Résous ton problème avec un clin d'œil

Le monsieur de la banque connaît mon nom et a beaucoup trop de temps libre

Comment reconnaître un faux appel de votre banque et vérifier vous-même l'identité de votre interlocuteur



Max Paradox

Le monsieur de la banque connaît mon nom et a beaucoup trop de temps libre

Comment reconnaître un faux appel de votre banque et vérifier vous-même l'identité de votre interlocuteur

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384905746

ALL-IN Rafał Płonkowski



TABLE DES MATIÈRES

INTRO 5

Chapitre 1 - Bonjour, je vous appelle de votre banque. Du moins, c'est ce que je prétends 12

Chapitre 2 - Comment sait-il tout cela ? Anatomie d'une confiance accordée à crédit 22

Chapitre 3 - Votre argent disparaîtra dans cinq minutes, ou comment un escroc vous vole votre temps avant de vous voler quoi que ce soit d'autre 33

Chapitre 4 - Trois mots magiques : « Je m'y connais ». Pourquoi les fausses protections échouent 43

Chapitre 5 - Excusez-moi de ne pas me laisser escroquer. Le piège de l'excès de politesse 55

Chapitre 6 - Veuillez cliquer ici. La technologie qui devait nous aider et qui s'est mise à donner des ordres 66

Chapitre 7 - Encore une dernière étape. Pourquoi est-il si difficile d'interrompre une procédure déjà commencée ? 76

Chapitre 8 - Quand l'escroc revêt l'uniforme de l'autorité. Pourquoi un titre professionnel ne remplace pas une preuve 85

Chapitre 9 - Raccrochez, mais faites-le intelligemment. L'art de reprendre le contrôle de votre téléphone 94

Chapitre 10 - Vérifiez auprès de la banque, pas auprès de l'histoire qu'on vous raconte. Comment réellement contrôler l'identité de votre interlocuteur 104

Chapitre 11 - Vous avez reçu un code, donc tout va bien ? Comment lire les messages de votre banque avant qu'il ne soit trop tard 114

Chapitre 12 - J'ai déjà donné le code. Et maintenant ? Les premiers secours pour votre compte, sans panique ni autoflagellation.....125

Chapitre 13 - Un appel de la banque passé au crible. Comment vérifier une histoire suspecte sans devenir détective.....137

Chapitre 14 - Votre centre de sécurité à domicile. Préparez-vous avant que le monsieur chargé de sauver vos économies ne vous appelle 147

Chapitre 15 - La banque ne répond pas, le téléphone fait des siennes et l'escroc est de très bonne humeur. Que faire quand le plan idéal tombe à l'eau ?.....158

Chapitre 16 - L'argent est parti et le monsieur de la banque a disparu. Comment reprendre les choses en main après une escroquerie 169

Chapitre 17 - Ce n'est pas mon compte, mais c'est mon problème. Comment aider un proche qui parle à un escroc.....180

Chapitre 18 - Une bonne habitude plutôt qu'une méfiance quotidienne. Comment rester vigilant sans vivre en état d'alerte.....190

Chapitre 19 - Ils rappellent. Comment reconnaître une menace qui revient avant qu'elle ne s'empare à nouveau de votre attention.....200

Chapitre 20 - Le monsieur de la banque peut attendre. Votre argent, vos règles 211

INTRO

Le téléphone sonne à 14 h 37. Le numéro vous semble familier, il ressemble peut-être même à celui qui figure sur le site officiel de votre banque. Vous décrochez, parce que vous êtes une personne responsable, après tout. À l'autre bout du fil, un homme courtois se présente comme un employé du service de sécurité, vous appelle par votre prénom et votre nom, puis vous annonce qu'une tentative de virement suspecte vient d'être détectée sur votre compte. Cela paraît sérieux. Très sérieux. D'autant plus que ce monsieur parle avec calme, professionnalisme et une assurance telle qu'on pourrait croire qu'il vient personnellement de sauver le système financier mondial et qu'il a encore trouvé cinq minutes pour sauver vos économies.

Le problème, c'est que vous n'avez absolument aucune idée de qui il est réellement.

Ce monsieur connaît votre nom. Il sait dans quelle banque vous avez un compte. Il peut citer la ville où vous habitez et parfois même une partie de votre numéro de compte. Tout correspond. Votre cerveau commence donc à effectuer une opération assez risquée : transformer la connaissance de quelques informations en preuve de la fiabilité de votre interlocuteur. Pourtant, votre prénom, votre nom ou votre numéro de téléphone ne sont pas des formules magiques réservées exclusivement aux employés de banque. Ces informations ont pu tomber entre de mauvaises mains par différentes voies. Quant au numéro affiché sur votre écran ? Malheureusement, lui non plus ne dit pas toujours la vérité. Une technique d'usurpation de numéro, appelée spoofing,

permet de faire apparaître sur votre téléphone un numéro qui ne correspond pas à l'origine réelle de l'appel.

Et c'est précisément pour cela que ce livre existe. Pas pour que, dès demain, vous répondiez à chaque appel par : « Veuillez me communiquer le nom de jeune fille du président de la banque ainsi que le troisième chiffre de la pointure du directeur de l'agence. » Même si, je dois l'admettre, ce serait une méthode intéressante pour décourager les télévendeurs. L'objectif est beaucoup plus pratique : apprendre à reconnaître les situations dans lesquelles quelqu'un tente d'exploiter votre confiance et à vérifier l'identité de votre interlocuteur sans suivre les instructions de la personne que vous cherchez justement à identifier.

Car c'est là que se cache la plus grande absurdité de toute cette histoire. Un inconnu vous appelle, affirme travailler pour votre banque et, lorsque vous lui demandez de confirmer son identité, vous propose de le croire sur parole. Éventuellement, il peut aussi vous passer son supérieur hiérarchique. Ce supérieur existe, bien entendu, du moins dans le cadre de cette conversation. Il est peut-être assis sur la chaise d'à côté, possède le même téléphone et vient d'être promu responsable du service de sécurité grâce à son impressionnante capacité à modifier le ton de sa voix.

Les escroqueries téléphoniques ne commencent pas toujours par un mensonge maladroit. Elles ressemblent souvent à une procédure préparée avec un grand professionnalisme. Votre interlocuteur peut employer les bons termes, connaître les principes fondamentaux des opérations bancaires et savoir parfaitement quels messages vous vous attendez à recevoir d'un établissement financier.

Il peut même vous mettre en garde contre les escrocs, ce qui constitue une manœuvre particulièrement culottée, mais malheureusement très utile pour lui. Lorsqu'une personne vous affirme qu'elle vous protège des criminels, vous avez naturellement envie de la considérer comme quelqu'un qui se trouve du bon côté. Sauf qu'affirmer que l'on vous protège ne signifie pas encore que l'on vous protège réellement. Un pompier coiffé d'un casque en plastique peut lui aussi crier « Au feu ! », mais avant de lui confier les clés de votre appartement, mieux vaut vérifier qu'il est effectivement arrivé dans un camion de pompiers.

L'arme la plus importante de l'escroc n'est d'ailleurs pas toujours la technologie, mais la pression psychologique. On vous annonce que votre argent est sur le point de disparaître, qu'il faut agir immédiatement, que vous ne devez surtout pas raccrocher et que consulter quelqu'un d'autre pourrait compromettre la sécurité de votre compte. Chaque nouvelle phrase réduit un peu plus l'espace disponible pour réfléchir tranquillement. Il n'est pas nécessaire d'être naïf pour ressentir une telle tension. Il suffit d'avoir des économies, des factures à payer et de ne pas particulièrement apprécier l'idée que quelqu'un puisse s'acheter une télévision avec votre argent. L'escroc n'a pas besoin de vous convaincre de tout accepter d'un seul coup. Il lui suffit d'obtenir votre accord pour une première étape apparemment anodine, puis d'exploiter votre implication dans la suite de la conversation.

Vous pensez peut-être que vous ne tomberiez jamais dans le panneau. C'est une conviction très agréable. Malheureusement, l'escroc ne vous fait pas passer un examen d'intelligence. Il recherche le moment où vous êtes occupé, fatigué, inquiet ou simplement persuadé de parler à

la bonne personne. Quelqu'un peut parfaitement connaître les règles de sécurité et malgré tout commettre une erreur lorsqu'il entend, à l'autre bout du fil, un avertissement dramatique concernant son propre argent. Voilà pourquoi, plutôt que de cultiver un sentiment d'invincibilité, il vaut mieux adopter une façon de procéder simple, qui fonctionne même lorsque votre concentration a décidé de prendre sa pause déjeuner.

Dans ce livre, vous apprendrez à distinguer les informations qui semblent crédibles de celles qui constituent véritablement une confirmation. Vous découvrirez comment reconnaître les tentatives classiques de mise sous pression, pourquoi un numéro familier affiché sur votre écran ne garantit pas votre sécurité et quelle importance accorder aux demandes de codes, de mots de passe, d'installation d'applications ou d'exécution de virements. Mais surtout, vous découvrirez un principe qui permet de reprendre le contrôle de la conversation : c'est vous qui choisissez un moyen indépendant de contacter votre banque, au lieu de rester sur le canal de communication choisi par un inconnu.

Imaginez que l'on vous annonce une transaction suspecte particulièrement inquiétante. Au lieu d'engager une discussion, vous mettez fin à l'appel. Ensuite, vous ouvrez vous-même l'application officielle de votre banque ou utilisez le numéro trouvé sur son véritable site Internet ou sur votre carte bancaire. Vous contactez votre établissement indépendamment de votre précédent interlocuteur et demandez si un problème nécessite réellement une intervention. Vous ne composez pas le numéro dicté par la personne qui vous a appelé, vous ne cliquez pas sur le lien qu'elle vous a envoyé et vous ne considérez pas un nouvel appel de sa part comme une vérification. Ce n'est pas une

spectaculaire technique de contre-espionnage. Vous n'avez besoin ni d'une oreillette, ni de lunettes noires, ni du nom de code « Opération Compte à terme ». Vous avez simplement besoin d'une règle que vous pouvez appliquer même sous pression.

Bien entendu, les situations réelles sont parfois plus compliquées qu'un exemple soigneusement présenté. Que faire lorsque votre interlocuteur connaît les détails de votre compte ? Lorsqu'il affirme que raccrocher entraînera la perte de votre argent ? Lorsqu'il vous demande de confirmer une opération dans l'application, alors qu'il assurait quelques instants plus tôt vouloir justement la bloquer ? Et si vous avez déjà communiqué certaines informations ou suivi une instruction avant de commencer à trouver la situation suspecte ? Dans ces moments-là, vous n'avez pas besoin de culpabiliser, mais de disposer d'un ordre d'actions clair et compréhensible. Toutes les erreurs n'entraînent pas une perte d'argent, mais certaines exigent de contacter immédiatement la banque et de sécuriser l'accès au compte. Attendre par peur de se ridiculiser peut coûter plus cher que l'erreur elle-même.

Nous n'allons pas non plus prétendre que tous les appels provenant d'une banque sont des escroqueries. Les banques contactent réellement leurs clients, y compris pour des questions de sécurité. L'objectif n'est donc pas de transformer une prudence raisonnable en méfiance systématique envers toute personne possédant un téléphone. Il s'agit de distinguer deux choses : écouter une information et exécuter une instruction. Vous pouvez prendre un avertissement au sérieux sans accepter automatiquement l'identité de la personne qui vous le transmet. Vous pouvez rester poli sans divulguer vos

données. Vous pouvez mettre fin à une conversation sans demander la permission. Et surtout, vous pouvez vérifier la situation par vous-même, même si votre interlocuteur s'efforce de vous convaincre que c'est absolument impossible.

Ce dernier point est d'ailleurs particulièrement amusant. L'établissement auquel vous avez confié votre argent serait donc censé vous interdire de le contacter par ses propres canaux officiels. Cela ressemble à un restaurant qui vous avertirait que consulter son adresse sur son site Internet provoquerait l'explosion de la cuisine. Si quelqu'un cherche obstinément à vous empêcher d'effectuer une vérification indépendante, vous n'avez pas besoin de déterminer s'il s'agit d'un escroc pour cesser de suivre ses instructions. Il suffit de constater que vous n'avez aucune confirmation de l'identité de votre interlocuteur.

Je ne vous promets pas qu'après avoir lu ce livre, plus aucun criminel ne réussira jamais à vous surprendre. Les méthodes d'escroquerie évoluent, et même les personnes raisonnables peuvent commettre des erreurs. En revanche, il est possible d'apprendre à réagir de manière à ce qu'un simple appel téléphonique ne vous prive pas de votre capacité à prendre vos propres décisions. Au lieu d'essayer de mémoriser tous les scénarios imaginables, vous développerez l'habitude de vérifier l'origine des informations, de reconnaître les manipulations et d'interrompre les actions dont vous ne comprenez pas les conséquences.

Et lorsque, la prochaine fois, vous recevrez l'appel d'un monsieur de la banque qui connaît votre prénom, votre nom et dispose manifestement d'un temps illimité pour sauver votre patrimoine, vous n'aurez pas besoin de deviner s'il

s’agit d’un héros ou d’un individu ayant une conception particulièrement souple de la propriété d’autrui. Vous le remercierez pour l’information, mettrez fin à la conversation et vérifierez vous-même la situation auprès de la bonne source.

Ce monsieur connaît peut-être votre nom. Cela ne signifie pas qu’il doit avoir le dernier mot.

Chapitre 1 - Bonjour, je vous appelle de votre banque. Du moins, c'est ce que je prétends

Ce qu'il y a de plus inquiétant dans une escroquerie téléphonique, c'est que son commencement peut être parfaitement banal. Aucun rire diabolique, aucune musique dramatique, aucune voix d'homme qui rêvait depuis l'enfance de faire carrière dans le crime. Juste un appel ordinaire, une salutation polie et une phrase prononcée sur le ton de quelqu'un qui règle ce genre de problème tous les jours. Si l'on évaluait un interlocuteur uniquement sur ses bonnes manières, plus d'un escroc obtiendrait une excellente appréciation et se verrait même proposer d'animer une formation sur la relation client. Malheureusement, la courtoisie n'est pas un certificat d'honnêteté, et une voix professionnelle ne prouve pas que la personne travaille dans une banque.

Imaginez Marta, qui vient de rentrer des courses. Elle essaie de vider ses sacs, de trouver une place pour des produits qu'elle n'avait absolument pas prévu d'acheter et, en même temps, de convaincre les membres de sa famille que les yaourts doivent être rangés au réfrigérateur, et non faire l'objet de négociations interminables. C'est alors que son téléphone sonne. Un homme se présente comme Adam Kowalski, du service de sécurité de sa banque, et l'informe d'une tentative de transaction non autorisée. Il cite le nom de la banque, le prénom de Marta et les derniers chiffres de son numéro de téléphone. Puis il lui demande si elle vient d'essayer d'effectuer un virement. Marta répond que non. Son interlocuteur déclare aussitôt que c'est précisément ce

qu'il craignait. Son ton devient plus grave, tout en restant parfaitement courtois. L'ensemble paraît si crédible que Marta abandonne ses courses, oubliant même les glaces qui commencent leur transformation irréversible en soupe sucrée.

Dans cette courte scène, il s'est produit quelque chose de plus important qu'un simple échange d'informations. L'interlocuteur a pris le contrôle de l'attention de Marta. Quelques instants auparavant, elle décidait encore de ce qu'elle allait faire de son après-midi. Désormais, un inconnu fixe ses priorités, décrit une menace et laisse entendre que seule sa coopération permettra d'éviter des pertes financières. C'est l'une des raisons pour lesquelles les faux appels bancaires peuvent se révéler efficaces. L'escroc n'a pas besoin de réclamer de l'argent immédiatement. Il doit d'abord se faire une place dans votre esprit, de préférence dans la partie réservée aux urgences.

Quand la conversation se déroule exactement comme prévu

Beaucoup de gens imaginent l'escroc comme un individu qui parle nerveusement, confond les noms des établissements et propose une phrase sur deux de transférer de l'argent sur le compte de son cousin. De tels interlocuteurs existent peut-être, mais fonder sa sécurité sur l'espoir de repérer des erreurs évidentes est risqué. Un criminel bien préparé sait imiter la manière dont les véritables conseillers bancaires conduisent leurs conversations. Il emploie des formules officielles, annonce sa fonction, peut communiquer un matricule professionnel et utiliser le vocabulaire des procédures. Parfois, on entend à l'arrière-plan d'autres conversations qui évoquent l'activité d'un grand centre d'appels. Pourtant, cette impression

d'organisation ne prouve absolument pas que l'appel provient de la banque.

Il est essentiel de comprendre la différence entre une information communiquée par votre interlocuteur et une information confirmée de manière indépendante. Lorsqu'une personne déclare : « Je m'appelle Adam Kowalski et je suis conseiller principal en sécurité », vous apprenez uniquement la manière dont elle souhaite être présentée. Si elle vous donne son matricule, vous restez face à une information provenant de la même source. Vous pouvez bien entendu noter son nom et son identifiant, mais il ne faut pas les considérer comme un laissez-passer donnant automatiquement droit à votre confiance. Sinon, il suffirait d'acheter un élégant carnet, de mémoriser quelques expressions bancaires et de s'autoproclamer directeur de la sécurité de toute la galaxie.

Un véritable conseiller peut connaître les données d'un client parce qu'il utilise les systèmes informatiques de la banque. Un escroc peut également posséder certaines de ces informations, obtenues de différentes façons. Par conséquent, la correspondance d'un nom, d'une adresse ou de quelques renseignements élémentaires ne suffit pas. Ce qui compte davantage, c'est ce que votre interlocuteur attend de vous et s'il vous laisse vérifier tranquillement la situation par un canal officiel indépendant. Les demandes visant à obtenir un mot de passe, un code d'autorisation, un code PIN, à installer un logiciel inconnu ou à valider des opérations que vous n'avez pas initiées sont particulièrement préoccupantes. Face à de telles instructions, il faut interrompre toute action, aussi convaincante que puisse paraître la menace annoncée.

Une véritable banque peut vous appeler pour une question de sécurité. Cela ne signifie pas pour autant que vous êtes obligé de poursuivre chaque conversation jusqu'à ce que la personne qui vous appelle décide qu'elle est terminée. Vous avez parfaitement le droit d'indiquer que vous contacterez vous-même l'établissement. Vous n'avez pas à convaincre votre interlocuteur du bien-fondé de votre décision ni à expliquer en détail pourquoi vous ne lui faites pas confiance. Une conversation téléphonique n'est pas une audience judiciaire, et vous n'avez aucun dossier de preuves à présenter avant de raccrocher.

Premier piège : confondre politesse et obligation

Revenons à Marta. Le faux conseiller lui pose plusieurs questions supplémentaires. D'abord des questions simples, auxquelles il est facile de répondre. Possède-t-elle un compte dans cette banque ? Utilise-t-elle l'application mobile ? A-t-elle récemment effectué un virement vers un bénéficiaire inconnu ? Chaque réponse rend la conversation plus naturelle. Marta a l'impression de participer à une procédure habituelle. Elle commence également à ressentir une obligation discrète de coopérer, car quelqu'un consacre tout de même du temps à l'aider dans une situation dangereuse.

C'est ainsi que fonctionne le mécanisme d'engagement progressif. L'interlocuteur n'a pas besoin de commencer par une demande qui provoquerait immédiatement un refus. Il peut d'abord obtenir une série de réponses, puis passer à des instructions de plus en plus exigeantes. Bien entendu, avoir répondu à quelques questions neutres ne signifie pas que vous perdez ensuite le droit de refuser. Le problème apparaît lorsqu'une personne commence à considérer sa coopération précédente comme un engagement à

poursuivre. Puisqu'elle a déjà répondu à tant de questions, mettre fin à la conversation lui paraît impoli, voire irrationnel.

Cette illusion mérite d'être dissipée avant même qu'une telle situation se présente. Vous pouvez interrompre une conversation après la première phrase, après la cinquième question ou au bout de dix minutes. Aucune règle ne prévoit que le temps consacré à un inconnu vous oblige à lui communiquer davantage d'informations. Si vous commencez à ressentir un malaise pendant l'appel, c'est une raison suffisante pour vous arrêter. Vous n'avez pas besoin d'attendre une demande tellement suspecte qu'une alarme retentirait et que votre téléphone afficherait spontanément : « ATTENTION, ESCROC ».

Dans la pratique, préparer une phrase simple et calme peut vous aider : « Merci pour cette information. Je vais mettre fin à cet appel et contacter moi-même ma banque par un canal officiel. » Cette phrase ne contient aucune accusation, n'encourage pas la discussion et indique clairement ce que vous comptez faire ensuite. Si votre interlocuteur proteste, vous pouvez répéter votre décision, puis raccrocher. Vous n'avez pas besoin d'obtenir son approbation. D'ailleurs, une personne réellement soucieuse de la sécurité de votre argent ne devrait pas attendre de vous que vous renonciez à une vérification raisonnable uniquement pour éviter de la vexer.

Deuxième piège : le numéro familier affiché à l'écran

Le téléphone de Marta affiche un numéro ressemblant à celui de sa banque. Cela renforce encore sa conviction que tout est normal. Après tout, il est difficile de soupçonner son téléphone de mentir. L'appareil a coûté plusieurs milliers de zlotys, sait reconnaître le visage de sa propriétaire et calculer un itinéraire jusqu'à l'autre bout de l'Europe. Il

devrait donc savoir qui appelle. Malheureusement, les capacités techniques d'un smartphone ne signifient pas que chaque information affichée concernant un appel a été vérifiée de manière fiable.

L'usurpation de numéro de téléphone, appelée spoofing, peut faire apparaître sur l'écran du destinataire un numéro différent de celui d'où provient réellement l'appel. Il existe des mécanismes destinés à limiter ce type d'abus, mais il ne faut pas supposer que le numéro affiché garantit toujours l'identité de la personne qui appelle. Enregistrer le numéro de la banque dans ses contacts ne résout pas non plus le problème. Votre téléphone peut afficher un nom familier parce qu'il reconnaît le numéro présenté, et non parce qu'il a personnellement vérifié le contrat de travail de l'individu à l'autre bout du fil.

Il est important de distinguer un appel entrant d'un contact que vous établissez vous-même. Lorsque quelqu'un vous appelle, c'est cette personne qui prend l'initiative de la communication et affirme posséder une certaine identité. Lorsque vous composez vous-même un numéro obtenu auprès d'une source fiable et indépendante, vous reprenez le contrôle du choix de l'établissement que vous cherchez à joindre. Ce n'est pas une garantie magique qui résout tous les problèmes, mais cela change considérablement la situation. Vous ne dépendez plus uniquement des déclarations d'un inconnu.

Il ne faut cependant pas utiliser le numéro envoyé par SMS par votre interlocuteur suspect, ni suivre le lien qu'il vient de vous dicter. Ce serait un peu comme vérifier l'honnêteté d'un vendeur de montres douteuses en téléphonant à son ami, présenté comme un expert indépendant en authenticité. Les coordonnées doivent

provenir d'une source à laquelle vous faites confiance indépendamment de la conversation en cours : l'application officielle de votre banque, son véritable site Internet ouvert de votre propre initiative ou des documents reçus précédemment de l'établissement.

Reconnaître le danger commence par la bonne question

Vous ne saurez pas toujours si votre interlocuteur est un escroc. Et vous n'avez pas besoin de le savoir immédiatement. Réagir correctement n'exige pas de résoudre une énigme criminelle en trente secondes. Il suffit de reconnaître que la personne à l'autre bout du fil n'a pas été identifiée de manière indépendante et qu'elle cherche pourtant à influencer vos décisions financières. C'est une raison suffisante pour suspendre l'exécution de ses instructions.

Beaucoup de gens se concentrent sur la question : « Cet homme semble-t-il crédible ? » Une question beaucoup plus utile serait : « Que puis-je faire en toute sécurité sans supposer que cet homme dit la vérité ? » La première vous oblige à juger une voix, une attitude et des détails qui peuvent tous faire partie d'une escroquerie soigneusement préparée. La seconde vous permet de choisir une action indépendante de ces impressions. Vous pouvez noter l'information concernant la prétendue transaction, mettre fin à l'appel et effectuer vous-même les vérifications nécessaires. Vous n'avez besoin ni d'être certain que votre interlocuteur ment, ni de posséder la preuve qu'il est honnête.

C'est exactement ce que fait Marta lorsqu'elle retrouve un instant de calme. Elle annonce qu'elle appellera elle-même sa banque. L'homme répond qu'il n'y a pas de temps à perdre et que chaque minute augmente le risque de perdre

son argent. Marta ressent de l'inquiétude, mais ne change pas d'avis. Elle met fin à la conversation, ouvre l'application bancaire officielle et utilise le moyen de contact qui y est proposé. Elle décrit l'appel reçu et demande que son compte soit vérifié. Ce sont uniquement les informations obtenues grâce à cette démarche indépendante qui servent ensuite de base à ses décisions.

Dans cet exemple, la banque ne confirme aucune tentative de virement correspondant à la description donnée. Marta n'a pas besoin de savoir qui était réellement l'homme au téléphone ni comment il avait obtenu ses informations. Elle a fait ce qui était nécessaire : elle n'a communiqué aucune donnée confidentielle, n'a validé aucune opération et n'a pas laissé un inconnu lui imposer sa méthode de vérification.

Quant aux glaces ? Malheureusement, la protection des produits surgelés ne relève pas des compétences des établissements bancaires. Toute procédure a ses limites.

Pourquoi le bon sens ne suffit pas toujours

Il est facile de dire qu'il suffit de faire preuve de bon sens. Il est plus difficile d'expliquer précisément ce que cela signifie lorsque quelqu'un vous annonce que l'argent économisé pendant plusieurs années est menacé. Le bon sens n'est pas un bouton sur lequel on appuie pour désactiver instantanément la peur. C'est plutôt un ensemble de règles définies à l'avance, grâce auxquelles vous n'avez pas besoin de reprendre chaque décision depuis le début.

Il est donc utile, avant même de recevoir un appel suspect, de savoir où trouver les coordonnées officielles de votre banque et comment se déroulent les communications sécurisées avec ses employés. Vous pouvez examiner les

moyens de contact proposés dans l'application, prendre connaissance des avertissements publiés par votre banque et vous renseigner sur la conduite à tenir en cas de transaction non autorisée. Une telle préparation n'a rien d'excessif. De même que connaître une issue de secours ne signifie pas que vous vous attendez à un incendie chaque matin, savoir contacter votre banque n'implique pas de croire que le monde entier essaie de prendre le contrôle de votre compte.

Il est également important de ne pas évaluer votre sécurité uniquement à partir de vos expériences passées. Le fait qu'aucun appel suspect reçu au cours des dix dernières années n'ait entraîné de problème ne prouve pas que le prochain sera tout aussi inoffensif. À l'inverse, recevoir un faux appel bancaire ne signifie pas automatiquement que votre compte a été compromis. Il faut distinguer une tentative d'escroquerie d'une véritable atteinte à la sécurité. Paniquer après chaque appel inconnu serait aussi peu pratique que faire aveuglément confiance à toute personne se présentant comme conseiller bancaire.

Un interlocuteur bien préparé peut paraître extrêmement convaincant, tandis qu'un véritable employé de banque peut passer une mauvaise journée, parler de manière peu claire ou oublier les formules de politesse les plus élégantes. Il vaut donc mieux éviter de prendre ses décisions sur la base d'un concours de charisme téléphonique. Une conduite prudente doit fonctionner aussi bien lorsque l'appelant possède la voix veloutée d'un animateur de radio que lorsqu'il ressemble à quelqu'un qui vient de boire son troisième café sans toujours comprendre le principe du lundi.

En définitive, il ne s'agit pas de remporter une discussion contre un escroc. Vous n'avez pas à lui prouver que vous avez découvert ses intentions ni à prolonger la conversation jusqu'à ce qu'il avoue sa culpabilité. Parfois, la conclusion la plus raisonnable consiste simplement à raccrocher. Sans réplique dramatique, sans discours et sans dénouement spectaculaire digne d'un film d'action.

Votre argent n'a pas besoin d'un héros flamboyant. Il a besoin d'un propriétaire qui sait quand arrêter d'écouter un inconnu.

Chapitre 2 - Comment sait-il tout cela ? Anatomie d’une confiance accordée à crédit

Lorsqu’un inconnu prononce votre prénom, cela ne vous impressionne généralement pas beaucoup. Votre prénom figure sur des colis, dans des messages, des documents et des profils Internet. Mais si la personne qui appelle ajoute votre nom de famille, le nom de votre banque et plusieurs informations concernant votre vie, la situation commence à prendre une autre dimension. Vous avez l’impression de parler à quelqu’un qui bénéficie d’un accès privilégié. Une équation très simple se forme alors dans votre esprit : puisqu’il connaît ces détails, il doit forcément être celui qu’il prétend être. Le problème, c’est que cette équation repose sur une hypothèse erronée, et que quelqu’un s’apprête justement à vous présenter la facture de cette erreur.

Imaginez Tomasz, qui répond à un appel pendant sa pause au travail. Son interlocutrice se présente comme une employée de sa banque, prononce son prénom et son nom complets, puis évoque sa carte bancaire et une activité suspecte sur son compte. Tomasz lui demande comment elle possède ces informations. La femme répond calmement qu’elle les voit dans le système. Elle cite même quelques chiffres qui lui rappellent son numéro de compte. Tomasz cesse de poser des questions. Puisque l’employée voit ces informations dans le système, tout semble forcément officiel. Il ne lui vient pas à l’esprit qu’on peut également prononcer les mots « Je le vois dans notre système » lorsque le seul système disponible est un tableur ouvert à l’écran.