Résous ton problème avec un clin d'œil

# Je vends un canapé, et l'acheteur veut les coordonnées de ma carte bancaire ?

## Comment acheter et vendre en toute sécurité sur les sites de petites annonces



**Max Paradox**

# Je vends un canapé, et l'acheteur veut les coordonnées de ma carte bancaire ?

Comment acheter et vendre en toute sécurité sur les sites de petites annonces

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384905951

ALL-IN Rafał Płonkowski



# TABLE DES MATIÈRES

INTRO ..... 5

Chapitre 1 - Quand une simple petite annonce se transforme en piège ..... 11

Chapitre 2 - Pourquoi un escroc paraît-il plus crédible que votre propre bon sens ? ..... 21

Chapitre 3 - Sept signaux d'alarme qui devraient vous faire arrêter une transaction ..... 33

Chapitre 4 - Le faux sentiment de sécurité, ou comment nous facilitons nous-mêmes le travail des escrocs ..... 44

Chapitre 5 - Toutes les bonnes affaires n'en sont pas : comment acheter sans mettre son bon sens en veille ..... 57

Chapitre 6 - Le vendeur doit lui aussi rester vigilant : comment ne pas perdre son argent en même temps que son objet ..... 68

Chapitre 7 - Payer en toute sécurité, ou pourquoi l'argent ne devrait pas circuler sur une simple promesse ..... 79

Chapitre 8 - Vous n'êtes pas obligé d'être aimable à tout prix : l'art de mettre fin aux conversations suspectes ..... 90

Chapitre 9 - Une transaction sous contrôle : du premier message à la dernière confirmation ..... 103

Chapitre 10 - Détective numérique sans loupe : comment vérifier les informations avant de croire une petite annonce ..... 113

Chapitre 11 - Un lien vers votre argent ou vers les ennuis ? Comment reconnaître les faux messages et les fausses pages de paiement ..... 124

Chapitre 12 - Votre compte n'est pas un vestiaire collectif : comment protéger l'accès aux plateformes et aux services bancaires ..... 134

Chapitre 13 - Le colis est arrivé, mais la réalité ne correspond pas à la description : comment résoudre les litiges après un achat ..... 145

Chapitre 14 - Avant que l'escroc ne disparaisse avec votre argent : que faire lorsqu'une transaction suspecte devient une menace réelle ? ..... 157

Chapitre 15 - Quand une escroquerie comporte plusieurs niveaux : ces cas complexes où la prudence ordinaire ne suffit plus ..... 168

Chapitre 16 - Quand la prudence se heurte à la réalité : que faire lorsque vous manquez de temps, de connaissances ou de conditions idéales ? ..... 180

Chapitre 17 - Je me suis fait avoir. Et maintenant ? Comment reprendre le contrôle quand le mal est déjà fait ..... 192

Chapitre 18 - Acheter en sécurité sans devenir paranoïaque : comment conserver les bonnes habitudes ..... 203

Chapitre 19 - Quand le bon sens prend des vacances : comment reconnaître le retour des anciennes erreurs ..... 215

Chapitre 20 - Vendez votre canapé, pas votre tranquillité : comment prendre vous-même des décisions sûres ..... 228

# INTRO

Vous mettez un canapé en vente. Les photos sont prises, le prix est raisonnable, la description est honnête. Vous avez même disposé les coussins de manière à ce qu'ils aient l'air plus heureux de vivre que vous un lundi matin. Sept minutes passent et un message arrive. L'acheteur est décidé, il ne négocie pas, ne demande pas les dimensions, ne s'intéresse ni à la couleur ni au fait que l'accoudoir gauche a connu le précédent propriétaire. Il veut acheter immédiatement. Il n'a qu'une seule demande : vous devez cliquer sur le lien qu'il vous envoie, saisir les coordonnées de votre carte bancaire et confirmer la réception de l'argent.

Curieux. Vous vendez un canapé pour six cents zlotys, et quelqu'un se comporte comme s'il venait de vous inviter à gérer un système de règlement interbancaire.

C'est là que commence une histoire qui peut se terminer de trois façons. Première possibilité : vous reconnaissez l'arnaque, vous refusez et vous retournez regarder votre série. Deuxième possibilité : vous commencez à soupçonner que quelque chose ne tourne pas rond, mais l'acheteur, si aimable, vous explique la procédure avec une telle assurance que vous finissez par cliquer. Troisième possibilité : quelques minutes plus tard, vous fixez votre téléphone en vous demandant pourquoi, au lieu de recevoir six cents zlotys, vous venez d'autoriser une opération que vous n'aviez absolument pas prévue.

Ce livre a été écrit pour que le premier scénario devienne votre réflexe naturel. Sans avoir besoin de décrocher un doctorat en cybersécurité, de cultiver la paranoïa ou de considérer chaque personne intéressée par votre petite

table d'occasion comme un membre d'un syndicat international du crime.

Les sites de petites annonces sont une invention formidable. Ils permettent de vendre des objets devenus inutiles, de trouver du matériel d'occasion à un prix intéressant et de transmettre à quelqu'un un objet qui, chez nous, ne fait plus qu'occuper de la place. Grâce à eux, un objet peut connaître une seconde vie et une maison récupérer quelques précieux mètres carrés. Le problème, c'est que là où se rencontrent des inconnus, de l'argent, de la précipitation et Internet, apparaissent également des individus qui ont décidé de gagner leur vie en exploitant la confiance des autres.

Certaines arnaques sont rudimentaires. Le message semble avoir été traduit automatiquement depuis une langue que son auteur n'a jamais entendue, et le lien mène à une page dont l'adresse ressemble à un mot de passe inventé par un chat se promenant sur un clavier. D'autres sont beaucoup plus convaincantes. Un escroc peut connaître le nom d'une plateforme populaire, reprendre son identité visuelle, imiter les notifications d'une société de livraison ou se faire passer pour un employé de banque. Il sait parler calmement, poliment et avec fermeté. Il donne parfois l'impression de mieux maîtriser les procédures que le véritable service client.

Mais le plus important, c'est qu'un escroc n'a pas besoin d'être un génie de l'informatique. Il lui suffit de bien comprendre les êtres humains.

Il sait qu'un vendeur se réjouit lorsqu'il trouve rapidement un acheteur. Il sait qu'un acheteur redoute de laisser passer une bonne affaire. Il sait que la plupart d'entre nous souhaitent conclure leur transaction sans complications,

sans passer pour quelqu'un de soupçonneux et sans poser de questions qui pourraient sembler stupides. Voilà pourquoi un escroc commence rarement une conversation par : « Bonjour, j'aimerais vous voler votre argent. » À la place, il propose une solution pratique, donne des garanties de sécurité et suggère une petite étape supplémentaire.

Cette petite étape peut devenir le clic le plus coûteux de toute l'histoire.

Et contrairement à ce que l'on pourrait croire, il n'est pas nécessaire d'être mal à l'aise avec la technologie pour tomber dans le piège. Vous pouvez utiliser les services bancaires en ligne tous les jours, faire vos achats depuis votre téléphone et parfaitement comprendre le fonctionnement d'un paiement par carte. Cela ne vous empêche pas d'être pris au dépourvu dans une situation où votre attention est concentrée sur tout autre chose. Après tout, vous ne vous installez pas devant votre ordinateur avec l'intention de participer à un exercice de détection de la cybercriminalité. Vous voulez vendre le vélo de votre enfant, acheter un téléphone d'occasion ou vous débarrasser d'un petit meuble qui bloque l'accès à une prise électrique depuis deux ans.

C'est précisément cette banalité que l'escroquerie exploite.

Il existe aussi l'autre côté de la transaction. Les acheteurs ont, eux aussi, de bonnes raisons d'être prudents. Un prix attractif, de superbes photos et la mention « état impeccable, utilisé seulement quelques fois » ne prouvent pas automatiquement que l'objet existe réellement. On rencontre de fausses annonces, des tentatives d'extorsion d'acomptes, des pressions pour payer en dehors du système officiel et des colis dont le contenu a autant de

rapport avec la description que la photo d'un hôtel de luxe avec une nuit passée dans un placard à balais. Pourtant, toute transaction qui tourne mal n'est pas nécessairement une escroquerie. Parfois, le vendeur n'a réellement pas remarqué un défaut, le transporteur a interverti deux colis ou les deux parties n'ont pas compris leurs accords de la même manière. Savoir distinguer une erreur, un litige et une tentative de fraude délibérée est tout aussi important que de reconnaître les liens suspects.

Je ne vais pas essayer de vous convaincre qu'Internet est une jungle où, derrière chaque annonce, se cache un criminel armé d'un ordinateur portable et d'un rire machiavélique. La plupart des transactions quotidiennes peuvent se dérouler normalement et en toute sécurité. L'objectif est beaucoup plus pratique : apprendre à reconnaître le moment où une opération d'achat ou de vente tout à fait ordinaire commence à ressembler à une mise en scène orchestrée par quelqu'un qui cherche à prendre le contrôle de votre décision.

Dans ce livre, nous examinerons pourquoi il est si facile de faire confiance à un message apparemment crédible, comment fonctionnent les fausses confirmations de paiement, ce que peut cacher une demande de code, de coordonnées bancaires ou d'autorisation supplémentaire, et pourquoi un message urgent provenant prétendument d'un livreur n'a pas forcément été envoyé par un livreur. Nous aborderons également la sélection prudente des annonces, la vérification des vendeurs, la définition des conditions d'une transaction et la conservation des échanges, afin qu'en cas de problème, votre seule preuve ne soit pas une conversation intitulée « Mais vous m'aviez pourtant promis ».

Nous n'allons pas construire notre sécurité autour d'une règle magique. Le conseil populaire « ne cliquez jamais sur les liens » est percutant, mais il n'apprend pas grand-chose à lui seul. Un lien peut mener à un véritable site ou à une imitation remarquablement bien réalisée. De la même manière, toute demande d'informations supplémentaires ne constitue pas nécessairement une tentative criminelle. Ce qui compte, c'est le contexte : qui vous demande quelque chose, dans quel but, par quel canal, si vous pouvez vérifier cette demande de manière indépendante et ce que vous êtes réellement en train d'autoriser. La sécurité ne consiste pas à mémoriser cent interdictions, mais à comprendre quelques mécanismes qui reviennent sous différentes formes.

Nous verrons aussi ce qu'il faut faire lorsque quelque chose a déjà mal tourné. Car une personne qui réalise son erreur après avoir cliqué a besoin de mesures concrètes, pas d'une conférence expliquant qu'elle aurait dû faire attention. Selon la situation, il peut être nécessaire de contacter rapidement sa banque, de faire opposition à sa carte, de sécuriser son compte, de conserver les preuves ou de signaler les faits aux organismes compétents. Toutes les pertes ne peuvent pas être récupérées, mais l'hésitation et la honte risquent d'aggraver encore la situation. Personne ne récupérera son argent en passant trois heures à se traiter d'idiot.

Et si vous n'avez encore jamais vécu une telle mésaventure ? Tant mieux. La leçon la moins chère sur les escroqueries est celle que vous n'avez pas besoin de financer avec vos propres économies.

Vous n'avez pas besoin de cesser de faire confiance aux gens après avoir lu ce livre. Il suffit d'arrêter de considérer la

politesse, l'urgence et un message à l'apparence professionnelle comme des preuves de fiabilité. Vous pourrez continuer à vendre, à acheter, à négocier et à profiter des bonnes affaires. Simplement, avant de suivre une instruction inhabituelle, vous vous poserez quelques questions pertinentes et vérifierez ce qui peut l'être indépendamment de votre interlocuteur.

Parce que lorsque vous vendez un canapé, l'acheteur devrait avant tout s'intéresser au canapé.

Et s'il s'intéresse davantage au numéro de votre carte bancaire, il serait peut-être raisonnable d'envisager qu'il ne cherche pas vraiment un endroit où s'asseoir.

# Chapitre 1 - Quand une simple petite annonce se transforme en piège

Vous mettez une machine à café en vente. Elle fonctionne, elle est en assez bon état et son seul défaut est d'avoir récemment servi davantage de décoration sur le plan de travail que d'appareil destiné à préparer des boissons. Vous fixez le prix à trois cents zlotys, ajoutez quelques photos et publiez votre annonce. Cinq minutes ne se sont pas encore écoulées qu'un acheteur potentiel vous contacte. Il ne pose aucune question sur la marque, l'état technique ou la raison de la vente. Il n'essaie même pas de négocier une réduction de vingt zlotys, ce qui, dans l'univers des petites annonces en ligne, est presque aussi extraordinaire que d'apercevoir une licorne sur le parking d'un supermarché.

L'acheteur écrit que tout lui convient. Il souhaite payer immédiatement et faire venir un transporteur. Il vous envoie un lien pour confirmer la transaction. La page semble professionnelle, affiche des éléments graphiques familiers et indique que l'argent attend d'être récupéré. Il suffit de saisir les coordonnées de votre carte bancaire.

Pendant un instant, vous vous demandez pourquoi votre carte est nécessaire alors que c'est vous qui devez recevoir de l'argent. Mais l'acheteur répond rapidement, poliment et avec assurance. Il explique que c'est ainsi que fonctionne le nouveau système de paiement. Il ajoute qu'il l'a déjà utilisé de nombreuses fois. Pour finir, il vous rappelle que le transporteur ne devrait pas tarder et qu'il vaut donc mieux tout régler immédiatement.

Vous venez de vous retrouver dans une situation où le déroulement de la transaction ne dépend plus vraiment de la machine à café. Le produit le plus important est désormais votre attention.

Pourquoi est-il si facile de confondre intérêt et fiabilité ?

Lorsque nous vendons quelque chose sur Internet, nous nous attendons à un scénario bien précis. Quelqu'un remarque notre annonce, pose des questions, nous convenons des conditions, puis viennent le paiement et la remise de l'objet. Si l'acheteur se montre poli et affirme être prêt à payer, nous l'intégrons automatiquement à ce scénario. Notre cerveau n'analyse pas chaque message comme une pièce à conviction dans une affaire pénale. Il s'appuie sur nos expériences passées, reconnaît des situations familières et cherche à économiser de l'énergie. Si nous traitions chaque conversation quotidienne comme un interrogatoire de suspect, faire ses courses prendrait plus de temps que rénover un appartement.

Les escrocs exploitent cette tendance naturelle à simplifier la réalité. Leurs messages commencent souvent exactement comme devraient commencer de véritables conversations. Ils demandent si l'objet est toujours disponible, confirment leur intérêt et proposent un paiement ainsi qu'une livraison. Ce n'est que plus tard qu'apparaît l'élément qui change la nature de la transaction : un lien inhabituel, une demande de données personnelles, des frais supplémentaires ou l'obligation d'autoriser une opération.

Il est important de comprendre qu'une escroquerie sur Internet repose rarement sur un seul énorme mensonge. Bien plus souvent, elle consiste en une succession de petites étapes, dont chacune semble découler logiquement de la précédente. Vous acceptez d'abord de vendre l'objet.

Ensuite, vous acceptez l'expédition. Puis, vous consentez à vérifier certaines informations. À la fin, on peut vous demander d'effectuer une opération que vous n'auriez jamais acceptée si elle avait été présentée dès le début de la conversation.

C'est un peu comme si quelqu'un venait examiner votre réfrigérateur et parvenait, dix minutes plus tard, à vous convaincre que son achat nécessite impérativement un accès à votre compte bancaire. S'il avait commencé par cette proposition, vous lui auriez probablement fermé la porte au nez. Pourtant, une histoire présentée avec suffisamment d'habileté peut transformer une absurdité en procédure apparemment normale.

Les trois côtés d'une même transaction

Une petite annonce classique implique au moins deux personnes : le vendeur et l'acheteur. Souvent, une plateforme de petites annonces, un prestataire de services de paiement ou une société de livraison intervient également. Chacun de ces participants possède un rôle précis. Le vendeur propose un objet, l'acheteur le paie, et les autres intervenants peuvent faciliter le paiement, la communication ou la livraison.

Le problème commence lorsqu'une seule personne essaie d'endosser tous les autres rôles.

Imaginez un acheteur qui vous envoie lui-même un lien vers un prétendu système de paiement, qui vous en explique lui-même le fonctionnement, qui vous assure lui-même que tout est sécurisé et qui vous informe lui-même que tout a été validé. Toutes les informations concernant la transaction proviennent d'une seule source. Vous ne disposez d'aucune confirmation indépendante, mais vous pouvez malgré tout

avoir l'impression de participer à un processus contrôlé par plusieurs institutions professionnelles.

C'est l'un des pièges les plus importants : confondre une information communiquée par votre interlocuteur avec une information confirmée par un système indépendant.

Si quelqu'un écrit qu'il a payé, cela ne signifie pas nécessairement que l'argent a effectivement été transféré. S'il vous envoie une capture d'écran d'un justificatif de virement, vous ne pouvez pas être certain que le document est authentique ni que l'opération a été correctement finalisée. Si vous recevez un message ressemblant à une notification de la plateforme, vous devriez le vérifier directement sur le site officiel ou dans l'application officielle, que vous aurez ouverts vous-même.

Une capture d'écran reste une image. Elle peut représenter la réalité, mais elle peut aussi représenter une réalité qui n'a jamais existé. De la même manière, la photographie d'un homme debout à côté d'une voiture de luxe ne prouve pas qu'il en est propriétaire. Peut-être a-t-il simplement demandé au véritable propriétaire de s'éloigner un instant du capot.

Les signaux d'alarme ne sont pas toujours rouges

Beaucoup de personnes s'attendent à ce qu'un message suspect ait une apparence suspecte. Les fautes de langue, les caractères étranges, un numéro de téléphone étranger ou des formulations artificielles peuvent effectivement constituer des signaux d'alerte. Il ne faut cependant pas s'accrocher à l'image de l'escroc maladroit, qui rédige des messages si bancals que même le correcteur automatique refuse de collaborer.

Les messages actuels peuvent être parfaitement rédigés, polis et adaptés à l'objet proposé. Un escroc peut répondre à vos questions, mentionner la ville dans laquelle vous habitez et même reprendre des détails figurant dans votre annonce. Cela ne prouve pas son honnêteté. Cela signifie simplement que quelqu'un a lu votre offre ou utilisé les informations que vous avez vous-même rendues publiques.

Voilà pourquoi il est plus utile d'examiner le sens des demandes de votre interlocuteur que de juger son style. Sa demande découle-t-elle réellement de la transaction convenue ? L'opération demandée est-elle indispensable ? Pouvez-vous l'effectuer sur le site officiel plutôt qu'en utilisant le lien reçu ? Comprenez-vous exactement ce qui se passera lorsque vous donnerez votre autorisation ?

Dans le cadre d'une vente, une demande visant à obtenir toutes les coordonnées de votre carte bancaire, son code CVV/CVC, des codes d'autorisation ou vos identifiants de connexion à la banque, uniquement pour recevoir un paiement, est particulièrement inquiétante. Un virement classique vers votre compte bancaire ne nécessite pas de communiquer ces informations à l'acheteur. Les systèmes de paiement officiels peuvent posséder leurs propres procédures, mais vous devriez les découvrir dans une application ou sur un site de confiance, et non en suivant les instructions d'un inconnu.

Cela ne signifie pas que toute demande inhabituelle constitue automatiquement la preuve d'une infraction. Il arrive qu'une personne ne connaisse réellement pas les règles d'une plateforme, utilise une autre méthode de livraison ou explique simplement ses intentions de manière maladroite. La différence apparaît dans sa réaction lorsque vous essayez de vérifier tranquillement les informations. Un

acheteur honnête peut s'impatienter, mais il ne devrait pas exiger que vous révéliez des données confidentielles ou que vous autorisiez une opération que vous ne comprenez pas.

La confiance n'est pas un abonnement illimité

Les gens abordent souvent les transactions de manière binaire. Soit ils font confiance à quelqu'un, soit ils le considèrent comme suspect. Pourtant, la confiance peut être accordée progressivement, et uniquement dans les limites réellement nécessaires.

Vous pouvez faire suffisamment confiance à votre interlocuteur pour répondre à une question concernant l'état de l'objet. Vous pouvez convenir d'une date de récupération et d'un moyen de paiement. Cela ne vous oblige absolument pas à lui transmettre des informations concernant votre carte bancaire, l'historique de votre compte ou les codes reçus de votre banque. Le fait qu'une première opération se soit correctement déroulée ne donne à personne le droit d'exiger toutes les suivantes.

Supposons que vous vendiez un appareil photo d'occasion. L'acheteur demande une photographie supplémentaire montrant la référence du modèle et l'objectif. C'est une demande compréhensible, même s'il convient de faire attention aux documents et autres informations privées qui pourraient apparaître à l'arrière-plan. Ensuite, votre interlocuteur vous demande si vous pouvez expédier le colis. Cela reste également dans le cadre normal de la transaction. Ce n'est que lorsqu'il exige que vous vous connectiez à votre banque par l'intermédiaire d'une page indiquée dans son message que vous franchissez une limite qui n'a aucune justification dans la vente de cet appareil photo.

La frontière de la sécurité ne passe donc pas entre le fait de parler à un inconnu et le silence absolu. Elle se situe entre les informations nécessaires à la transaction et l'accès à votre argent et à vos comptes.

Retenez cette règle simple : accepter une chose ne signifie pas accepter tout ce que votre interlocuteur pourra imaginer ensuite.

La première minute de bon sens

Au début d'une transaction, la compétence la plus utile consiste à savoir s'arrêter lorsque quelqu'un en modifie soudainement les règles. Vous n'avez besoin d'aucune connaissance spécialisée pour remarquer que vous aviez prévu de vendre un objet et que la conversation porte désormais, de façon inattendue, sur vos données bancaires.

Vous pouvez effectuer une vérification rapide en vous posant quatre questions :

1. Qu'est-ce que je vends ou achète exactement, et quelles conditions avons-nous déjà convenues ?
2. Quelle nouvelle opération mon interlocuteur exige-t-il, et pourquoi ?
3. Puis-je vérifier moi-même la nécessité de cette opération auprès d'une source officielle ?
4. Qu'est-ce que je risque si je l'effectue sans vérification ?

Ces questions sont particulièrement pertinentes lorsque votre interlocuteur essaie de précipiter votre décision. Vous n'avez pas besoin de mener une enquête de plusieurs heures pour y répondre. Il suffit d'interrompre la conversation, d'ouvrir l'application officielle et de vérifier si la transaction mentionnée ou l'opération demandée existe réellement.

Si le message indique qu'un paiement attend d'être récupéré, mais que vous ne voyez aucune opération correspondante dans le système officiel, n'essayez pas de résoudre la situation en suivant de nouvelles instructions de l'acheteur. Commencez par déterminer si la notification est authentique.

Il est possible que l'acheteur proteste. Il peut écrire qu'il n'a pas le temps, qu'il a déjà payé et que votre comportement complique inutilement une affaire très simple. Dans ce cas, une réponse calme suffit : « Je réaliserai la transaction uniquement par l'intermédiaire du système officiel. Je n'ouvre pas de liens externes pour confirmer les paiements. »

Vous n'avez pas besoin de justifier cette décision pendant quinze messages. Une vente sécurisée n'est pas un concours destiné à récompenser l'argumentation la plus convaincante.

Quand il y a une véritable personne de l'autre côté

Il faut ici apporter une précision importante. Une méfiance excessive peut compliquer les transactions normales. Tous les acheteurs qui répondent rapidement ne sont pas des escrocs. Tous ceux qui ne négocient pas le prix ne préparent pas une fraude. Certaines personnes ont réellement besoin d'une commode d'occasion, savent combien elles souhaitent payer et n'ont aucune envie de participer à des négociations ressemblant à des débats parlementaires.

L'objectif n'est pas de dresser une liste de traits de personnalité permettant d'identifier un criminel. Une telle liste serait peu fiable. Il est bien plus important d'observer

les comportements concrets concernant l'argent, les informations et le contrôle de la transaction.

La remise en main propre en constitue un bon exemple. Un acheteur peut demander à examiner l'objet et proposer de payer lors de la récupération. Il n'y a là rien d'inhabituel. De son côté, le vendeur peut convenir d'un lieu de rendez-vous, demander de la ponctualité et préciser clairement les conditions. Dans ce cas, la prudence consiste à choisir un endroit raisonnable, à protéger sa vie privée et à s'assurer que le paiement a réellement été effectué avant de remettre l'objet.

Si quelqu'un paie en espèces, vous pouvez tranquillement vérifier le montant reçu. En cas de virement, il faut vérifier que le compte a effectivement été crédité, sans se fier uniquement à un message ou à une image présentée comme une preuve de paiement. Lorsqu'un système officiel de paiement et de protection des transactions est utilisé, il convient de respecter ses règles en vigueur et de vérifier le statut de l'opération depuis son propre compte.

Ces précautions ne signifient pas que vous accusez l'autre partie de malhonnêteté. Elles font simplement partie d'un échange responsable.

Au restaurant, vous n'insultez pas le serveur lorsque vous vérifiez l'addition. De la même manière, un acheteur ne devrait pas se sentir offensé simplement parce que vous vérifiez son paiement. Évidemment, vous pouvez aussi effectuer cette vérification avec l'expression grave d'un enquêteur venant de découvrir un scandale international concernant la vente d'une lampe de chevet d'occasion. Dans ce cas, l'atmosphère risque effectivement de devenir un peu tendue.

La différence essentielle

Dans une transaction honnête, les deux parties poursuivent le même objectif : échanger un objet contre le paiement convenu. Il peut y avoir des questions, des négociations et des complications pratiques, mais le but principal reste clair.

Dans une escroquerie, l'objet devient souvent un simple prétexte pour vous amener à effectuer une autre opération. L'escroc peut ne vouloir ni acheter ni vendre quoi que ce soit. Ce qui l'intéresse, ce sont vos données, votre argent, l'accès à votre compte ou l'autorisation d'une opération. Voilà pourquoi il est important d'observer non seulement ce que votre interlocuteur raconte, mais également l'action vers laquelle il vous conduit avec insistance.

Si une conversation concernant une machine à café d'occasion parle de moins en moins de la machine et de plus en plus de votre banque, quelque chose a clairement changé de direction.

La prochaine fois que vous recevrez un message d'un acheteur particulièrement déterminé, vous n'aurez pas besoin d'imaginer immédiatement le pire. Vous pourrez répondre, convenir des détails et poursuivre tranquillement la vente. Mais conservez toujours le droit de vérifier par vous-même toute opération concernant votre argent ou vos informations confidentielles.

Un bon acheteur veut conclure la transaction. Un escroc veut que vous cessiez de poser des questions.

Et c'est précisément pour cette raison que quelques questions raisonnables peuvent avoir davantage de valeur que le filtre antispam le plus sophistiqué.

# Chapitre 2 - Pourquoi un escroc paraît-il plus crédible que votre propre bon sens ?

Il est 21 h 43. Vous êtes assis sur votre canapé, vous parcourez vos messages et vous vous demandez si cela vaut encore la peine de préparer du thé alors que vous devriez bientôt aller dormir. Soudain, votre téléphone signale une nouvelle notification. Quelqu'un souhaite acheter votre téléphone d'occasion. Le prix est fixé à huit cents zlotys, et la personne intéressée affirme vouloir payer immédiatement.

Normalement, vous liriez le message, répondriez et reprendriez vos occupations. Mais cette fois, la conversation s'accélère. L'acheteur explique qu'il a besoin d'une expédition rapide parce que le téléphone est destiné à être offert en cadeau. Il affirme que le paiement a déjà été effectué, mais que le système exige une confirmation supplémentaire. Quelques instants plus tard, il envoie une capture d'écran, puis vous rappelle que la transaction risque d'être annulée si vous ne terminez pas la procédure dans les minutes qui suivent.

Vous n'êtes pas particulièrement naïf. Vous savez utiliser Internet et vous n'avez aucune intention de distribuer votre argent à des inconnus. Pourtant, vous commencez à agir plus rapidement que vous ne prenez habituellement vos décisions.

Pourquoi ?

Parce que l'escroc ne cherche pas seulement à vous convaincre avec des arguments. Il essaie de modifier les conditions dans lesquelles vous prenez votre décision.

L'urgence modifie notre façon de réfléchir

Imaginez deux situations. Dans la première, quelqu'un vous demande si vous accepteriez de saisir les coordonnées de votre carte bancaire sur un site que vous ne connaissez pas pour recevoir l'argent de la vente d'un téléphone. Vous avez le temps de réfléchir. Vous trouverez probablement cette proposition suspecte.

Dans la seconde situation, on vous informe que l'acheteur a déjà payé, que le transporteur attend une confirmation et que le système clôturera la transaction dans cinq minutes. Vous n'analysez plus calmement le sens de toute la procédure. Vous cherchez surtout à savoir comment éviter de perdre la vente.

C'est une différence fondamentale. Le sentiment d'urgence peut déplacer votre attention de la question « Est-ce sécurisé ? » vers la question « Est-ce que je vais avoir le temps ? ».

Les escrocs comprennent parfaitement l'intérêt de ce changement. Voilà pourquoi ils utilisent des messages laissant entendre que l'offre va bientôt disparaître, que le paiement sera annulé ou que la possibilité de récupérer l'argent va expirer. Ils n'emploient pas toujours des menaces directes. Parfois, un rappel poli suffit : « Merci de confirmer rapidement, car je ne peux pas attendre plus longtemps. »

Dans une véritable transaction, il peut aussi exister des contraintes de temps. Un acheteur peut n'avoir qu'une seule soirée de libre, tandis qu'un vendeur peut avoir besoin d'une décision rapide. La précipitation, à elle seule, ne prouve donc pas l'existence d'une escroquerie. Elle devient particulièrement dangereuse lorsqu'une personne s'en sert pour vous imposer une opération que vous ne comprenez

pas ou que vous ne pouvez pas vérifier de manière indépendante.

La réponse la plus simple est la suivante : ne laissez pas l'échéance imposée par quelqu'un d'autre remplacer votre propre évaluation de la sécurité.

Si une transaction exige une opération financière que vous ne connaissez pas, arrêtez-vous. Même si votre interlocuteur affirme qu'il ne reste que trois minutes. Perdre une occasion de vendre un téléphone d'occasion est moins grave que perdre l'argent présent sur votre compte bancaire.

D'ailleurs, une transaction honnête qui ne peut pas supporter les quelques minutes nécessaires à une vérification mérite probablement, de toute façon, un examen plus attentif.

Une autorité que personne n'a vérifiée

Une autre manière de gagner votre confiance consiste à invoquer des institutions. L'escroc ne parle plus uniquement en son propre nom. Il prétend représenter la plateforme de petites annonces, le service des paiements, une société de livraison ou une banque. Il utilise des noms, des logos et un vocabulaire qui donnent l'impression d'une procédure officielle.

Les gens ont généralement tendance à prendre les communications institutionnelles plus au sérieux que les messages provenant d'inconnus. C'est compréhensible. Une banque peut réellement envoyer des informations importantes, une plateforme peut exiger certaines opérations et un transporteur peut parfois avoir besoin de renseignements supplémentaires pour livrer un colis.

Le problème, c'est que le simple fait de déclarer représenter une institution ne confirme absolument pas l'identité de l'expéditeur.

Un message signé « Service de sécurité » ne devient pas automatiquement sûr. Le logo d'une entreprise peut être copié. Le nom de l'expéditeur peut être trompeur, tout comme le numéro de téléphone affiché à l'écran. Même le fait de connaître correctement votre prénom et les détails de votre annonce ne prouve pas que vous êtes en contact avec un employé autorisé.

Un escroc peut écrire : « Conformément à la procédure du prestataire de services de paiement, une vérification d'identité est obligatoire. » Cela semble sérieux. Surtout si la phrase s'accompagne d'informations concernant la sécurité de la transaction, d'un numéro de dossier et de l'assurance que toutes les opérations demandées sont parfaitement habituelles.

Mais un vocabulaire professionnel ne prouve pas que le message provient d'un professionnel. Il est tout à fait possible de décrire une opération absurde avec beaucoup d'élégance. La phrase « Afin de finaliser le transfert des fonds, nous vous prions d'autoriser le débit de votre compte » peut toujours signifier que quelqu'un cherche à vous prendre de l'argent. Habiller une demande malhonnête d'un beau costume ne change pas sa nature.

C'est pourquoi l'authenticité d'un message doit être vérifiée en dehors du canal indiqué par votre interlocuteur suspect. Si quelqu'un prétend représenter une plateforme, ouvrez vous-même son application officielle. S'il affirme travailler pour une banque, mettez fin à la conversation et contactez l'établissement à l'aide d'un numéro ou d'une application que vous connaissez grâce à une source fiable.