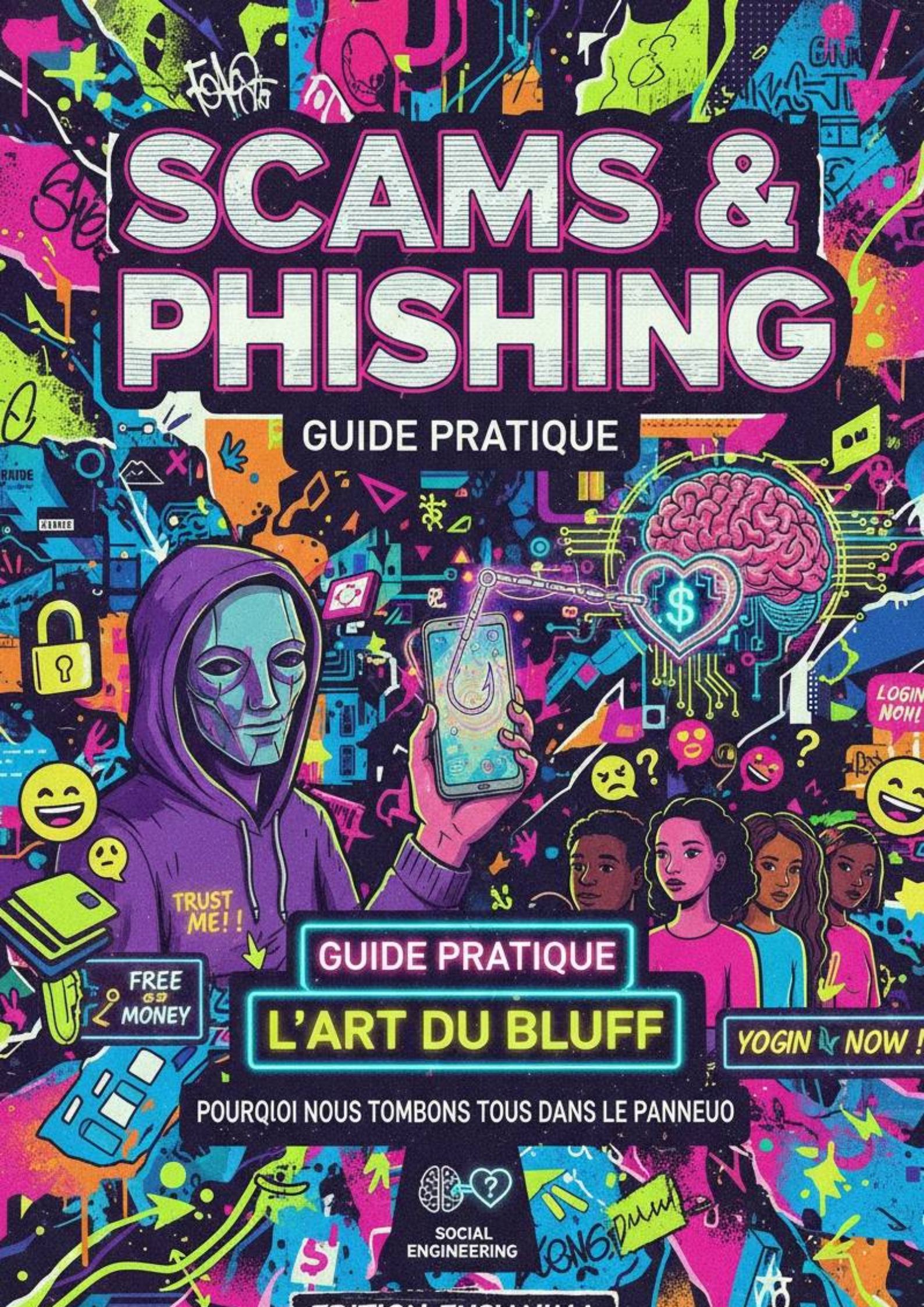
SCAMS & PHISHING

GUIDE PRATIQUE



GUIDE PRATIQUE

L'ART DU BLUFF

POURQIOI NOUS TOMBONS TOUS DANS LE PANNEUO

Scams & Phishing

Par Fusianima Expert

ÉDITIONS FUSIANIMA

Lire la version interactive sur Fusianima.com

Table des matières

Chapitre 1

L'Art du Bluff : Pourquoi nous tombons tous dans le panneau

Module : L'Art du Bluff - Pourquoi nous tombons tous dans le panneau

Contrairement aux idées reçues, une arnaque réussie ne repose pas sur une technologie complexe, mais sur la manipulation de vos émotions. C'est ce qu'on appelle l'ingénierie sociale.

Comprendre les mécanismes psychologiques que les fraudeurs utilisent contre vous est la première étape pour devenir inattaquable.

Point Clé 1 : La Trinité de la Manipulation

Pour vous faire perdre votre sens critique, les escrocs activent généralement l'un des trois leviers suivants :

• L'Urgence : On vous demande d'agir immédiatement sous peine de conséquences graves (suppression de compte, amende majorée). L'objectif est de court-circuiter votre réflexion logique.

• La Peur : C'est le moteur le plus puissant. Un message prétendant que votre sécurité est compromise ou que vous faites l'objet d'une poursuite judiciaire déclenche un état de panique propice à l'erreur.

• La Curiosité : "Découvrez qui a visité votre profil" ou "Votre colis a été retenu". L'escroc mise sur votre besoin naturel de savoir ou de résoudre un mystère pour vous faire cliquer sur un lien piégé.

Point Clé 2 : Le Mythe de l'Immunité

Beaucoup pensent que les victimes de phishing sont "naïves" ou "peu éduquées". C'est une erreur fondamentale qui profite aux cybercriminels. Personne n'est immunisé pour les raisons suivantes :

• Le moment de faiblesse : Une personne fatiguée, stressée par son travail ou distraite par ses enfants est une cible idéale, peu importe son niveau d'études.

• La surcharge cognitive : Nous recevons tellement de notifications que notre cerveau traite l'information de manière automatique. L'escroc compte sur ce mode "pilote automatique".

• L'adaptation des scénarios : Les arnaques ciblent chaque tranche d'âge avec précision. Les jeunes via les réseaux sociaux (concours, cryptomonnaies) et les seniors via des institutions officielles (Assurance Maladie, Impôts).

Point Clé 3 : Les Ressorts de la Confiance Automatique

L'être humain est programmé pour coopérer. Les fraudeurs exploitent des biais cognitifs profondément ancrés :

• L'Autorité : Nous avons tendance à obéir sans réfléchir à une figure d'autorité. L'utilisation de logos officiels (Police, Banque, État) crée une soumission immédiate.

• La Preuve Sociale : En créant de faux commentaires ou de faux likes sous une publicité frauduleuse, l'escroc vous rassure. Si "les autres" disent que c'est vrai, alors c'est crédible.

• La Réciprocité : En vous offrant un prétendu cadeau ou un remboursement, l'escroc crée une dette morale inconsciente qui vous pousse à fournir vos informations personnelles en retour.

Point Clé 4 : Comment sortir du piège psychologique

Pour déjouer le bluff, vous devez réintroduire de la distance entre le stimulus et votre

action :

• La règle des 10 secondes : Respirez. Si un message exige une action immédiate, c'est le signe numéro un d'une tentative de fraude.

• Vérifiez le canal : Ne cliquez jamais sur un lien reçu par SMS ou email. Allez manuellement sur le site officiel de l'organisme concerné via votre navigateur habituel.

• Doutez de l'exceptionnel : Si une offre semble trop belle pour être vraie ou si un problème semble trop grave pour être réglé par un simple clic, c'est probablement un bluff.

LE CONSEIL PRO : Adoptez la posture du "Scepticisme Bienveillant". Partez du principe que tout message non sollicité demandant une action de votre part est suspect jusqu'à preuve du contraire. Le temps est votre meilleur allié : un véritable organisme ne vous harcèlera jamais pour obtenir vos codes en moins de deux minutes.

Chapitre 2

Phishing, Smishing, Vishing : Le lexique pour ne plus être une cible

Module : Phishing, Smishing, Vishing – Le lexique pour ne plus être une cible

Pour se protéger efficacement, il est essentiel de comprendre le vocabulaire des cybercriminels. Ces trois techniques reposent sur un même principe : l'usurpation d'identité pour voler vos données ou votre argent.

Point 1 : Le Phishing (Hameçonnage) par E-mail

Le Phishing est la méthode la plus ancienne et la plus répandue. L'attaquant envoie un courriel en se faisant passer pour un organisme officiel (Banque, Impôts, Assurance Maladie, Netflix, etc.).

• L'expéditeur : L'adresse mail semble réelle au premier coup d'œil, mais si vous cliquez sur le nom, l'adresse réelle est souvent fantaisiste (ex: securite@banque-verif-78.com).

• L'urgence : Le message utilise un ton alarmiste ("Compte bloqué", "Action requise sous 24h") pour vous empêcher de réfléchir.

• Le lien : En survolant le bouton avec votre souris (sans cliquer !), l'adresse qui s'affiche en bas de votre écran ne correspond pas au site officiel.

• L'orthographe : Présence fréquente de fautes de français, de syntaxes lourdes ou de caractères spéciaux inhabituels.

Point 2 : Le Smishing (Hameçonnage par SMS)

Contraction de "SMS" et "Phishing", le Smishing cible votre téléphone portable. C'est une attaque redoutable car nous avons tendance à faire plus confiance aux messages reçus sur notre smartphone.

• Le prétexte : Les thèmes classiques incluent la livraison d'un colis (Chronopost, DHL), une amende de stationnement impayée (ANTAI) ou une mise à jour de la carte Vitale.

• Le lien court : Les SMS utilisent presque toujours des liens raccourcis (type bit.ly ou tinyurl.com) pour masquer la destination réelle.

• Le numéro : Le message provient souvent d'un numéro de mobile classique (06 ou 07) ou d'un numéro court étrange, ce qui est anormal pour une administration.

• L'action demandée : On vous demande de cliquer immédiatement pour "éviter une majoration" ou "débloquer un envoi".

Point 3 : Le Vishing (Hameçonnage par la voix)

Le Vishing (Voice Phishing) utilise le téléphone pour vous manipuler de vive voix. L'escroc mise sur la pression sociale et l'autorité pour vous soutirer des informations confidentielles.

• L'usurpation de numéro : Grâce à des logiciels, l'escroc peut faire apparaître le vrai numéro de votre banque sur votre écran. C'est le "Spoofing".

• Le scénario : Un prétendu "conseiller du service fraude" vous appelle pour vous signaler une opération suspecte sur votre compte.

• La demande de code : L'attaquant vous demande de lui dicter un code de validation reçu par SMS ou de valider une opération sur votre application bancaire.

• Le ton : L'interlocuteur est souvent très professionnel, calme et rassurant pour gagner votre confiance avant de devenir pressant.

Point 4 : Tableau récapitulatif pour trancher

• C'est un mail ? Vérifiez l'adresse de l'expéditeur et le lien (Phishing).

• C'est un SMS ? Ne cliquez jamais sur le lien. Allez sur le site officiel via votre navigateur (Smishing).

• C'est un appel ? Raccrochez immédiatement. Rappelez vous-même votre conseiller avec le numéro enregistré dans votre répertoire (Vishing).

LE CONSEIL PRO : Retenez cette règle d'or : Aucune banque ni administration ne vous demandera jamais votre mot de passe, votre code de carte bleue ou un code de validation SMS par téléphone ou par message. Si on vous le demande, c'est systématiquement une tentative de vol.

Chapitre 3

L'Email Fatal : Démonter la mécanique d'un courrier frauduleux

MODULE : L'Email Fatal : Démonter la mécanique d'un courrier frauduleux

Le phishing (ou hameçonnage) repose sur une illusion. Pour ne pas tomber dans le piège, vous devez apprendre à regarder derrière le décor. Voici comment disséquer un e-mail suspect comme un expert en cybersécurité.

Point Clé 1 : L'imposture de l'adresse d'expédition

Les pirates utilisent souvent un nom d'affichage rassurant pour masquer leur véritable identité.

• Le nom d'affichage : Un mail peut s'afficher comme provenant de "L'Assurance Maladie" ou "Netflix", mais cela n'est qu'une simple étiquette modifiable par n'importe qui.

• L'adresse réelle : Sur ordinateur, survolez le nom de l'expéditeur. Sur mobile, appuyez sur le nom pour voir l'adresse complète derrière les chevrons (ex: support@security-update-99.com).

• Le domaine : Vérifiez ce qui suit le symbole "@". Si l'e-mail prétend venir de Microsoft mais finit par @gmail.com ou @outlook.fr, c'est une fraude manifeste.

Point Clé 2 : L'usurpation de l'identité visuelle

Le pirate veut que vous vous sentiez en terrain connu en copiant l'esthétique officielle des grandes marques.

• Les logos : Ils sont souvent copiés-collés depuis le site officiel, mais peuvent paraître légèrement flous ou étirés.

• La mise en page : Les boutons, les couleurs et les polices de caractères imitent parfaitement les mails de facturation ou d'alerte de sécurité habituels.

• Le pied de page : Les mentions légales et les liens vers les réseaux sociaux sont souvent présents mais non cliquables ou renvoient vers des pages vides.

Point Clé 3 : Les anomalies de langage et la pression psychologique

L'objectif du pirate est de vous faire agir sans réfléchir en utilisant des leviers émotionnels.

• Le sentiment d'urgence : Des termes comme "Action requise immédiatement", "Votre compte sera suspendu dans 24h" ou "Dernier rappel avant poursuites" sont des signaux d'alerte.

• Les fautes d'orthographe : Elles sont parfois volontaires pour contourner les filtres anti-spam ou pour cibler les personnes les moins attentives.

• Les formules génériques : Un vrai service client utilise souvent votre nom ou un identifiant client. Un mail commençant par "Cher client" ou "Cher utilisateur" est suspect.

Point Clé 4 : Le piège caché derrière les liens

C'est l'élément le plus dangereux du mail. Le bouton sur lequel on vous demande de cliquer ne mène jamais là où vous le pensez.

• La technique du survol : Avant de cliquer, laissez votre souris sur le bouton ou le lien sans appuyer. L'adresse réelle (URL) s'affichera en bas à gauche de votre navigateur.

• Les adresses raccourcies : Méfiez-vous des liens de type "bit.ly" ou "t.co" dans des e-mails officiels ; les banques et administrations ne les utilisent pratiquement jamais.

• La redirection : Le lien peut ressembler à "impots.gouv.fr" mais pointer en réalité vers "impots.gouv.fr.verif-identite.com". Le vrai domaine est toujours celui juste avant le dernier point.

LE CONSEIL PRO : En cas de doute, n'utilisez JAMAIS les liens contenus dans l'e-mail. Fermez votre messagerie, ouvrez votre navigateur et connectez-vous manuellement sur le site officiel de l'organisme en tapant l'adresse vous-même. Si une action est réellement requise, elle apparaîtra dans votre espace client sécurisé.

Chapitre 4

Le Miroir aux Alouettes : Démasquer les faux sites de e-commerce

Le Miroir aux Alouettes : Démasquer les faux sites de e-commerce

Le commerce en ligne est le terrain de jeu favori des cyber-escrocs. Derrière des designs professionnels et des publicités alléchantes sur les réseaux sociaux se cachent souvent des boutiques éphémères conçues uniquement pour voler vos coordonnées bancaires ou ne jamais livrer vos commandes.

Étape 1 : Se méfier des prix "trop beaux pour être vrais"

• Remises excessives : Si vous voyez un produit premium (iPhone, sac de luxe, console de jeux) à -80% ou -90%, fuyez.

• Urgence artificielle : Méfiez-vous des comptes à rebours agressifs ("Plus que 10 minutes !") ou des mentions de stocks quasi épuisés visant à provoquer un achat impulsif.

• Publicités sociales : La majorité des arnaques au e-commerce transitent par des publicités ciblées sur Instagram, Facebook ou TikTok.

Étape 2 : L'audit de fiabilité (Le réflexe détective)

Avant d'ajouter un article au panier, prenez deux minutes pour vérifier l'identité réelle du vendeur :

• Les mentions légales : Elles sont obligatoires. Cherchez un lien en bas de page. Un site sérieux doit afficher le nom de la société, son siège social et son numéro d'immatriculation (SIRET en France).

• L'URL du site : Observez attentivement la barre d'adresse. Les escrocs utilisent souvent des noms de domaine proches de marques connues (ex: vente-privee-destock.com au lieu du site officiel).

• L'ancienneté du domaine : Utilisez des outils gratuits comme "Whois" pour voir quand le site a été créé. Un site de e-commerce qui n'a que quelques jours ou semaines d'existence est extrêmement suspect.

• Les fautes d'orthographe : Une interface truffée de fautes de français ou de traductions approximatives est un indicateur majeur de site frauduleux.

Étape 3 : Analyser les avis clients et la réputation

• Recherche externe : Ne vous fiez jamais aux avis affichés directement sur le site (ils sont souvent faux). Taper le nom du site suivi du mot "arnaque" ou "avis" dans un moteur de recherche.

• Plateformes tierces : Consultez des sites de confiance comme Trustpilot ou Signal-Arnaques pour vérifier les expériences des autres utilisateurs.

• Réseaux sociaux : Vérifiez si le site possède des pages de réseaux sociaux actives avec de vrais commentaires d'utilisateurs, et non simplement des images de catalogue.

Étape 4 : Sécuriser le paiement et la transaction

Le moment du paiement est l'étape critique où vos données sont les plus exposées :

• Le protocole HTTPS : Vérifiez la présence du petit cadenas à gauche de l'URL. S'il est absent ou barré en rouge, ne saisissez jamais vos coordonnées bancaires.

• Moyens de paiement suspects : Un site qui exige un paiement par virement bancaire direct, par mandat cash (Western Union) ou en crypto-monnaies est presque systématiquement une arnaque.

• Utilisation de services tiers : Privilégiez les solutions comme PayPal qui offrent une protection des achats en cas de non-livraison.

• La double authentification : Assurez-vous que votre banque déclenche une validation 3D Secure (code par SMS ou validation sur application mobile) lors de la transaction.

LE CONSEIL PRO : Utilisez systématiquement une carte bancaire virtuelle (e-carte bleue) pour vos achats sur des sites que vous utilisez pour la première fois. Ce service, proposé par la plupart des banques, génère un numéro de carte à usage unique avec un montant plafonné. Même si le site est une arnaque, vos véritables coordonnées bancaires restent à l'abri et le pirate ne pourra pas vous prélever une seconde fois.

Chapitre 5

Cœur Brisé et Portefeuille Vide : Les arnaques aux sentiments

Cœur Brisé et Portefeuille Vide : Les arnaques aux sentiments

Les arnaques aux sentiments, souvent orchestrées par ceux qu'on appelle les "brouteurs", sont redoutables car elles s'attaquent à l'intimité et à la solitude des victimes. Voici comment décrypter leur stratégie pour ne jamais tomber dans le piège.

Étape 1 : La création du personnage idéal

• L'usurpation d'identité : Le brouteur utilise des photos volées de personnes séduisantes, souvent des mannequins peu connus, des militaires ou des entrepreneurs réussis.

• Le profil "trop beau pour être vrai" : Le profil affiche une vie stable, des valeurs morales fortes (religion, famille) et une recherche sincère de l'amour.

• L'éloignement géographique : Le personnage est souvent en déplacement à l'étranger (mission humanitaire, voyage d'affaires en Afrique ou au Moyen-Orient) pour justifier l'impossibilité de se rencontrer physiquement.

Étape 2 : La phase de mise en confiance (Le "Love Bombing")

• L'attention constante : Le fraudeur envoie des dizaines de messages par jour, créant une dépendance affective rapide.

• Les déclarations précoces : Des mots d'amour enflammés arrivent dès les premiers jours de discussion, avant même toute rencontre réelle.

• L'isolement de la victime : L'arnaqueur demande rapidement de quitter le site de

rencontre officiel pour passer sur des messageries privées comme WhatsApp ou Telegram afin d'échapper à la modération.

Étape 3 : Le déclenchement de l'urgence financière

• Le scénario de la catastrophe : Une fois le lien émotionnel établi, un problème grave survient subitement (accident, hospitalisation d'un enfant, blocage de compte bancaire, frais de douane imprévus).

• La demande d'aide : Le brouteur demande une somme d'argent, souvent "modeste" au début, en jurant de rembourser dès son retour.

• Les modes de paiement intraçables : Ils exigent systématiquement des moyens de transfert anonymes comme Western Union, MoneyGram, des tickets PCS, Transcash ou des cryptomonnaies.

Les signes qui doivent vous alerter immédiatement

• La caméra "en panne" : L'interlocuteur refuse systématiquement les appels vidéo ou utilise des vidéos pré-enregistrées de mauvaise qualité qui ne correspondent pas au son.

• Les incohérences : Des fautes de syntaxe surprenantes pour quelqu'un censé être très éduqué, ou des détails qui changent d'un jour à l'autre dans son récit.

• La demande de photos intimes : Le brouteur peut tenter d'obtenir des clichés compromettants pour pratiquer ensuite une sextorsion (chantage à la webcam).

Comment protéger vos données et votre portefeuille

• Effectuez une recherche d'image inversée : Utilisez Google Lens ou TinEye pour voir si la photo de votre correspondant apparaît sur d'autres profils sous d'autres noms.

• Gardez vos distances : Ne donnez jamais votre adresse précise, vos coordonnées bancaires ou des détails sur votre patrimoine lors des premières semaines de discussion.

• La règle d'or : N'envoyez JAMAIS d'argent à une personne que vous n'avez jamais rencontrée en chair et en os, quelles que soient l'urgence et la détresse affichées.

• Signalez et bloquez : Dès qu'une demande d'argent est formulée, coupez tout contact et signalez le profil sur la plateforme de rencontre.

LE CONSEIL PRO : Appliquez le test de la "vidéo en direct" très tôt. Demandez-lui de faire un geste spécifique devant sa caméra (ex: toucher son oreille gauche, tenir un papier avec votre prénom). S'il refuse ou s'il trouve une excuse technique, c'est systématiquement une arnaque.

Chapitre 6

L'Urgence Bancaire : Déjouer les faux conseillers au téléphone

L'Urgence Bancaire : Déjouer les faux conseillers au téléphone

C'est l'une des arnaques les plus redoutables aujourd'hui. Vous recevez un appel, et le numéro qui s'affiche sur votre écran est exactement celui de votre agence bancaire ou du service client de votre banque. Pourtant, au bout du fil, ce n'est pas un employé, mais un escroc professionnel.

Étape 1 : Le "Spoofing" ou l'usurpation d'identité technique

Pour réussir leur coup, les fraudeurs utilisent une technique appelée le spoofing téléphonique. Voici comment ils procèdent :

• Ils utilisent des logiciels spécialisés pour masquer leur véritable numéro.

• Ils programment l'affichage pour que votre téléphone reconnaisse et affiche le nom ou le numéro officiel de votre banque.

• L'objectif est de briser immédiatement vos défenses en instaurant un climat de confiance totale dès la première seconde.

Étape 2 : La mise en scène de "l'urgence absolue"

Une fois que vous avez décroché, l'escroc adopte un ton calme, professionnel et très sérieux. Le scénario est presque toujours le même :

• L'interlocuteur se présente comme un conseiller du service fraude.

• Il vous informe qu'une opération suspecte (souvent un achat à l'étranger ou un

virement important) est en cours sur votre compte.

• Il prétend que vous devez agir immédiatement pour bloquer cette transaction avant qu'il ne soit trop tard.

Étape 3 : Le piège de la validation "d'annulation"

C'est ici que l'arnaque se concrétise. Sous prétexte de sécuriser votre compte ou d'annuler la fraude, le faux conseiller vous demande de réaliser des manipulations :

• Il vous demande de lui dicter un code reçu par SMS.

• Ou il vous demande de vous connecter à votre application et de valider une notification (en prétendant que c'est une procédure d'annulation).

• La réalité : En faisant cela, vous ne bloquez rien. Vous êtes en train de valider un virement ou d'ajouter le compte de l'escroc comme nouveau bénéficiaire.

Les signaux d'alerte : Comment les repérer ?

Même si le numéro affiché est le bon, certains détails prouvent qu'il s'agit d'une tentative de vishing (phishing vocal) :

• La demande de codes : Une banque ne vous demandera JAMAIS de lui communiquer un code reçu par SMS ou votre mot de passe.

• La validation d'annulation : Une banque n'a pas besoin que vous validiez une opération sur votre application pour "l'annuler".

• La pression psychologique : Si l'interlocuteur insiste lourdement ou vous interdit de raccrocher, c'est une alerte majeure.

La procédure de défense immédiate

Si vous avez le moindre doute lors d'un appel, suivez scrupuleusement ces étapes

pour protéger vos économies :

• Raccrochez immédiatement : Ne cherchez pas à argumenter avec l'interlocuteur.

• Ne rappelez pas le numéro : Si vous rappelez le numéro qui s'affiche, vous pourriez retomber sur l'escroc via leur système technique.

• Utilisez un autre canal : Appelez vous-même votre conseiller via le numéro que vous trouverez sur vos relevés de compte papier ou sur l'application officielle que vous aurez ouverte manuellement.

• Vérifiez vos comptes : Connectez-vous à votre espace client pour vérifier si des mouvements suspects sont réellement visibles.

LE CONSEIL PRO : Considérez que l'affichage du nom ou du numéro de l'appelant n'est plus une preuve d'identité fiable. En cas d'alerte sur vos comptes, le réflexe de sécurité absolue est de raccrocher et de rappeler vous-même votre banque. Si c'est une vraie urgence, votre conseiller ne s'offusquera jamais de votre prudence.

Chapitre 7

Réseaux Sociaux : Quand vos amis deviennent des vecteurs d'attaque

Module : Réseaux Sociaux : Quand vos amis deviennent des vecteurs d'attaque

Sur les réseaux sociaux, la menace ne vient pas toujours d'un inconnu. Les pirates utilisent souvent le compte piraté d'une personne de confiance pour vous piéger. Voici comment identifier et déjouer ces attaques.

1. Le piratage de compte et le vol d'accès

Pour prendre le contrôle de votre vie numérique, les cybercriminels n'ont pas besoin de compétences techniques complexes, mais de votre inattention.

• Le Phishing par message : Vous recevez un message privé (Messenger, DM Instagram) d'un contact disant : "Regarde cette vidéo, on dirait toi !".

• Le faux formulaire de connexion : Le lien vous renvoie vers une page imitant parfaitement le réseau social.

• La capture d'identifiants : Dès que vous saisissez vos accès, le pirate change votre mot de passe et votre e-mail de récupération pour vous exclure définitivement.

2. Les jeux concours bidon : Le piège à clics

Ces arnaques pullulent sur Facebook et Instagram sous forme de publications sponsorisées ou partagées par des amis imprudents.

• La promesse : Des lots incroyables (iPhone, billets d'avion, robots de cuisine) offerts pour célébrer un faux anniversaire de marque.

• L'engagement forcé : On vous demande de partager la publication, de taguer des amis et de cliquer sur un lien pour "valider votre gain".

• Le résultat : Vous êtes redirigé vers des sites de collecte de données personnelles ou des abonnements payants cachés facturés sur votre mobile.

3. L'arnaque à l'urgence (Le proche en détresse)

C'est l'attaque la plus cruelle, car elle exploite votre empathie et votre désir d'aider un ami.

• Le scénario : Un ami vous contacte en urgence. Il prétend être bloqué à l'étranger sans téléphone, ou avoir un besoin vital de fonds suite à un accident.

• Le mode de paiement : Le pirate demande systématiquement des méthodes intraçables comme des tickets PCS, des coupons Transcash ou des cryptomonnaies.

• La manipulation : Il vous demande de ne prévenir personne pour ne pas l'inquiéter, isolant ainsi la victime pour mieux la dépouiller.

4. Le vol d'identité numérique et le "Cloning"

Le pirate n'a pas toujours besoin d'entrer dans votre compte pour vous nuire. Il peut simplement créer un double malveillant.

• La copie du profil : Le pirate télécharge vos photos de profil et de couverture pour créer un nouveau compte à votre nom.

• L'ajout des amis : Il envoie des invitations à votre liste de contacts en prétextant que "son ancien compte a été bloqué".

• L'usurpation : Une fois les amis acceptés, il commence à envoyer des liens frauduleux ou des demandes d'argent en se faisant passer pour vous.

5. Les réflexes de défense indispensables

Protéger votre compte, c'est aussi protéger l'ensemble de vos contacts contre ces attaques en cascade.

• Double Authentification (2FA) : Activez-la systématiquement dans vos paramètres de sécurité. Sans le code reçu par SMS ou via une application, le pirate ne peut rien faire.

• Confidentialité de la liste d'amis : Réglez la visibilité de vos amis sur "Moi uniquement" pour empêcher les pirates de savoir qui contacter en cas de clonage.

• Vérification hors ligne : Si un ami vous demande de l'argent ou un service inhabituel, appelez-le directement sur son numéro de téléphone habituel.

• Signalez les faux profils : Utilisez les outils de signalement natifs de Facebook et Instagram pour faire supprimer les comptes usurpateurs.

LE CONSEIL PRO : Adoptez la règle du "Canal de Secours". Si vous recevez une demande suspecte sur un réseau social, changez immédiatement de plateforme pour vérifier (envoyez un SMS ou passez un appel vocal). Ne validez jamais une information critique via le canal sur lequel vous avez été contacté initialement.

Chapitre 8

Le Far West des Cryptos : Éviter les mirages du gain facile

Le Far West des Cryptos : Éviter les mirages du gain facile

Le monde des actifs numériques offre des opportunités réelles, mais il est aussi devenu le terrain de jeu favori des escrocs. Derrière les promesses de richesse instantanée se cachent souvent des mécanismes sophistiqués conçus pour vider votre portefeuille.

Étape 1 : Démasquer les plateformes de trading frauduleuses

De nombreux sites web imitent à la perfection les interfaces de plateformes professionnelles pour gagner votre confiance. Voici comment les repérer :

• L'absence d'enregistrement légal : Vérifiez si la plateforme possède un agrément (comme le statut PSAN en France délivré par l'AMF). Si elle n'apparaît sur aucune liste officielle, fuyez.

• L'URL suspecte : Les escrocs utilisent souvent des noms de domaine proches de sites connus (ex: binance-security-check.com au lieu de binance.com).

• Le design "miroir aux alouettes" : Des graphiques de gains permanents et une interface qui vous pousse à déposer toujours plus d'argent sans jamais pouvoir en retirer.

• Le démarchage agressif : Une plateforme sérieuse ne vous contactera jamais par WhatsApp, Telegram ou téléphone pour vous proposer un "investissement exclusif".

Étape 2 : Identifier les schémas de Ponzi modernes

Le système de Ponzi s'est adapté à la blockchain. L'argent des nouveaux entrants sert à payer les intérêts des anciens, jusqu'à l'écroulement inévitable du système.

• Les rendements fixes et irréalistes : En crypto, la volatilité est la règle. Une promesse de 1% de gain par jour (ou 30% par mois) est mathématiquement impossible et signe une arnaque.

• L'obligation de parrainage : Si votre profit dépend principalement du nombre de personnes que vous recrutez, vous n'êtes pas dans un investissement, mais dans un système pyramidal.

• Le blocage des fonds : On vous demande souvent de "bloquer" vos actifs pendant plusieurs mois pour obtenir des bonus, ce qui permet aux escrocs de s'enfuir avant que vous ne tentiez un retrait.

Étape 3 : Reconnaître les techniques de manipulation psychologique

Les fraudeurs utilisent des biais cognitifs pour court-circuiter votre esprit critique :

• L'urgence artificielle : "Plus que 2 heures pour profiter de cette ICO !" ou "Offre limitée aux 50 premiers". Cette pression vise à vous faire agir sous le coup de l'émotion.

• La preuve sociale bidon : Utilisation de faux témoignages, de montages photos avec des célébrités (Elon Musk est le plus détourné) ou de faux comptes sur les réseaux sociaux.

• Le jargon technique excessif : L'utilisation de mots complexes (algorithmes quantiques, métavers décentralisé, arbitrage IA) pour masquer le vide du projet.

Étape 4 : La check-list de sécurité avant tout versement

Avant d'envoyer le moindre centime, passez par ces points de contrôle rigoureux :

• Consulter la liste noire de l'AMF (Autorité des Marchés Financiers) qui recense les sites frauduleux.

• Vérifier la réputation du projet sur des outils d'analyse comme CoinMarketCap ou CoinGecko. Si le jeton n'y figure pas, la prudence est de mise.

• Tester le support client avec une question technique complexe. Une réponse évasive ou trop commerciale est un mauvais signe.

• Ne jamais partager sa phrase de récupération (seed phrase) : aucun support technique légitime ne vous la demandera.

LE CONSEIL PRO : Appliquez toujours la règle "Don't trust, verify" (Ne faites pas confiance, vérifiez). Si une opportunité semble trop belle pour être vraie, c'est qu'elle l'est. Dans l'écosystème crypto, être sceptique est votre meilleure assurance vie financière.

Chapitre 9

Intelligence Artificielle : L'ère des Deepfakes et des clones vocaux

L'IA : La Nouvelle Arme des Cyber-Escrocs

L'intelligence artificielle n'est plus un concept de science-fiction. Elle est devenue un outil accessible qui permet de créer des doubles numériques (voix et image) d'une fidélité déconcertante. Bienvenue dans l'ère de l'escroquerie synthétique.

1. Le Clonage Vocal : L'arnaque à l'urgence familiale

Imaginez recevoir un appel de votre enfant ou d'un parent en détresse. La voix est absolument identique, les intonations sont les mêmes, et l'émotion est palpable. C'est la puissance du clonage vocal par IA.

Étape 1 : La collecte des échantillons

• Les escrocs récupèrent quelques secondes d'audio sur vos réseaux sociaux (vidéos TikTok, Reels Instagram, stories Facebook).

• Un logiciel d'IA analyse le timbre, l'accent et les tics de langage pour générer un clone vocal capable de dire n'importe quelle phrase.

Étape 2 : La mise en scène du choc

• L'appel simule une situation de crise : un accident de voiture, une arrestation ou une perte totale de documents à l'étranger.

• Le but est de provoquer un stress émotionnel intense pour paralyser votre esprit critique et vous pousser à envoyer de l'argent rapidement.

2. Les Deepfakes : L'arnaque au président 2.0

Le Deepfake consiste à superposer le visage et le corps d'une personne sur une autre vidéo, ou à générer un avatar animé en temps réel lors d'une visioconférence.

Point Clé : L'usurpation d'identité en entreprise

• L'escroc se fait passer pour le PDG ou un cadre dirigeant lors d'un appel Zoom ou Teams avec un employé du service comptable.

• Le faux dirigeant prétexte une opération confidentielle (rachat d'entreprise, audit secret) nécessitant un virement bancaire immédiat.

• La présence visuelle du patron lève les dernières barrières de sécurité psychologique des employés.

3. Comment détecter une manipulation par l'IA ?

Malgré les progrès techniques, les contenus générés par IA conservent souvent des signaux faibles que vous pouvez apprendre à repérer.

Les indices visuels (Deepfakes)

• Le regard : Les yeux clignent rarement de manière naturelle ou ne semblent pas regarder dans la bonne direction.

• Le contour du visage : Observez les zones de jonction entre le visage et les cheveux ou les oreilles ; des flous ou des "glitchs" apparaissent souvent.

• La synchronisation labiale : Un léger décalage entre le mouvement des lèvres et le son de la voix est fréquent.

Les indices sonores (Clones vocaux)

• Le rythme : Une voix d'IA peut avoir un rythme trop régulier ou, au contraire, faire

des pauses étranges au milieu d'un mot.

• Le manque de texture : La voix peut paraître "trop propre", sans les bruits de respiration ou les imperfections naturelles d'une voix humaine.

4. Les protocoles de protection essentiels

Face à une technologie qui imite parfaitement l'humain, la solution est de revenir à des procédures de vérification strictes.

• Le canal secondaire : Si vous recevez un appel suspect d'un proche, raccrochez immédiatement. Rappelez-le sur son numéro habituel ou contactez un autre membre de la famille pour vérifier l'information.

• Le test de la question personnelle : Posez une question dont seul votre proche connaît la réponse (ex: "Comment s'appelait notre premier animal de compagnie ?"). L'IA ne peut pas improviser sur des faits non publics.

• La procédure d'entreprise : Ne validez jamais un virement exceptionnel sur la base d'un simple appel vidéo. Exigez toujours une validation par un canal écrit officiel et sécurisé.

LE CONSEIL PRO : Établissez dès aujourd'hui un "code secret familial" ou un mot de passe de sécurité avec vos proches. Si l'un d'entre vous appelle pour une urgence financière, l'usage de ce mot simple permet de confirmer instantanément l'identité, car l'IA ne pourra jamais le deviner.

Chapitre 10

Votre Armure Numérique : Mots de passe et Double Authentification

Module : Votre Armure Numérique : Mots de passe et Double Authentification

Dans le monde de la cybersécurité, votre mot de passe est la première ligne de défense. Mais face à des pirates de plus en plus sophistiqués, cette ligne est souvent trop fragile. Ce module vous apprend à forger une armure numérique robuste pour protéger vos comptes personnels et professionnels.

Étape 1 : Créer des mots de passe réellement inviolables

Oubliez les noms de vos enfants ou vos dates de naissance. Un bon mot de passe doit être complexe pour une machine, mais simple à retenir pour vous grâce à la méthode de la "phrase de passe".

• La longueur prime sur la complexité : Visez au minimum 12 à 14 caractères. Un mot de passe long est exponentiellement plus difficile à casser qu'un mot de passe court avec des caractères spéciaux.

• Utilisez la méthode des phrases : Choisissez une phrase absurde, facile à visualiser. Exemple : LeChatBleuMangeDuSaucisson!22.

• Mélangez les types de caractères : Intégrez systématiquement des majuscules, des minuscules, des chiffres et des symboles (ex: @, , $, !).

• L'unicité est la règle d'or : N'utilisez jamais le même mot de passe pour deux sites différents. Si un site est piraté, tous vos autres comptes restent ainsi en sécurité.

Étape 2 : Centraliser avec un gestionnaire de mots de passe

Il est humainement impossible de retenir 50 mots de passe complexes et différents. C'est ici qu'intervient le gestionnaire de mots de passe, votre coffre-fort numérique.

• Un seul mot de passe à retenir : Vous ne retenez que la clé de votre coffre-fort (le "mot de passe maître").

• Génération automatique : L'outil crée pour vous des mots de passe aléatoires et ultra-sécurisés pour chaque nouveau compte.

• Remplissage automatique : Le gestionnaire remplit vos identifiants sur les sites web et applications, vous protégeant ainsi contre certains types de phishing.

• Synchronisation : Vos accès sont disponibles sur votre ordinateur, smartphone et tablette de manière sécurisée.

• Outils recommandés : Bitwarden (gratuit et open-source), Dashlane ou 1Password.

Étape 3 : Activer la Double Authentification (2FA)

La 2FA est votre ultime bouclier. Même si un pirate parvient à voler votre mot de passe, il ne pourra pas accéder à votre compte sans ce second code unique.

• Le principe : C'est la combinaison de quelque chose que vous connaissez (votre mot de passe) et de quelque chose que vous possédez (votre téléphone).

• Les applications d'authentification (Recommandé) : Utilisez des applications comme Google Authenticator, Microsoft Authenticator ou Authy. Elles génèrent un code toutes les 30 secondes.

• Les clés de sécurité physiques : Pour une sécurité maximale, utilisez des clés USB type YubiKey. C'est la méthode la plus infaillible contre le phishing.

• Le SMS (Mieux que rien) : Bien que moins sécurisé que les applications, le code par SMS reste une protection efficace pour le grand public.

Étape 4 : Les réflexes de survie numérique

Maintenir votre armure demande quelques vérifications régulières pour s'assurer qu'aucune brèche n'est apparue.

• Vérifiez les fuites de données : Utilisez le site Have I Been Pwned pour savoir si votre adresse email est associée à une fuite de données connue.

• Changez vos accès critiques : Si une fuite est détectée, changez immédiatement le mot de passe du compte concerné.

• Méfiez-vous des alertes de sécurité : Si vous recevez un code de connexion 2FA que vous n'avez pas demandé, quelqu'un tente de se connecter. Changez votre mot de passe immédiatement.

LE CONSEIL PRO : Ne stockez jamais vos mots de passe dans un fichier Excel, un document Word ou sur un post-it collé à votre écran. Ces supports sont les premières cibles lors d'un vol physique ou d'une intrusion informatique simple. Si vous devez noter votre mot de passe maître, cachez-le dans un endroit physique sécurisé, loin de votre ordinateur.

Chapitre 11

Le Détecteur de Mensonges : Les 7 signaux d'alerte universels

Le Détecteur de Mensonges : Les 7 signaux d'alerte universels

Dans le monde numérique, votre meilleure défense n'est pas un logiciel, mais votre capacité d'analyse. Les cybercriminels utilisent des techniques de psychologie pour contourner vos réflexes de sécurité.

Apprenez à identifier ces 7 signaux d'alerte. Si un seul de ces points est présent, la probabilité d'une tentative de fraude est extrêmement élevée.

Signal 1 : L'Urgence Artificielle

C'est l'outil numéro un des escrocs. Ils veulent vous placer dans un état de stress émotionnel pour court-circuiter votre esprit logique.

• Le message : "Votre compte sera supprimé dans 2 heures" ou "Une amende impayée va être majorée".

• Le but : Vous faire agir immédiatement, sans prendre le temps de vérifier l'information.

Signal 2 : L'Identité de l'Expéditeur

L'apparence d'un e-mail peut être trompeuse, mais l'adresse réelle ment rarement. Un nom d'affichage peut être "Ma Banque", alors que l'adresse derrière est fantaisiste.

• Le test : Cliquez ou survolez le nom de l'expéditeur pour voir l'adresse e-mail complète.

• Le piège : Une adresse finit par @gmail.com ou @outlook.fr pour un service officiel, ou contient des fautes (ex: @ameli-service-france.fr).

Signal 3 : La Demande de Données Sensibles

Une règle d'or absolue existe : aucune administration ou grande entreprise ne vous demandera vos identifiants par message.

• Ne communiquez jamais votre code de carte bancaire ou vos codes reçus par SMS.

• Méfiez-vous des demandes de mots de passe ou de copies de documents d'identité envoyées de manière impromptue.

Signal 4 : Les Promesses Trop Belles

Le phishing ne joue pas que sur la peur, il utilise aussi l'appât du gain. Si c'est trop beau pour être vrai, c'est que c'est un piège.

• Exemples classiques : Un tirage au sort gagné sans avoir participé, un héritage d'un lointain parent, ou un remboursement d'impôts inattendu.

• L'objectif : Vous inciter à remplir un formulaire pour "recevoir vos fonds", capturant ainsi vos données bancaires.

Signal 5 : Le Ton et l'Orthographe

Les escrocs automatisent leurs envois et utilisent parfois des outils de traduction de mauvaise qualité, même si les progrès de l'IA rendent ce signal plus difficile à détecter.

• Soyez attentif aux fautes de grammaire grossières.

• Repérez les formules de politesse inhabituelles ou un ton trop agressif/familier.

• Vérifiez la qualité des logos : s'ils sont flous ou déformés, soyez méfiant.

Signal 6 : L'Absence de Personnalisation

Les messages de phishing sont souvent envoyés à des milliers de personnes en même temps. Ils manquent de précision sur votre identité.

• Les salutations : Un message commençant par "Cher Client" ou "Cher Utilisateur" est suspect.

• Le manque de preuves : Une vraie banque citera souvent les derniers chiffres de votre compte ou votre conseiller référent.

Signal 7 : Les Liens et Pièces Jointes Masqués

Le lien est le piège qui vous transporte sur un faux site imitant parfaitement l'original.

• Le réflexe : Sur ordinateur, survolez le bouton (sans cliquer) pour voir l'adresse réelle apparaître en bas de votre écran.

• Les fichiers : Ne téléchargez jamais de pièces jointes dont l'extension est .zip, .exe ou .html provenant d'une source non vérifiée.

Votre Checklist Mentale avant le Clic

Avant chaque interaction avec un e-mail ou un SMS, cochez mentalement ces cases :

• Est-ce que j'attendais ce message précisément aujourd'hui ?

• Le ton cherche-t-il à me faire peur ou à m'exciter ?

• L'adresse de l'expéditeur semble-t-elle officielle et cohérente ?

• On me demande de cliquer : puis-je faire la même chose directement sur le site officiel ?

LE CONSEIL PRO : Appliquez toujours la règle de la "Contre-Vérification Hors Canal". Si vous recevez une alerte de votre banque, fermez le message, ouvrez votre navigateur et tapez vous-même l'adresse de votre banque, ou passez par l'application officielle. Si l'alerte est réelle, elle s'affichera dans votre espace sécurisé.

Chapitre 12

Panique à Bord : Que faire si vous avez été victime ?

Module : Panique à Bord : Que faire si vous avez été victime ?

Le choc est là : vous avez cliqué sur le mauvais lien, partagé un code confidentiel ou remarqué un retrait suspect. L'adrénaline monte, mais c'est le moment d'agir avec méthode.

Ce protocole d'urgence vous guide pas à pas pour limiter les dégâts et reprendre le contrôle de votre identité numérique.

Étape 1 : Coupez les vannes financières

Si vous avez donné vos coordonnées bancaires ou si vous constatez une fraude, chaque seconde compte pour protéger votre argent.

• Faites opposition immédiatement : Appelez votre banque ou le numéro d'urgence de votre carte bancaire (disponible 24h/24).

• Surveillez vos comptes : Listez les opérations suspectes pour les signaler précisément.

• Contestez les débits : Demandez le remboursement des opérations frauduleuses auprès de votre conseiller.

• Bloquez vos chéquiers : Si vos informations d'identité complètes ont été dérobées, demandez également une mise en opposition préventive.

Étape 2 : Verrouillez vos accès numériques

Si l'attaque concerne un compte en ligne (e-mail, réseaux sociaux, administration), vous devez isoler le pirate au plus vite.

• Changez vos mots de passe : En priorité celui de votre boîte mail principale et des comptes compromis.

• Utilisez des mots de passe uniques : Ne réutilisez jamais le même code sur plusieurs sites.

• Déconnectez toutes les sessions : Dans les paramètres de sécurité, choisissez l'option "Se déconnecter de tous les appareils".

• Activez la double authentification (2FA) : Ajoutez une couche de sécurité via SMS ou application (Google Authenticator, Authy).

Étape 3 : Collectez et préservez les preuves

L'erreur classique est d'effacer les traces par honte ou par colère. Ne supprimez rien. Ces éléments sont indispensables pour les autorités.

• Faites des captures d'écran : Photographiez l'e-mail de phishing, les SMS frauduleux ou les messages de menace.

• Notez les informations techniques : Relevez l'adresse e-mail de l'expéditeur, l'URL du site frauduleux et les numéros de téléphone utilisés.

• Conservez les e-mails : Ne les mettez pas à la corbeille, déplacez-les dans un dossier "Preuves".

Étape 4 : Alertez votre cercle de confiance

De nombreux scams consistent à pirater un compte pour demander de l'argent aux contacts de la victime en son nom.

• Prévenez vos proches : Envoyez un message général (ou passez des appels) pour

dire que votre compte a été piraté.

• Donnez une consigne claire : "Si vous recevez un message de ma part demandant de l'argent ou un code, ne répondez pas."

• Alertez vos collègues : Si l'attaque touche votre environnement professionnel, prévenez immédiatement votre service informatique.

Étape 5 : Signalez et déposez plainte

Le signalement permet de bloquer les sites malveillants et d'aider les autorités à identifier les réseaux de cybercriminels.

• Utilisez les plateformes officielles : Signalez le contenu sur Cybermalveillance.gouv.fr ou Pharos.

• Déposez plainte : Rendez-vous en gendarmerie ou au commissariat avec vos preuves.

• Utilisez la plateforme THÉSÉE : Pour les escroqueries sur internet, vous pouvez porter plainte directement en ligne.

LE CONSEIL PRO : Si vous craignez une usurpation d'identité après avoir envoyé vos documents officiels (carte d'identité, fiche de paie), déposez immédiatement une main-courante. Vous pouvez aussi ajouter un filigrane sur vos documents numériques à l'avenir grâce au service gratuit filigrane.beta.gouv.fr pour empêcher leur réutilisation par des fraudeurs.

Chapitre 13

Cyber-Hygiène : Les 10 commandements du citoyen connecté

Module : Cyber-Hygiène – Les 10 commandements du citoyen connecté

Adopter une hygiène numérique est aussi essentiel que de verrouiller sa porte d'entrée. Ce module vous guide pour instaurer une routine simple et efficace afin de protéger votre identité et vos biens numériques.

1. Tes logiciels, tu mettras à jour sans tarder

• Activez systématiquement les mises à jour automatiques sur votre smartphone, ordinateur et tablettes.

• Ces mises à jour ne servent pas qu'à ajouter des fonctions : elles bouchent des failles de sécurité exploitées par les pirates.

• N'oubliez pas votre box internet et vos objets connectés (caméras, montres).

2. Tes données précieuses, tu sauvegarderas

• Appliquez la règle du 3-2-1 : 3 copies de vos données, sur 2 supports différents (disque dur, clé USB), avec 1 copie hors ligne ou sur le Cloud.

• Planifiez une sauvegarde automatique une fois par semaine.

• Une sauvegarde récente est votre seule assurance vie contre les Ransomwares (logiciels de rançon).

3. Des mots de passe robustes, tu créeras

• Utilisez une phrase complexe ou une suite de mots aléatoires (ex:

Chapeau-Bleu-42-Guitare!).

• Chaque compte doit avoir un mot de passe unique. Si un site est piraté, vos autres comptes restent à l'abri.

• Utilisez un gestionnaire de mots de passe (comme Bitwarden ou Dashlane) pour ne plus avoir à les retenir.

4. La double authentification (MFA), tu activeras

• Activez la validation en deux étapes sur tous vos comptes sensibles (e-mails, banque, réseaux sociaux).

• Même si un pirate vole votre mot de passe, il ne pourra pas se connecter sans le code temporaire reçu sur votre téléphone.

• Privilégiez les applications d'authentification (Google Authenticator) aux SMS.

5. Ta discrétion sur les réseaux, tu cultiveras

• Évitez de partager des informations qui servent aux questions de récupération de compte (nom de votre animal, école primaire).

• Ne publiez jamais de photos de vos billets de train, documents officiels ou clés de maison.

• Réglez vos comptes sur "Privé" pour limiter la visibilité de vos publications aux seuls amis réels.

6. Avant de cliquer, sept fois tu réfléchiras

• Méfiez-vous des messages urgents ou alarmistes (ex: "Votre compte va être supprimé").

• Passez votre souris sur un lien pour vérifier l'adresse URL réelle avant de cliquer.

• Ne téléchargez jamais de pièces jointes provenant d'expéditeurs inconnus ou suspects.

7. Les Wi-Fi publics, avec prudence tu utiliseras

• Évitez de vous connecter à votre banque ou de faire des achats sur un Wi-Fi gratuit (gare, café).

• Si vous devez le faire, utilisez impérativement un VPN pour chiffrer votre connexion.

• Le plus sûr reste d'utiliser le partage de connexion de votre propre smartphone (4G/5G).

8. Tes applications, avec soin tu trieras

• Téléchargez uniquement vos applications sur les boutiques officielles (App Store, Google Play).

• Vérifiez les autorisations : une application de lampe-torche n'a pas besoin d'accéder à vos contacts ou à votre micro.

• Supprimez les applications que vous n'utilisez plus pour réduire votre surface d'exposition.

9. Le cadenas "HTTPS", tu vérifieras

• Avant de saisir des coordonnées bancaires, assurez-vous que l'URL commence par https:// et affiche un petit cadenas.

• Attention : le cadenas garantit que la connexion est chiffrée, mais pas que le site est honnête. Vérifiez toujours l'orthographe du nom de domaine.

10. Tes appareils physiques, tu verrouilleras

• Configurez un code de verrouillage complexe (6 chiffres minimum) ou utilisez la biométrie (empreinte, visage).

• Ne laissez jamais votre ordinateur ou téléphone sans surveillance dans un lieu public.

• Activez la fonction "Localiser mon appareil" pour pouvoir l'effacer à distance en cas de vol.

LE CONSEIL PRO : Une fois par mois, effectuez un "bilan de santé numérique". Vérifiez vos relevés bancaires, changez un mot de passe important et supprimez les comptes en ligne dont vous ne vous servez plus. La sécurité est un processus continu, pas un effort ponctuel.

Chapitre 14

Justice et Recours : Le guide des démarches légales

Justice et Recours : Le guide des démarches légales

Découvrir que l'on a été victime d'une escroquerie provoque souvent un sentiment de vulnérabilité. Pourtant, agir rapidement est essentiel pour limiter les dégâts et tenter d'obtenir réparation.

Étape 1 : Préserver l'intégrité des preuves

Avant de supprimer quoi que ce soit par colère ou par peur, vous devez figer la situation. Les preuves numériques sont volatiles.

• Réalisez des captures d'écran complètes des messages, emails ou pages web frauduleuses.

• Conservez précieusement les en-têtes (headers) des emails reçus.

• Notez les adresses URL exactes des sites de phishing.

• Gardez une trace de tous les échanges (SMS, messageries instantanées, appels).

• Récupérez vos relevés bancaires mettant en évidence les transactions suspectes.

Étape 2 : Utiliser les plateformes de signalement officielles

L'État français a mis en place des outils spécialisés pour traiter chaque type de cybercriminalité de manière efficace et rapide.

• PHAROS : Pour signaler les contenus illicites en ligne (sites de phishing, tentatives d'escroquerie visibles par tous).

• PERCEVAL : Indispensable en cas de fraude à la carte bancaire si vous êtes toujours en possession de votre carte physique.

• THESEE : La plateforme de plainte en ligne dédiée aux escroqueries sur internet (faux sites de vente, chantages, faux investissements).

• Signal-Conso : Pour signaler un litige commercial ou une pratique trompeuse avec une entreprise.

Étape 3 : Porter plainte officiellement

Le signalement ne remplace pas toujours la plainte. Pour déclencher une enquête pénale et espérer un remboursement, la plainte est obligatoire.

• Le commissariat ou la gendarmerie : Vous pouvez vous rendre sur place. Il est conseillé de remplir une pré-plainte en ligne pour gagner du temps.

• Le Procureur de la République : Vous pouvez envoyer une lettre recommandée avec accusé de réception directement au tribunal judiciaire du lieu de l'infraction ou de votre domicile.

• Les délais : Vous disposez de 6 ans pour porter plainte pour une escroquerie, mais chaque jour compte pour bloquer les fonds.

Étape 4 : Contacter sa banque et ses assurances

Le volet judiciaire doit s'accompagner d'un volet financier immédiat.

• Faites opposition immédiatement sur vos moyens de paiement.

• Demandez le "Chargeback" (rétrofacturation) auprès de votre conseiller si la fraude concerne un achat par carte.

• Vérifiez vos contrats d'assurance : beaucoup incluent une protection juridique ou une garantie contre l'usurpation d'identité.

Étape 5 : S'entourer d'associations d'aide aux victimes

Vous n'êtes pas seul face à cette épreuve. Des structures gratuites vous accompagnent dans vos démarches juridiques et psychologiques.

• France Victimes : Un réseau national qui offre une écoute et des conseils juridiques gratuits au 116 006.

• Info Escroqueries : Une plateforme d'information joignable au 0 805 805 817 pour identifier le type d'arnaque.

• Cybermalveillance.gouv.fr : Un portail complet pour obtenir un diagnostic et être mis en relation avec des prestataires spécialisés.

LE CONSEIL PRO : Ne cédez jamais à la "double arnaque". De nombreux escrocs recontactent leurs victimes en se faisant passer pour des experts en récupération de fonds ou des agents de police. Sachez que les autorités officielles ne vous demanderont jamais d'argent pour résoudre une enquête ou récupérer vos pertes.

FIN

Merci d'avoir lu "Scams & Phishing"

Une œuvre écrite par Fusianima Expert

Lire la version interactive et commenter

Découvrir les autres œuvres de l'auteur