Une fois que l'attaquant a collecté suffisamment d'informations personnelles ou de paiements auprès des participants au concours, il peut disparaître subitement et cesser toute communication. Les informations collectées peuvent être utilisées à des fins de phishing, de vol d'identité ou de fraude, tandis que les paiements effectués sont généralement irrécupérables.
6. **Conséquences pour les victimes** : Les participants au concours peuvent subir des pertes financières ou être victimes de fraude en partageant leurs informations personnelles ou en effectuant des paiements en ligne à l'attaquant. De plus, leurs informations personnelles peuvent être utilisées à des fins de vol d'identité, ce qui peut entraîner des conséquences à long terme sur leur sécurité financière et leur réputation.

Ce scénario souligne l'importance de vérifier l'authenticité de toute annonce ou publication avant de partager des informations personnelles ou d'effectuer des paiements en ligne. Il est essentiel de ne jamais partager d'informations sensibles ou financières avec des sources non vérifiées et de signaler toute activité suspecte aux administrateurs du site ou aux autorités compétentes.

Scénario "L'arnaque à la loterie"

Description du scénario *: Dans ce scénario, un individu malveillant contacte sa victime pour lui annoncer qu'elle a gagné à une loterie ou à un tirage au sort, et lui demande de fournir des informations personnelles ou de payer des frais pour recevoir son prix. L'objectif est de tromper la victime en lui faisant croire qu'elle a gagné une somme d'argent importante afin de lui extorquer de l'argent ou de voler ses informations personnelles.*

1. **L'annonce du gain** : L'attaquant contacte sa victime par e-mail, par téléphone ou par courrier pour lui annoncer qu'elle a gagné une loterie ou un tirage au sort. Il lui indique qu'elle a été sélectionnée au hasard parmi des milliers de participants et qu'elle a droit à un prix en argent ou à un cadeau de grande valeur.
2. **La demande d'informations personnelles** : Pour recevoir son prix, la victime est invitée à fournir des informations personnelles telles que son nom complet, son adresse, son numéro de téléphone et parfois même ses coordonnées bancaires. L'attaquant prétend avoir besoin de ces informations pour procéder au paiement du prix ou pour organiser la livraison du cadeau.
3. **La demande de paiement de frais ou de taxes** : Après avoir recueilli les informations personnelles de la victime, l'attaquant lui annonce soudainement qu'elle doit payer des frais de traitement, des taxes ou des frais de livraison pour recevoir son prix. Ces frais sont présentés comme nécessaires pour débloquer le prix et sont souvent demandés avant que la victime puisse recevoir son argent ou son cadeau.
4. **L'urgence et la pression pour agir rapidement** : L'attaquant met généralement la pression sur la victime pour qu'elle agisse rapidement en lui annonçant qu'elle risque de perdre son prix si elle ne paie pas les frais dans un délai imparti. Il peut également utiliser des tactiques de manipulation émotionnelle pour inciter la victime à agir rapidement, en lui faisant croire qu'elle pourrait perdre une opportunité unique.
5. **La disparition une fois les fonds obtenus** : Une fois que la victime a versé les frais demandés, l'attaquant peut disparaître subitement et cesser toute communication. Les fonds versés sont généralement irrécupérables, et la victime se rend compte qu'elle a été victime d'une arnaque à la loterie.
6. **Conséquences pour la victime** : La victime peut subir des pertes financières importantes en versant des frais pour un prix qui n'existe pas réellement. De plus, les informations personnelles fournies à l'attaquant peuvent être utilisées à des fins de vol d'identité ou de fraude, ce qui peut entraîner des conséquences à long terme sur la sécurité financière et la réputation de la victime.

Ce scénario met en évidence l'importance pour les individus d'être prudents lorsqu'ils sont contactés par des inconnus leur annonçant qu'ils ont gagné à une loterie ou à un tirage au sort.

Il est essentiel de vérifier l'authenticité de toute annonce de gain et de ne jamais fournir d'informations personnelles ou de verser des frais à moins d'être certain de la légitimité de la demande.

Scénario "L'arnaque aux petits-enfants en détresse"

***Description du scénario** : Dans ce scénario, un escroc cible une personne âgée en se faisant passer pour son petit-enfant en détresse. L'objectif est de manipuler les émotions de la victime et de lui extorquer de l'argent en prétendant que le petit-enfant a besoin d'aide urgente pour résoudre un problème fictif.*

1. **L'appel ou le message d'urgence** : L'escroc contacte la personne âgée par téléphone ou parfois même par e-mail, se faisant passer pour son petit-enfant. Il prétend être impliqué dans un accident de voiture, avoir été arrêté par la police, ou rencontrer d'autres situations d'urgence nécessitant une aide financière immédiate.
2. **La manipulation émotionnelle** : L'escroc utilise des tactiques de manipulation émotionnelle pour inciter la personne âgée à agir rapidement et sans réfléchir. Il peut prétendre être dans une situation dangereuse, paniquée, ou pleurer au téléphone pour susciter de la compassion et une réaction rapide de la part de la victime.
3. **La demande d'argent** : Une fois qu'il a établi un sentiment d'urgence et manipulé les émotions de la victime, l'escroc demande à la personne âgée de lui envoyer de l'argent pour l'aider à résoudre ses problèmes. Il peut prétendre avoir besoin d'argent pour payer une amende, pour couvrir des frais médicaux, ou pour acheter un billet d'avion pour rentrer chez lui.
4. **La demande de discrétion** : L'escroc demande souvent à la victime de garder secrète la situation, en lui demandant de ne pas en parler à d'autres membres de la famille pour éviter tout problème supplémentaire. Cette demande de discrétion vise à empêcher la victime de vérifier la véracité de l'appel auprès d'autres proches qui pourraient identifier la fraude.
5. **L'envoi d'argent** : Sous l'effet de la peur et de l'inquiétude pour le bien-être de leur petit-enfant, la personne âgée peut être incitée à envoyer de l'argent à l'escroc via un transfert d'argent, un virement bancaire ou l'achat de cartes-cadeaux prépayées. Une fois l'argent envoyé, il est souvent impossible de le récupérer.
6. **La découverte de l'arnaque** : Après avoir envoyé l'argent, la victime peut réaliser qu'elle a été victime d'une arnaque lorsque d'autres membres de la famille contactent le vrai petit-enfant et découvrent qu'il n'était pas en détresse. À ce stade, il est souvent trop tard pour récupérer les fonds envoyés à l'escroc.

Ce scénario souligne l'importance pour les personnes âgées d'être vigilantes face aux appels ou aux messages non sollicités prétendant provenir de membres de la famille en détresse.

Il est essentiel de prendre le temps de vérifier l'authenticité de l'appel en contactant directement le prétendu petit-enfant ou d'autres membres de la famille avant d'envoyer de l'argent ou de partager des informations personnelles.

Scénario "L'arnaque aux investissements frauduleux"

Description du scénario *: Dans ce scénario, un escroc cible une personne âgée en lui proposant des opportunités d'investissement prétendument lucratives. L'objectif est de convaincre la victime d'investir de l'argent dans des projets frauduleux en promettant des rendements élevés, mais fictifs.*

1. **Le contact initial** : L'escroc contacte la personne âgée par téléphone, par e-mail ou par le biais de publicités en ligne pour lui présenter une opportunité d'investissement alléchante. Il peut prétendre être un courtier en investissements, un gestionnaire de fonds ou un expert financier pour gagner la confiance de la victime.
2. **Les promesses de rendements élevés** : L'escroc utilise des tactiques de vente agressives pour convaincre la victime que l'investissement proposé est très rentable et offre des rendements exceptionnels. Il peut promettre des rendements garantis, des bénéfices rapides ou des opportunités d'investissement exclusives pour attirer l'attention de la victime.
3. **La pression pour investir rapidement** : Pour inciter la victime à agir rapidement, l'escroc met souvent la pression en lui disant que l'opportunité d'investissement est limitée dans le temps ou qu'elle risque de manquer une occasion unique si elle n'investit pas rapidement. Cette pression vise à empêcher la victime de prendre le temps de réfléchir et de vérifier l'authenticité de l'offre.
4. **La demande de fonds** : Une fois qu'il a convaincu la victime de l'attrait de l'investissement, l'escroc demande à la personne âgée de lui envoyer de l'argent pour investir dans le projet. Il peut demander un montant initial pour démarrer l'investissement, ou encourager la victime à investir des sommes supplémentaires pour maximiser les rendements.
5. **L'investissement dans des projets fictifs** : En réalité, l'argent de la victime n'est jamais investi dans des projets réels, mais est plutôt utilisé par l'escroc pour ses propres besoins personnels ou pour payer d'autres victimes. Les rendements promis ne se matérialisent jamais, et la victime se rend compte qu'elle a été victime d'une arnaque aux investissements frauduleux.
6. **La découverte de l'arnaque** : Après avoir investi de l'argent, la victime peut réaliser qu'elle a été victime d'une arnaque lorsque les rendements promis ne se concrétisent pas, ou lorsque l'escroc disparaît avec les fonds investis. À ce stade, il peut être difficile voire impossible de récupérer l'argent investi.

Ce scénario souligne l'importance pour les personnes âgées d'être prudentes lorsqu'elles sont contactées par des inconnus leur proposant des opportunités d'investissement alléchantes.

Il est essentiel de prendre le temps de vérifier l'authenticité de l'offre, de consulter un conseiller financier de confiance et de ne jamais investir d'argent dans des projets qui semblent trop beaux pour être vrais.

L'arnaque au site de petites annonces :

***Création de fausses annonces attractives** : Les escrocs créent de fausses annonces pour des produits ou services attractifs, tels que des voitures d'occasion, des appartements à louer, des offres d'emploi, ou même des animaux de compagnie. Ces annonces sont conçues pour attirer l'attention des acheteurs potentiels.*

1. **Prix alléchants** : Les annonces proposent souvent des prix très bas ou des offres exceptionnelles pour les produits ou services annoncés. Ces prix attractifs incitent les acheteurs à contacter rapidement le vendeur sans prendre le temps de vérifier l'authenticité de l'annonce.
2. **Communication via des plateformes non sécurisées** : Les escrocs préfèrent souvent communiquer avec les acheteurs potentiels en dehors des plateformes de petites annonces sécurisées, comme par e-mail ou via des applications de messagerie instantanée. Cela leur permet d'éviter la détection par les modérateurs de la plateforme et de continuer leur arnaque sans être détectés.
3. **Demande de paiement anticipé ou d'informations personnelles** : Une fois qu'un acheteur potentiel montre de l'intérêt pour l'annonce, l'escroc demande généralement un paiement anticipé ou des informations personnelles sensibles pour finaliser la transaction. Il peut s'agir d'un virement bancaire, d'un envoi d'argent via un service de transfert d'argent, ou même de données d'identité telles que le numéro de carte de crédit ou de sécurité sociale.
4. **Fausses promesses de livraison ou de services** : Pour gagner la confiance de l'acheteur, l'escroc peut faire de fausses promesses concernant la livraison du produit ou la prestation du service. Il peut prétendre avoir déjà expédié l'article ou qu'un service sera fourni une fois le paiement reçu, alors qu'en réalité, rien n'est envoyé ou fourni.
5. **Disparition après le paiement** : Une fois que l'acheteur a effectué le paiement ou fourni les informations personnelles demandées, l'escroc disparaît souvent sans laisser de trace. Les tentatives de contacter le vendeur pour obtenir le produit ou le service acheté sont souvent vaines, et l'acheteur se rend compte qu'il a été victime d'une arnaque.
6. **Difficulté à récupérer les fonds ou à signaler l'arnaque** : Il peut être difficile pour les victimes d'arnaques aux petites annonces de récupérer leur argent ou de signaler l'arnaque aux autorités compétentes. Les escrocs utilisent souvent des identités fausses ou des adresses éphémères, ce qui rend leur localisation et leur poursuite difficiles.

En évitant de traiter avec des vendeurs peu fiables ou des annonces suspectes, en vérifiant l'authenticité des informations fournies et en utilisant des plateformes sécurisées pour les transactions en ligne, les acheteurs peuvent réduire les risques de tomber victimes d'une arnaque aux petites annonces.

L'arnaque à la fausse location de vacances :

***Création de fausses annonces attractives** : Les escrocs créent de fausses annonces pour des locations de vacances dans des destinations populaires. Ils utilisent souvent des photos attrayantes et des descriptions détaillées pour attirer les vacanciers potentiels.*

1. **Prix attractifs et conditions alléchantes** : Les annonces proposent généralement des prix inférieurs à la moyenne pour des locations de vacances similaires et offrent des conditions de location très favorables, telles que des séjours prolongés à prix réduit ou des offres de dernière minute.
2. **Communication par e-mail ou messagerie instantanée** : Les escrocs préfèrent souvent communiquer avec les vacanciers potentiels en dehors des plateformes de location de vacances sécurisées, comme par e-mail ou via des applications de messagerie instantanée. Cela leur permet d'éviter la détection par les modérateurs de la plateforme et de continuer leur arnaque sans être détectés.
3. **Demande de paiement anticipé** : Une fois qu'un vacancier potentiel montre de l'intérêt pour l'annonce, l'escroc demande généralement un paiement anticipé pour réserver la location. Il peut s'agir d'un virement bancaire, d'un envoi d'argent via un service de transfert d'argent ou même d'un paiement par carte de crédit.
4. **Fausse documentation et réservation** : Pour donner l'apparence de légitimité, l'escroc peut envoyer au vacancier potentiel de faux documents de réservation ou de confirmation de paiement. Ces documents peuvent sembler authentiques, mais en réalité, la réservation n'existe pas, et l'argent envoyé est perdu.
5. **Indisponibilité du logement ou modification des conditions** : Peu de temps avant la date d'arrivée prévue, l'escroc informe le vacancier que le logement n'est plus disponible pour diverses raisons, telles que des problèmes de maintenance ou des imprévus familiaux. Ils peuvent également demander des frais supplémentaires pour garantir la disponibilité du logement ou proposer un logement alternatif à des conditions moins avantageuses.
6. **Disparition après le paiement** : Une fois que le vacancier a effectué le paiement anticipé, l'escroc disparaît souvent sans laisser de trace. Les tentatives de contacter le propriétaire pour obtenir un remboursement ou des explications sont souvent vaines, et le vacancier se rend compte qu'il a été victime d'une arnaque.
7. **Difficulté à récupérer les fonds ou à signaler l'arnaque** : Il peut être difficile pour les victimes d'arnaques à la fausse location de vacances de récupérer leur argent ou de signaler l'arnaque aux autorités compétentes. Les escrocs utilisent souvent des identités fausses ou des adresses éphémères, ce qui rend leur localisation et leur poursuite difficiles.

En évitant de traiter avec des propriétaires peu fiables ou des annonces suspectes, en vérifiant l'authenticité des informations fournies et en utilisant des plateformes sécurisées pour les transactions en ligne, les vacanciers peuvent réduire les risques de tomber victimes d'une arnaque à la fausse location de vacances.

L'arnaque aux faux produits en ligne

Création de faux sites web ou annonces en ligne *: Les brouteurs créent de faux sites web ou annonces sur des plateformes de commerce en ligne, offrant des produits populaires à des prix très attractifs. Ces produits peuvent être des articles de mode, des appareils électroniques, des produits de beauté, etc.*

1. **Prix très bas** : Les prix proposés pour les produits sont souvent très bas par rapport à ceux du marché. Cette stratégie vise à attirer les acheteurs en offrant des économies importantes sur des produits populaires et attractifs.
2. **Images et descriptions trompeuses** : Les brouteurs utilisent souvent des images et des descriptions de produits volées à d'autres sites légitimes. Ces images peuvent être de haute qualité et les descriptions peuvent sembler authentiques, mais en réalité, elles ne correspondent pas nécessairement au produit réel.
3. **Paiement demandé à l'avance** : Pour passer commande, les acheteurs sont invités à effectuer un paiement à l'avance, généralement par carte de crédit ou virement bancaire. Les brouteurs peuvent également offrir des options de paiement telles que Western Union ou des cartes-cadeaux prépayées.
4. **Non-livraison ou envoi de produits de mauvaise qualité** : Une fois que le paiement est effectué, les brouteurs n'envoient jamais le produit commandé ou envoient un produit de mauvaise qualité qui ne correspond pas à la description. Dans certains cas, les colis peuvent être vides ou contenir des produits de contrefaçon de qualité inférieure.
5. **Difficultés pour contacter le vendeur** : Après avoir passé commande, les acheteurs peuvent rencontrer des difficultés pour contacter le vendeur en cas de problème. Les adresses e-mail ou numéros de téléphone fournis peuvent être inactifs ou ne pas recevoir de réponse, laissant les acheteurs sans recours.
6. **Absence de remboursement** : En cas de non-livraison ou de réception d'un produit de mauvaise qualité, les acheteurs ont souvent du mal à obtenir un remboursement. Les brouteurs peuvent ignorer les demandes de remboursement ou refuser de les traiter, laissant les acheteurs avec une perte financière.

Cette arnaque aux faux produits en ligne exploite la confiance des consommateurs dans les achats en ligne et vise à leur faire croire qu'ils obtiennent une bonne affaire.

Il est essentiel pour les acheteurs de rester vigilants, de vérifier l'authenticité des sites web et des vendeurs avant de faire un achat, et de privilégier les sites de commerce en ligne réputés et fiables.

(voir page suivante)

L'arnaque au faux e-mail de "Itsme"

L'arnaque au faux e-mail de "Itsme" est une escroquerie où les fraudeurs envoient des e-mails frauduleux prétendant provenir du service d'authentification belge "Itsme". Voici comment cela se déroule :

1. **Réception de l'e-mail** : La victime reçoit un e-mail prétendument envoyé par Itsme. L'e-mail peut sembler authentique, utilisant des logos et des informations de mise en page similaires à ceux de la véritable entreprise.
2. **Contenu de l'e-mail** : Le contenu de l'e-mail peut varier, mais il impliquera souvent une action urgente de la part de la victime. Par exemple, l'e-mail peut prétendre qu'il y a eu une activité suspecte sur le compte Itsme de la victime et qu'elle doit se connecter immédiatement pour vérifier son compte ou prendre des mesures de sécurité.
3. **Liens malveillants ou pièces jointes** : L'e-mail contient généralement des liens malveillants ou des pièces jointes infectées par des logiciels malveillants. Les liens peuvent rediriger vers de faux sites web conçus pour voler les informations de connexion ou installer des logiciels malveillants sur l'ordinateur de la victime.
4. **Tentative de vol d'informations personnelles** : L'objectif principal de l'arnaque est de voler les informations personnelles et les identifiants de connexion de la victime. Les fraudeurs peuvent utiliser ces informations pour accéder aux comptes en ligne de la victime, voler des fonds ou commettre d'autres formes de fraude.
5. **Utilisation de tactiques de manipulation** : Les fraudeurs utilisent souvent des tactiques de manipulation pour inciter la victime à agir rapidement et sans réfléchir. Ils peuvent créer un sentiment d'urgence en prétendant que l'accès au compte est bloqué ou que des fonds sont en danger.
6. **Prévention et signalement** : Pour se protéger, il est essentiel de vérifier attentivement l'authenticité des e-mails prétendant provenir de services comme Itsme. Ne cliquez jamais sur des liens suspects ou des pièces jointes, et ne fournissez jamais d'informations personnelles ou de connexion en réponse à des e-mails non sollicités. Signalez tout e-mail suspect à l'entreprise prétendument représentée et aux autorités compétentes.

VOIR :

https://safeonweb.be/fr/actualite/attention-aux-messages-de-phishing-semblant-provenir-ditsme

L’arnaque « VISA Awards »

L'arnaque aux faux e-mails prétendant être de Visa et offrant une importante somme d'argent :

1. **Réception de l'e-mail frauduleux** : La victime reçoit un e-mail prétendant être de Visa, indiquant qu'elle a été sélectionnée pour participer à un programme de promotion des services de Visa. L'e-mail peut sembler officiel, utilisant des logos et des mises en page similaires à ceux de Visa pour paraître légitime.
2. **Promesse d'une somme importante d'argent** : L'e-mail informe la victime qu'elle a été choisie pour recevoir une somme importante d'argent, souvent sous la forme d'un montant fixe comme 1.000.000 €. Cette promesse de gain important est utilisée pour attirer l'attention de la victime et la pousser à répondre à l'e-mail.
3. **Demande d'informations personnelles** : Pour recevoir le montant promis, l'e-mail demande à la victime de fournir une série d'informations personnelles, telles que son nom complet, son adresse, son numéro de téléphone, son numéro de carte d'identité ou de passeport, son numéro de sécurité sociale, etc. Ces informations sont utilisées pour voler l'identité de la victime ou pour commettre d'autres formes de fraude.
4. **Utilisation de tactiques de manipulation** : Les fraudeurs utilisent souvent des tactiques de manipulation pour inciter la victime à agir rapidement et sans réfléchir. Ils peuvent créer un sentiment d'urgence en prétendant que la promotion est limitée dans le temps et que la victime doit fournir ses informations rapidement pour bénéficier de l'offre.
5. **Faux frais ou conditions cachées** : Après avoir fourni leurs informations personnelles, les victimes peuvent être informées qu'elles doivent payer des frais de traitement, des frais de dossier ou d'autres frais imaginaires pour recevoir le montant promis. Les escrocs peuvent également imposer des conditions supplémentaires, telles que l'achat de produits ou services spécifiques, pour obtenir le gain.
6. **Absence de récompense et risques pour les données personnelles** : Après avoir fourni leurs informations personnelles ou payé les frais demandés, les victimes ne reçoivent jamais le montant promis. Au lieu de cela, elles risquent d'être victimes d'usurpation d'identité, de fraude financière ou d'autres formes de cybercriminalité.
7. **Prévention et signalement** : Il est crucial pour les destinataires de ces e-mails de ne pas répondre, de ne pas fournir d'informations personnelles et de ne pas effectuer de paiement en réponse à de telles offres. Ils doivent signaler l'e-mail suspect à Visa et aux autorités compétentes pour enquête et suppression de la fraude.

En restant vigilants et en refusant de partager des informations personnelles ou de répondre à de telles offres alléchantes, les utilisateurs peuvent se protéger contre les tentatives d'arnaque aux faux e-mails prétendant être de grandes entreprises telles que Visa.

Remote Access Scam / Main-mise sur votre ordinnateur

1. **Contact initial** : Le scam commence généralement par un appel téléphonique non sollicité ou un e-mail prétendant être d'une entreprise de technologie réputée, comme Microsoft ou Apple. Les escrocs prétendent souvent être des représentants du support technique ou de la sécurité informatique de ces entreprises.
2. **Prétexte alarmiste** : Les escrocs utilisent des prétextes alarmistes pour inciter la victime à agir rapidement. Ils peuvent prétendre avoir détecté des activités suspectes sur l'ordinateur de la victime, comme des virus, des piratages ou des violations de données.
3. **Offre d'aide technique** : Pour résoudre le problème prétendu, les escrocs offrent leur aide technique à la victime. Ils prétendent pouvoir résoudre les problèmes à distance en accédant à l'ordinateur de la victime via un logiciel de contrôle à distance.
4. **Installation d'un logiciel malveillant** : Les escrocs demandent à la victime de télécharger et d'installer un logiciel de contrôle à distance, souvent en prétendant qu'il s'agit d'un outil de sécurité légitime. En réalité, ce logiciel est un malware conçu pour donner aux escrocs un accès complet à l'ordinateur de la victime.
5. **Vol d'informations sensibles** : Une fois que le logiciel malveillant est installé, les escrocs peuvent accéder aux fichiers et aux données sensibles de l'ordinateur de la victime, y compris les identifiants de connexion, les informations financières et les données personnelles.
6. **Demande de paiement** : Après avoir pris le contrôle de l'ordinateur de la victime, les escrocs peuvent exiger un paiement pour supprimer les logiciels malveillants prétendument détectés ou pour fournir un support technique supplémentaire. Ils peuvent également menacer de supprimer des fichiers ou de corrompre le système si la victime refuse de payer.
7. **Extorsion et chantage** : Certains escrocs utilisent des tactiques d'extorsion et de chantage pour inciter la victime à payer. Ils menacent de divulguer des informations sensibles ou des images compromettantes présumées stockées sur l'ordinateur de la victime à moins qu'elle ne paie une rançon.
8. **Prévention et signalement** : Pour se protéger contre le Remote Access Scam, il est important de ne jamais donner accès à distance à son ordinateur à des personnes non fiables ou non sollicitées. En outre, il est essentiel de ne pas télécharger de logiciels ou de fichiers à partir de sources non vérifiées et de garder son système informatique à jour avec des logiciels de sécurité fiables. Toute activité suspecte doit être signalée aux autorités compétentes.

Pour vérifier l'authenticité d'un site en ligne, voici quelques points à vérifier :

1. **URL du site** : Vérifiez l'URL du site web. Assurez-vous qu'elle est correctement orthographiée et qu'elle utilise le protocole HTTPS, indiquant une connexion sécurisée.
2. **Certificat SSL** : Recherchez la présence d'un certificat SSL. Vous devriez voir un petit cadenas à côté de l'URL du site, ce qui indique que la connexion est sécurisée.
3. **Contact et coordonnées** : Recherchez les informations de contact du vendeur, telles qu'une adresse physique, un numéro de téléphone et une adresse e-mail. Un site légitime devrait fournir ces informations clairement.
4. **Politique de confidentialité** : Vérifiez s'il existe une politique de confidentialité sur le site. Cela indique que le site prend la protection des données personnelles au sérieux.
5. **Avis et témoignages** : Recherchez des avis et des témoignages d'autres clients sur le site. Des avis positifs et authentiques peuvent indiquer que le site est fiable, mais méfiez-vous des avis excessivement positifs ou trop génériques.
6. **Informations sur la société** : Recherchez des informations sur la société derrière le site, telles que son histoire, sa réputation et son expérience dans le domaine.
7. **Méthodes de paiement sécurisées** : Assurez-vous que le site propose des méthodes de paiement sécurisées, telles que PayPal, les cartes de crédit ou les portefeuilles électroniques réputés. Évitez les sites qui demandent des paiements par virement bancaire ou Western Union.
8. **Politique de retour et de remboursement** : Consultez la politique de retour et de remboursement du site. Un site légitime devrait offrir des options claires pour les retours et les remboursements en cas de problème avec votre commande.
9. **Design du site** : Évaluez la conception générale du site. Les sites web légitimes ont généralement un design professionnel et cohérent, tandis que les sites frauduleux peuvent sembler bâclés ou comporter des erreurs de grammaire et d'orthographe.
10. **Recherche en ligne** : Faites une recherche en ligne sur le site et la société qui le gère. Vérifiez s'il existe des signalements d'arnaques ou des plaintes de consommateurs concernant le site.

En suivant ces conseils, vous pouvez réduire les risques d'acheter sur des sites web frauduleux et vous assurer que vos transactions en ligne sont sécurisées et fiables.

Pour vérifier l'authenticité d'un e-mail reçu, voici quelques points à vérifier :

1. **Adresse de l'expéditeur** : Vérifiez l'adresse e-mail de l'expéditeur. Assurez-vous qu'elle correspond à celle d'une organisation légitime. Méfiez-vous des adresses e-mail suspectes ou inhabituelles :
    - **Afficher l'adresse complète** : Dans votre logiciel de messagerie, recherchez l'option pour afficher l'adresse e-mail complète de l'expéditeur. Parfois, seuls le nom et l'adresse e-mail raccourcie sont affichés par défaut.
    - **Analyser l'adresse e-mail** : Examinez attentivement l'adresse e-mail complète de l'expéditeur. Assurez-vous qu'elle correspond à l'adresse d'une organisation légitime ou d'une personne que vous connaissez.
    - **Vérifier la syntaxe de l'adresse e-mail** : Assurez-vous que l'adresse e-mail est correctement orthographiée et formatée. Méfiez-vous des adresses e-mail contenant des caractères inhabituels, des fautes d'orthographe ou des chiffres aléatoires.
    - **Regarder le domaine de l'adresse e-mail** : Faites attention au domaine de l'adresse e-mail (la partie après le "@"). Les e-mails provenant d'organisations légitimes utilisent généralement des domaines correspondant au nom de l'entreprise (par exemple, "@nomdelentreprise.com").
    - **Utiliser une loupe** : Si nécessaire, utilisez la fonction de zoom ou une loupe pour agrandir l'adresse e-mail et examiner les détails. Cela peut vous aider à repérer les éléments suspects ou les caractères non conformes.
    - **Comparaison avec les contacts connus** : Comparez l'adresse e-mail de l'expéditeur avec celles des contacts que vous connaissez déjà. Si l'adresse semble différente de celles des communications précédentes, cela peut être un signe d'arnaque.
    - **Recherche en ligne** : Si vous avez des doutes sur l'authenticité de l'adresse e-mail, effectuez une recherche en ligne pour voir si d'autres personnes ont signalé des activités frauduleuses provenant de cette adresse.
    - **Utiliser des outils de vérification** : Utilisez des outils en ligne qui vous permettent de vérifier la légitimité d'une adresse e-mail. Certains services peuvent fournir des informations sur le propriétaire du domaine et les antécédents de l'adresse e-mail.
2. **Nom de l'expéditeur** : Vérifiez le nom de l'expéditeur affiché dans l'e-mail. Assurez-vous qu'il correspond à celui d'une personne ou d'une organisation avec laquelle vous avez une relation ou que vous connaissez.
3. **Orthographe et grammaire** : Faites attention à l'orthographe et à la grammaire de l'e-mail. Les e-mails frauduleux peuvent contenir des fautes d'orthographe ou de grammaire, ce qui peut indiquer qu'ils ne sont pas légitimes.
4. **Liens et URL** : Ne cliquez pas sur les liens inclus dans l'e-mail avant de les avoir vérifiés. Passez le curseur de la souris sur les liens pour voir l'URL réelle. Assurez-vous qu'ils dirigent vers des sites web légitimes et sécurisés.

5. **Pièces jointes** : Ne téléchargez pas de pièces jointes provenant d'e-mails suspects. Les pièces jointes peuvent contenir des logiciels malveillants ou des virus qui pourraient endommager votre ordinateur ou voler vos informations personnelles.
6. **Demandes de renseignements personnels ou financiers** : Soyez sceptique face aux e-mails demandant des informations personnelles ou financières sensibles, telles que des mots de passe, des numéros de carte de crédit ou des numéros de sécurité sociale. Les organisations légitimes ne demandent généralement pas de telles informations par e-mail.
7. **Sentiment d'urgence** : Méfiez-vous des e-mails qui créent un sentiment d'urgence ou de peur pour vous inciter à agir rapidement. Les escrocs utilisent souvent des tactiques de manipulation émotionnelle pour inciter les destinataires à prendre des décisions hâtives.
8. **Vérification auprès de l'organisation** : Si vous avez des doutes sur la légitimité d'un e-mail, contactez directement l'organisation ou la personne mentionnée dans l'e-mail pour vérifier son authenticité. Utilisez les coordonnées de contact officielles et ne répondez pas directement à l'e-mail suspect.
9. **Filtrage des e-mails** : Utilisez des filtres anti-spam pour bloquer les e-mails suspects avant qu'ils n'atteignent votre boîte de réception. De nombreux fournisseurs de messagerie électronique offrent des options de filtrage pour vous aider à identifier et à bloquer les e-mails indésirables.

En suivant ces conseils, vous pouvez réduire les risques de tomber victime d'une arnaque par e-mail et protéger vos informations personnelles et financières contre les cybercriminels.

Liste des télévendeurs et bureaux de recouvrement pour lesquels le SPF Economie a reçu des signalements

Liste des télévendeurs frauduleux

Le SPF Economie et le Centre Européen des Consommateurs vous recommandent la prudence lorsque vous recevez des appels pour des offres de bons de réduction pour des achats en ligne, des voyages à prix avantageux, des produits en ligne, etc.

Redoublez de vigilance si ces appels proviennent des entreprises suivantes :

- 100 with 100
- Active Tours
- AuSoley
- All Great Dealz
- BeneluxKorting
- BeterPrijs
- Buy2Fly
- Cheap Travel
- Checking hotel / Checkinhotel
- City Trip on/citytripon.com
- DLand
- Evitale
- Evasion Belgique
- Fortunaspel
- Go and Fly
- Holiday Check
- Home @ holiday
- Lotto en ligne
- LuxStyle / Digital Sourcing
- Malloni Voyages
- Next Fly
- Nils Travel
- Pay Care
- Shop&Fly
- Shoppen doe je zo
- Skinbooster
- Spaarcodes
- Tour Vacation
- Travel Club Express
- Voordelig Winkelen
- Weekendje genieten

Bureaux de recouvrement frauduleux

Le SPF Economie vous conseille de ne pas payer si vous recevez une injonction de paiement d'un des bureaux de recouvrement suivants :

- Anthony & Partners
- **Bureaux de recouvrement ayant « fixdebt » dans leurs adresses e-mail**
- Cannock Chase Incasso BV
- Dijkstra en Rademakers
- Edward & Rhoda
- Facture collect
- Finance collect b.v.
- Flanderijn en Partners
- Goudsmit en Jacobs
- Hoiman en Guzel
- Internationaal Collect B.V.
- International finance collect B.V.
- Inter Payment Service
- Interpay Collect B.V.
- Jagersma & Kacmaz
- Jansens en Guzel
- Jonkheer en Partners
- Juilan & Jackman
- Juristen Incasso
- Leijten en Partners
- Molmans & Guezel
- Nijhof & Guzel
- Pragma Finance
- Raadsma en Koc
- Sanders en Anthony
- Smits en Co. / Smits Deurwaarders
- Sloq bv
- Sloq en Lootsma
- Sloq en Partners
- Sloq en Reinders
- Sloq Finance
- Veenstra en de Jong
- Wijngaard en Jansen

Vous êtes ou vous avez été victime d’une fraude

La fraude informatique est la variante en ligne de l'escroquerie au sens classique du terme :

soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand cela se passe par internet, il s'agit également d'escroquerie.

Pour dénoncer une fraude informatique, rendez-vous sur le site Safeonweb à l’adresse à

https://www.safeonweb.be/fr/au-secours

Vous avez reçu un message suspect ?

Envoyez-le à l’adresse suspect@safeonweb.be et supprimez-le ensuite.

Si vous recevez un message suspect au travail, vous devez suivre les procédures en vigueur pour le phishing. Par exemple, l’envoyer vers le service ICT.

Contacter Safeonweb ?

Avez-vous une question sur la cybersécurité? Avez-vous une suggestion? Voulez-vous témoigner en tant que victime? Envoyez votre question à info@safeonweb.be. Une équipe de cyber experts répondra à votre question. Décrivez votre problème aussi clairement que possible et joignez toute capture d'écran ou autre matériel visuel.

Trop tard, vous avez été escroqué ?

Si vous avez perdu de l'argent ou si vous êtes victime d'une extorsion, nous vous conseillons de faire une déclaration à la police. Vous pouvez le signaler à la police locale de votre lieu de résidence.

Contactez votre banque et/ou Card Stop au 078 170 170 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 peuvent être bloquées.