LE GUIDE DES ARNAQUES

ÉDITION FUSIANIMA

Le Guide Des Arnaques

Par Fusianima Expert

ÉDITIONS FUSIANIMA

Lire la version interactive sur Fusianima.com

Table des matières

Chapitre 1

Comprendre la psychologie du pirate : Pourquoi on se fait tous piéger ?

Comprendre la psychologie du pirate : Pourquoi on se fait tous piéger ?

Contrairement aux idées reçues, se faire escroquer en ligne n'est pas une question d'intelligence ou d'âge. Les pirates ne s'attaquent pas à votre ordinateur, ils s'attaquent à votre cerveau. C'est ce qu'on appelle l'ingénierie sociale : l'art de manipuler l'humain pour obtenir un mot de passe ou de l'argent.

Point Clé 1 : Le mécanisme de "l'interrupteur émotionnel"

Pour réussir leur coup, les escrocs cherchent à éteindre votre cerveau logique (celui qui réfléchit et analyse) pour allumer votre cerveau émotionnel (celui qui réagit par instinct). Voici comment ils s'y prennent :

• Ils créent une situation de stress intense pour court-circuiter votre réflexion.

• Ils vous placent dans une position où vous devez agir immédiatement.

• Ils utilisent des mots familiers et des logos rassurants pour endormir votre méfiance.

• Ils exploitent nos réflexes sociaux naturels (l'obéissance, l'envie d'aider, la peur de l'erreur).

Point Clé 2 : Le levier de l'Urgence (Le temps presse)

C'est l'outil le plus utilisé. L'objectif est de vous empêcher de demander conseil à un proche ou de vérifier l'information.

• Le message type : "Votre compte sera supprimé dans 2 heures si vous ne validez pas vos coordonnées."

• Pourquoi ça marche : Le sentiment d'urgence provoque une poussée d'adrénaline qui nous pousse à agir avant de réfléchir.

• Le piège : On clique sur le lien pour "sauver" son compte, sans remarquer que l'adresse email de l'expéditeur est bizarre.

Point Clé 3 : Le levier de la Peur (La menace)

La peur est une émotion paralysante que les pirates adorent exploiter pour vous faire perdre vos moyens.

• Le message type : "Une plainte a été déposée contre vous" ou "Votre colis est bloqué et va être renvoyé".

• Le rôle de la peur : Elle crée un besoin immédiat de résolution de problème.

• L'objectif : Vous faire payer une "petite taxe" ou remplir un formulaire contenant vos données bancaires pour "débloquer" la situation.

Point Clé 4 : Le levier de l'Autorité (L'uniforme numérique)

Nous sommes conditionnés depuis l'enfance à respecter l'autorité. Les pirates usurpent donc des identités prestigieuses.

• Les identités volées : La Gendarmerie, les Impôts, l'Assurance Maladie (Ameli), ou même votre propre banquier.

• La technique : Utiliser des termes techniques, des références de lois ou des logos officiels pour paraître légitime.

• Le résultat : On n'ose pas contredire ou poser de questions à une figure d'autorité perçue.

Point Clé 5 : Le levier de l'Appât du gain (La chance inespérée)

Ici, le pirate utilise une émotion positive mais tout aussi aveuglante : l'excitation.

• Le message type : "Félicitations, vous avez gagné un iPhone" ou "Un remboursement de 300€ vous attend".

• La psychologie : Notre cerveau adore les récompenses gratuites et rapides.

• Le danger : L'envie d'obtenir le gain nous fait ignorer tous les signaux d'alerte (le "trop beau pour être vrai").

Point Clé 6 : Pourquoi personne n'est à l'abri ?

Il est crucial de comprendre que la vulnérabilité est humaine et non technique. Vous pouvez vous faire piéger si :

• Vous êtes fatigué ou distrait (fin de journée, multitâche).

• Vous traversez une période de stress personnel.

• Le message tombe au moment parfait (ex: vous attendez réellement un colis).

• Le pirate possède une information réelle sur vous (votre nom ou votre ville) qui vous met en confiance.

LE CONSEIL PRO : Face à un message alarmant ou trop séduisant, appliquez la "Règle des 10 secondes". Posez votre téléphone, respirez, et demandez-vous : "Si je ne fais rien tout de suite, que se passe-t-il vraiment ?". Dans 99% des cas, l'urgence est artificielle et créée uniquement par le pirate pour vous manipuler.

Chapitre 2

Le Bouclier Mental : La méthode de détection ultra-rapide en 3 étapes

Module : Le Bouclier Mental - La méthode de détection ultra-rapide

Face à l'explosion des tentatives d'arnaques par SMS, e-mail ou messagerie, il est normal de se sentir vulnérable. Ce module vous enseigne le Bouclier Mental : un protocole simple qui s'active en quelques secondes pour vous protéger efficacement.

L'objectif n'est pas de devenir un expert en informatique, mais de développer un réflexe de prudence systématique avant chaque clic.

Étape 1 : Le Contrôle d'Identité (L'Émetteur)

La première technique des escrocs est de se faire passer pour quelqu'un d'autre (votre banque, l'Assurance Maladie, Netflix, ou même un proche). Ne vous fiez jamais au nom qui s'affiche en gros.

• Vérifiez l'adresse mail complète : Cliquez ou passez votre souris sur le nom de l'expéditeur pour voir l'adresse réelle. Si elle se termine par une suite de chiffres bizarres ou un nom de domaine inconnu (ex: @service-securite-portail-78.com), c'est une arnaque.

• Méfiez-vous des numéros mobiles : Une administration officielle ou une grande entreprise n'utilise quasiment jamais un numéro de portable classique (commençant par 06 ou 07) pour vous demander une action urgente.

• Cherchez l'anomalie : Un seul caractère peut changer. Par exemple, "service@ameli.fr" est correct, mais "service@amellii.fr" est une imitation.

Étape 2 : L'Analyse de la Demande (Le Fond)

Une fois l'identité vérifiée, posez-vous la question : "Est-ce que cette demande est logique et habituelle ?". Les arnaqueurs jouent sur vos émotions pour vous faire perdre votre discernement.

• Le sentiment d'urgence : Si le message dit "Agissez vite", "Sous 24h", ou "Votre compte va être bloqué", c'est un signal d'alerte majeur. L'urgence est l'outil préféré des voleurs.

• La promesse d'un gain ou d'un remboursement : Un colis en attente, une amende impayée alors que vous ne conduisez pas, ou un remboursement d'impôts inattendu sont des appâts classiques.

• La demande d'informations sensibles : Retenez cette règle d'or : Aucune banque ni administration ne vous demandera votre mot de passe ou votre numéro de carte bancaire par message.

Étape 3 : La Détection Structurelle (La Forme)

Même si l'escroc est doué, il laisse souvent des traces de son passage. Apprenez à regarder les détails techniques et visuels du message.

• L'orthographe et la ponctuation : Les institutions officielles font très peu de fautes. Un texte avec des majuscules partout, des fautes de grammaire ou une mise en page "bricolée" doit vous alerter.

• Le lien (URL) : Avant de cliquer, regardez l'adresse du lien. Si elle ne correspond pas exactement au site officiel (ex: "impots-gouv-paiement.net" au lieu de "impots.gouv.fr"), ne cliquez pas.

• La personnalisation : Un message qui commence par "Cher client" ou "Cher utilisateur" au lieu de votre Nom et Prénom est suspect. Les services qui possèdent réellement votre dossier connaissent votre identité.

LE CONSEIL PRO : En cas de doute, la règle d'or est le "Contournement". Ne cliquez jamais sur le lien du message. Fermez l'e-mail ou le SMS, et connectez-vous vous-même sur le site officiel en tapant l'adresse dans votre navigateur, ou utilisez l'application officielle que vous avez déjà installée. Si une action est vraiment nécessaire, vous y trouverez une notification sécurisée.

Chapitre 3

Votre Trousse de Survie Numérique : Les outils indispensables de protection

Votre Trousse de Survie Numérique : Les outils indispensables de protection

Bienvenue dans cette étape cruciale. Pour naviguer sereinement sur Internet, il ne suffit pas d'être vigilant : il faut aussi s'équiper des bons outils de défense. Considérez ce module comme la mise en place d'une porte blindée et d'un système d'alarme pour votre vie numérique.

Pas d'inquiétude : nous allons avancer pas à pas, avec des solutions simples et accessibles, même si vous débutez totalement.

Étape 1 : Le Gestionnaire de Mots de Passe (Votre mémoire numérique)

C’est l’outil numéro 1. Au lieu de retenir 50 mots de passe compliqués (ou d'utiliser le même partout, ce qui est très dangereux), vous n'en retenez qu'un seul : le mot de passe maître.

• Pourquoi l'utiliser : Il crée des mots de passe impossibles à deviner pour les pirates et les remplit automatiquement pour vous.

• Solution Gratuite : Bitwarden (très sécurisé et simple).

• Solution Payante : Dashlane ou 1Password (offrent une assistance simplifiée et une interface très élégante).

• Comment l'installer :

• Téléchargez l'application sur votre téléphone ou l'extension sur votre

ordinateur.

• Créez votre compte principal avec une phrase longue que vous n'oublierez jamais.

• Laissez l'outil enregistrer vos accès au fur et à mesure de vos connexions.

Étape 2 : La Double Authentification ou 2FA (Le deuxième verrou)

Même si un pirate vole votre mot de passe, la Double Authentification l'empêche d'entrer. C'est un code temporaire que vous recevez (souvent sur votre téléphone) pour confirmer que c'est bien vous.

• Le principe : C'est comme à la banque : vous insérez votre carte (ce que vous possédez) ET votre code secret (ce que vous savez).

• Outils recommandés : Google Authenticator ou Microsoft Authenticator (gratuits).

• Mise en place :

• Allez dans les réglages "Sécurité" de vos comptes importants (Email, Banque, Facebook).

• Activez la "Validation en deux étapes".

• Scannez le QR Code affiché avec l'application sur votre téléphone.

Étape 3 : Le Bloqueur de Publicités (Votre bouclier anti-pièges)

Beaucoup d'arnaques commencent par une fausse publicité ou une fenêtre surgissante (pop-up) qui vous annonce un faux virus. Le bloqueur empêche ces pièges de s'afficher.

• L'outil indispensable : uBlock Origin. C'est entièrement gratuit et c'est le plus efficace.

• Avantages : Navigation plus rapide, moins de pollution visuelle et protection contre les sites malveillants.

• Comment l'installer :

• Ouvrez votre navigateur (Chrome, Firefox ou Edge).

• Cherchez "uBlock Origin" dans le magasin d'extensions.

• Cliquez sur "Ajouter". C'est terminé, il travaille déjà pour vous !

Étape 4 : Le VPN (Le tunnel de navigation privé)

Un VPN masque votre présence sur Internet et chiffre vos données. C'est indispensable si vous vous connectez souvent à des réseaux Wi-Fi publics (cafés, gares, hôtels).

• Quand l'utiliser : Surtout pour vos achats ou vos opérations bancaires hors de chez vous.

• Solution Gratuite (Limitée) : ProtonVPN (respecte votre vie privée).

• Solutions Payantes : NordVPN ou CyberGhost (très rapides et simples avec un gros bouton "Connexion").

• Installation :

• Installez l'application sur votre ordinateur ou smartphone.

• Lancez l'application et cliquez sur "Connexion Rapide".

• Votre connexion est désormais illisible pour les curieux.

LE CONSEIL PRO : Ne cherchez pas à tout installer en une seule journée. Commencez par le Gestionnaire de Mots de Passe aujourd'hui. Une fois que vous êtes à l'aise, installez le Bloqueur de Publicités demain. La sécurité numérique est un marathon, pas un sprint. Votre sérénité vaut bien ces quelques minutes d'installation !

Chapitre 4

Le Top 20 des Arnaques - Vol d'identité et Phishing : Les classiques redoutables

Comprendre le vol d'identité et le phishing : Les bases

Pour bien vous protéger, il faut d'abord comprendre l'objectif des pirates : voler vos informations personnelles (nom, numéro de sécurité sociale, mots de passe) ou vos coordonnées bancaires. Ils utilisent pour cela une technique appelée le phishing (ou hameçonnage), qui consiste à se faire passer pour un organisme de confiance.

Point Clé 1 : Le Phishing par Email (L'hameçonnage classique)

C'est la méthode la plus ancienne mais elle fonctionne toujours. Vous recevez un message qui semble provenir d'un service officiel pour vous demander une action immédiate.

• Le prétexte : Une facture impayée, un colis bloqué, ou un remboursement en votre faveur.

• Le sentiment d'urgence : Le message dit souvent "Action requise sous 24h" ou "Votre compte va être suspendu".

• Le piège : Un bouton ou un lien qui vous dirige vers un faux site ressemblant à l'original pour voler vos codes.

• Comment le démasquer : Vérifiez l'adresse de l'expéditeur. Si elle semble bizarre (ex: securite@vrai-site-123.com), c'est une arnaque.

Point Clé 2 : Le Smishing (Arnaques par SMS)

Le "Smishing" est simplement du phishing par SMS. C'est aujourd'hui la méthode préférée des escrocs car nous faisons souvent moins attention sur nos téléphones.

• L'arnaque Assurance Maladie (Ameli) : Vous recevez un SMS disant que votre nouvelle carte Vitale est disponible ou qu'un remboursement est en attente.

• L'arnaque Crit'Air : Un message prétend que vous n'avez pas votre vignette pollution et que vous risquez une amende.

• Le lien suspect : Le SMS contient toujours un lien court vers un site frauduleux conçu pour copier vos coordonnées bancaires.

• Règle d'or : L'Assurance Maladie ou les services de l'État ne demandent jamais de coordonnées bancaires par SMS.

Point Clé 3 : Le Spoofing Bancaire (L'appel du faux conseiller)

Cette technique est particulièrement effrayante car elle utilise la manipulation par téléphone. C'est une étape supérieure dans le vol d'identité.

• L'affichage du numéro : Le pirate utilise un logiciel pour faire apparaître le vrai numéro de votre banque sur votre écran de téléphone.

• Le scénario : La personne se présente comme un conseiller du service fraude et vous informe d'une opération suspecte en cours sur votre compte.

• La demande : Pour "annuler" la transaction, elle vous demande de valider une notification sur votre application bancaire ou de donner vos codes secrets.

• La réalité : En validant, vous ne bloquez rien du tout : vous autorisez en réalité le virement du pirate.

Point Clé 4 : Comment repérer et éviter ces pièges ?

Même si vous débutez, certains signes ne trompent jamais. Adoptez ces réflexes

simples pour devenir inattaquable.

• Ne cliquez jamais sur les liens : Si vous recevez une alerte, fermez le message et allez directement sur le site officiel en tapant l'adresse vous-même dans votre navigateur.

• Observez l'orthographe : Les arnaques contiennent souvent des fautes de français ou des tournures de phrases étranges.

• Méfiez-vous de l'inconnu : Un organisme officiel ne vous demandera jamais votre mot de passe ou votre code de carte bleue.

• Prenez votre temps : L'urgence est l'outil du voleur. Si on vous presse, raccrochez ou supprimez le message.

LE CONSEIL PRO : En cas de doute lors d'un appel de votre "banquier", raccrochez immédiatement. Appelez ensuite vous-même votre conseiller habituel avec le numéro que vous avez sur vos relevés papier. Si c'était un vrai problème, il sera au courant. Sinon, vous venez d'éviter une grosse arnaque !

Chapitre 5

Le Top 20 des Arnaques - Shopping et Petites Annonces : Éviter les pièges financiers

Introduction : Acheter en toute sécurité sur Internet

Faire ses courses ou dénicher de bonnes affaires sur Internet est devenu une habitude pour beaucoup d'entre nous. Cependant, cet univers regorge de pièges financiers conçus pour tromper même les plus prudents. Ce module vous apprend à identifier les trois arnaques les plus fréquentes dans le domaine du shopping en ligne et des petites annonces.

1. Les fausses boutiques en ligne : Le miroir aux alouettes

Cette arnaque consiste à créer un site internet de vente qui ressemble à s'y méprendre à celui d'une grande marque ou d'un magasin professionnel, mais qui n'existe que pour voler votre argent.

Étape 1 : Comment repérer une fausse boutique ?

• Des prix anormalement bas : si un produit de luxe ou un appareil électronique est affiché à -80 %, méfiez-vous immédiatement.

• Une publicité alléchante sur les réseaux sociaux (Facebook, Instagram) qui vous redirige vers un site inconnu.

• L'absence de mentions légales ou de conditions générales de vente (CGV) claires.

• Une adresse URL (le nom du site) bizarre, par exemple "nom-de-marque-pas-cher.fr" ou contenant des fautes d'orthographe.

Étape 2 : Les conséquences pour l'acheteur

• Vous payez votre commande mais vous ne recevez jamais le produit.

• Vos coordonnées bancaires sont récupérées par les escrocs pour effectuer d'autres achats à votre insu.

• Vous recevez une contrefaçon de mauvaise qualité, voire dangereuse.

2. L'arnaque au trop-perçu sur les sites de petites annonces

Cette méthode cible particulièrement les vendeurs sur des sites comme Leboncoin ou Facebook Marketplace. L'escroc se fait passer pour un acheteur très intéressé.

Étape 1 : Le mécanisme de la fraude

• L'acheteur accepte votre prix sans négocier et se montre très pressé.

• Il vous envoie un faux règlement (souvent un faux virement ou un faux chèque) d'un montant supérieur au prix de l'objet.

• Il vous contacte en prétendant avoir fait une erreur de saisie et vous demande de lui rembourser la "différence" par virement ou ticket prépayé.

Étape 2 : Le piège se referme

• Le paiement initial de l'acheteur est fictif ou annulé par la banque quelques jours plus tard.

• L'argent que vous avez "remboursé", lui, est réel et définitivement perdu.

• L'escroc disparaît et bloque votre numéro de téléphone.

3. Les faux transporteurs et frais de douane fictifs

Vous recevez un SMS ou un e-mail vous informant qu'un colis vous attend, mais

qu'une petite somme doit être réglée pour le livrer.

Étape 1 : Le message d'alerte

• Le message utilise souvent le nom de transporteurs connus (La Poste, Chronopost, DHL, UPS).

• Il indique que votre colis est "suspendu" ou "bloqué en douane".

• On vous demande de cliquer sur un lien pour payer une somme dérisoire (souvent entre 1€ et 3€).

Étape 2 : Le vol de données bancaires

• Le lien vous dirige vers un faux site de paiement très réaliste.

• En saisissant vos numéros de carte pour payer les 2€, vous donnez en réalité l'accès total à votre compte aux fraudeurs.

• Certains escrocs en profitent pour mettre en place un abonnement caché très coûteux prélevé chaque mois.

Résumé des bons réflexes à adopter

• Vérifiez l'URL : Tapez vous-même l'adresse du site dans votre navigateur plutôt que de cliquer sur un lien reçu.

• Privilégiez le paiement sécurisé : Utilisez les systèmes intégrés des plateformes (comme celui de Leboncoin) qui protègent l'argent jusqu'à la réception.

• Ne remboursez jamais un trop-perçu : Si un acheteur s'est trompé, demandez à votre banque d'annuler l'opération, mais ne faites pas de virement inverse.

• Méfiez-vous de l'urgence : Les escrocs créent toujours un sentiment de panique pour vous empêcher de réfléchir.

LE CONSEIL PRO :

Avant d'acheter sur un nouveau site, effectuez toujours une recherche rapide sur un moteur de recherche en tapant le "nom du site + avis" ou "nom du site + arnaque". Si le site est frauduleux, d'autres victimes l'auront probablement déjà signalé sur des forums ou des plateformes de signalement.

Chapitre 6

Le Top 20 des Arnaques - Sentiments et Argent : Les manipulations émotionnelles

Le Top 20 des Arnaques : Quand l'émotion brouille le jugement

Dans ce module, nous abordons la forme la plus redoutable de manipulation : celle qui s'attaque à vos sentiments. Qu'il s'agisse d'amour, de l'espoir d'une vie meilleure ou de l'envie de mettre votre famille à l'abri, les escrocs utilisent vos émotions pour désactiver votre sens critique.

1. L'Arnaque Sentimentale (Le phénomène des "Brouteurs")

L'arnaque sentimentale est une manipulation de longue durée. L'escroc, souvent appelé "brouteur", crée un faux profil avec des photos volées (mannequins, militaires, infirmières) pour vous séduire sur les réseaux sociaux ou les sites de rencontre.

• La phase de séduction : L'arnaqueur vous couvre de compliments et feint le coup de foudre immédiat. Il passe des heures à discuter avec vous pour créer un lien intime.

• Le déclencheur : Une fois votre confiance acquise, un drame imprévu survient (accident, maladie, problème de passeport, héritage bloqué).

• La demande d'argent : Il vous demande une aide financière "temporaire", souvent via des moyens intraçables comme des coupons PCS, Transcash ou des mandats Western Union.

• Le chantage : Si vous refusez, il culpabilise ou menace de mettre fin à la relation, voire de diffuser des contenus compromettants si vous en avez partagé.

2. Les Fausses Offres d'Emploi à Domicile

Cette arnaque cible les personnes en recherche d'activité ou souhaitant un complément de revenu. Elle joue sur l'espoir d'une vie professionnelle plus facile et moins stressante.

• L'annonce alléchante : On vous propose un poste de "secrétaire", "testeur de produits" ou "gestionnaire de paiements" avec un salaire élevé pour peu d'heures de travail.

• Le faux recrutement : Tout se passe par messagerie (WhatsApp ou Telegram). Il n'y a jamais d'entretien physique ou en visioconférence réelle.

• Le piège de l'avance : L'employeur vous envoie un chèque pour acheter votre matériel (ordinateur, imprimante). Il vous demande de renvoyer le surplus par virement.

• La réalité brutale : Le chèque reçu est volé ou faux. Votre banque l'annule après quelques jours, mais l'argent que vous avez renvoyé de votre poche, lui, est définitivement perdu.

3. Le Mirage des Cryptomonnaies "Miracles"

Ici, les escrocs utilisent la peur de "rater le train" de la richesse technologique. Ils vous promettent des rendements exceptionnels sans aucun risque.

• La publicité ciblée : Vous voyez une publicité sur Facebook ou Instagram utilisant l'image d'une célébrité (Elon Musk, un présentateur TV connu) vantant une plateforme d'investissement.

• Le conseiller dédié : Un prétendu "expert" vous appelle pour vous guider. Il se montre très rassurant et pédagogue au début.

• Le tableau de bord factice : On vous demande de miser une petite somme (souvent 250 €). Sur le site, vous voyez vos gains grimper virtuellement de façon spectaculaire pour vous inciter à miser plus.

• L'impossibilité de retrait : Le jour où vous voulez récupérer votre argent, on vous demande de payer des "frais de sortie" ou des "taxes" imaginaires. Vous ne récupérez jamais votre capital.

Comment reconnaître une manipulation émotionnelle ?

Voici des signes qui doivent impérativement vous alerter, quel que soit le domaine :

• L'urgence : L'interlocuteur vous pousse à agir immédiatement pour ne pas "perdre l'opportunité" ou pour "le sauver".

• Le secret : On vous demande de ne pas en parler à vos proches ou à votre banquier (sous prétexte de surprise ou de confidentialité professionnelle).

• L'absence de contact réel : La personne trouve toujours une excuse pour ne pas allumer sa caméra ou ne pas vous rencontrer en vrai (micro cassé, zone de guerre, voyage à l'étranger).

• Le mode de paiement : Dès que l'on vous demande des tickets prépayés ou des cryptomonnaies pour une transaction administrative ou personnelle, c'est une arnaque dans 100% des cas.

LE CONSEIL PRO : Appliquez toujours la "Règle des 24 heures". Avant d'envoyer de l'argent ou de donner vos coordonnées bancaires à quelqu'un rencontré sur internet, attendez une journée entière et parlez-en à une personne de confiance de votre entourage physique. Le simple fait d'expliquer la situation à voix haute suffit souvent à briser le sort de la manipulation.

Chapitre 7

Mise en situation : Votre premier audit de sécurité en 30 minutes

Introduction : Pourquoi faire un audit de sécurité ?

Félicitations ! En décidant de consacrer 30 minutes à cet exercice, vous reprenez le contrôle de votre vie numérique. Un audit de sécurité n'est pas réservé aux experts en informatique. C'est simplement une vérification de routine, comme un contrôle technique pour votre voiture, afin de s'assurer que vos portes sont bien verrouillées face aux arnaqueurs.

Ce guide vous accompagne pas à pas, avec bienveillance et simplicité. Munissez-vous d'un papier et d'un stylo, et c'est parti !

Étape 1 : Vérifier si vos données sont déjà "dehors" (10 minutes)

Vérification des fuites de données

Les arnaqueurs utilisent souvent des bases de données volées lors de piratages de grands sites (comme Facebook, LinkedIn ou des sites de e-commerce). Voici comment savoir si vous êtes concerné :

• Rendez-vous sur le site de référence : Have I Been Pwned (haveibeenpwned.com).

• Tapez votre adresse email principale dans la barre de recherche.

• Si le résultat est rouge : Cela signifie que vos données (email, mot de passe, etc.) ont fuité lors d'un piratage passé. Pas de panique, cela arrive à presque tout le monde.

• Si le résultat est vert : Félicitations, votre adresse n'apparaît pas dans les fuites de

données majeures connues.

Action immédiate en cas de fuite

Si votre email est apparu en rouge, vous devez agir sur le compte concerné :

• Identifiez le site web mentionné dans la liste en bas de page.

• Si vous utilisez encore ce site, changez immédiatement le mot de passe de ce compte.

• Important : Si vous utilisiez ce même mot de passe sur d'autres sites (votre banque, vos impôts), changez-les également partout.

Étape 2 : Sécuriser vos "Comptes Piliers" (10 minutes)

Identifier vos comptes prioritaires

Tous les comptes ne se valent pas. Si un arnaqueur accède à votre compte Netflix, c'est agaçant. S'il accède à votre boîte mail, il peut réinitialiser les mots de passe de TOUS vos autres comptes.

• Le compte Email : C'est la clé de votre château.

• Le compte Bancaire : C'est là où se trouve l'argent.

• Les réseaux sociaux : C'est votre identité vis-à-vis de vos proches.

Activer la Double Authentification (A2F)

C'est l'étape la plus importante de cet audit. La double authentification ajoute une "deuxième serrure" (souvent un code reçu par SMS ou via une application).

• Allez dans les Paramètres de sécurité de votre compte Gmail, Outlook ou de votre banque.

• Cherchez l'option "Validation en deux étapes" ou "Double authentification".

• Activez-la. Désormais, même si un arnaqueur trouve votre mot de passe, il ne pourra pas entrer sans ce code unique envoyé sur votre téléphone.

Étape 3 : Faire le ménage dans vos mots de passe (5 minutes)

Évaluer la force de vos accès

Un bon mot de passe ne doit pas être facile à deviner (évitez le nom de votre chien ou votre date de naissance).

• Règle d'or : Un mot de passe différent pour chaque site important.

• Utilisez des phrases de passe : plus longues, plus faciles à retenir, mais impossibles à deviner pour une machine (ex: "LeChatBleuMange3Pommes!").

• Astuce : Évitez d'écrire vos mots de passe sur un post-it collé à l'écran. Utilisez plutôt la fonction "Mots de passe" sécurisée de votre smartphone ou de votre navigateur (Chrome/Safari).

Étape 4 : Nettoyer votre présence numérique (5 minutes)

Supprimer l'inutile pour réduire les risques

Moins vous laissez de traces, moins les arnaqueurs ont d'informations pour vous piéger (usurpation d'identité, phishing ciblé).

• Supprimez les vieux comptes : Si vous n'utilisez plus un site depuis 2 ans, supprimez votre compte.

• Vérifiez la confidentialité : Sur Facebook ou Instagram, passez votre profil en "Privé" pour que seuls vos amis voient vos photos et informations.

• Nettoyez vos applications : Sur votre téléphone, désinstallez les applications que

vous n'utilisez jamais ; elles collectent souvent des données en arrière-plan.

LE CONSEIL PRO : Adoptez un gestionnaire de mots de passe (comme Bitwarden ou Dashlane). C'est un coffre-fort numérique gratuit qui retient tous vos mots de passe compliqués à votre place. Vous n'aurez plus qu'un seul mot de passe à retenir : celui du coffre ! C'est l'outil ultime pour passer de "vulnérable" à "blindé" en quelques minutes.

Chapitre 8

Cellule de Crise : Que faire si vous avez cliqué ou si vous êtes victime ?

Cellule de Crise : Que faire si vous avez cliqué ou si vous êtes victime ?

Si vous lisez ces lignes parce que vous venez de transmettre vos coordonnées ou de cliquer sur un lien douteux, la première chose à faire est de respirer. Vous n'êtes pas seul, et des solutions existent pour limiter les dégâts.

Agir avec méthode et rapidité est la clé pour reprendre le contrôle. Voici votre protocole d'urgence, étape par étape.

Étape 1 : Couper l'accès à votre argent (Urgence Absolue)

Si vous avez donné vos numéros de carte bancaire ou vos identifiants de connexion à votre banque, chaque minute compte.

• Appelez votre banque immédiatement : Utilisez le numéro d'urgence disponible au dos de votre carte ou sur l'application officielle de votre banque.

• Faites opposition : Demandez le blocage complet de votre carte bancaire et de vos accès de banque en ligne.

• Contestez les opérations : Si des paiements suspects apparaissent déjà, signalez-les immédiatement à votre conseiller pour tenter un remboursement.

• Vérifiez vos prélèvements : Assurez-vous qu'aucun nouvel "ordre de virement" ou "nouvel ajout de bénéficiaire" n'a été programmé à votre insu.

Étape 2 : Signaler l'arnaque sur les plateformes officielles

Signaler n'est pas seulement utile pour vous, cela permet aussi de protéger les autres en faisant fermer les sites des fraudeurs.

• Phishing-initiative.fr : Si vous avez reçu un email ou un SMS frauduleux, copiez le lien et collez-le sur ce site pour qu'il soit analysé et bloqué sur les navigateurs.

• Cybermalveillance.gouv.fr : C'est la plateforme de référence. Elle vous guidera vers les bons formulaires et pourra vous mettre en relation avec des professionnels si votre ordinateur est infecté.

• Signal-Spam.fr : Pour signaler les emails indésirables qui encombrent votre boîte de réception.

Étape 3 : Le dépôt de plainte et le recours juridique

Pour être remboursé par certaines assurances ou pour que la police puisse enquêter, une trace officielle est indispensable.

• Utilisez PERCEVAL : Si vos coordonnées bancaires ont été utilisées pour un achat en ligne alors que vous avez toujours votre carte physique en main, déclarez la fraude sur la plateforme Perceval (via le site Service-Public.fr). C'est un document officiel rapide à obtenir.

• Déposez une plainte : Si vous avez subi un préjudice financier direct (virement effectué de votre plein gré sous la pression) ou un vol d'identité, rendez-vous au commissariat ou à la gendarmerie.

• Gardez les preuves : Ne supprimez rien. Prenez des captures d'écran des messages, notez les adresses emails des fraudeurs et les numéros de téléphone utilisés.

Étape 4 : Sécuriser votre environnement numérique

Une fois l'urgence financière gérée, il faut "fermer les portes" de votre vie numérique.

• Changez vos mots de passe : Si vous avez utilisé le même mot de passe sur le site frauduleux que sur d'autres comptes (Gmail, Facebook, etc.), changez-les immédiatement partout.

• Activez la double authentification (2FA) : C'est l'option qui demande un code par SMS ou via une application pour valider une connexion. C'est votre meilleure armure.

• Lancez un scan antivirus : Si vous avez téléchargé une pièce jointe ou installé un logiciel sur demande du fraudeur, votre appareil est peut-être infecté.

LE CONSEIL PRO : Ne répondez JAMAIS aux relances des fraudeurs après avoir coupé le contact. Ils essaieront souvent de vous recontacter en se faisant passer pour la police ou un service de "récupération de fonds" pour vous arnaquer une seconde fois. Coupez tout dialogue définitivement.

Chapitre 9

Maintenir sa vigilance : Comment rester à jour face aux nouvelles menaces

Maintenir sa vigilance : Comment rester à jour face aux nouvelles menaces

Le monde du numérique évolue très vite. Aujourd'hui, les escrocs utilisent l'Intelligence Artificielle (IA) pour créer des pièges de plus en plus réalistes. Pas d'inquiétude : même si la technologie change, les bons réflexes restent les mêmes.

Étape 1 : Comprendre les "Deepfakes" (Images et Vidéos Truquées)

Un "Deepfake" est une technologie qui permet de remplacer le visage ou la voix d'une personne par une autre sur une vidéo. C'est un véritable masque numérique.

• Le but des arnaqueurs : Vous faire croire qu'une célébrité ou un politicien vous recommande un investissement miracle.

• Comment les repérer : Regardez attentivement les clignotements d'yeux (souvent absents ou irréguliers).

• Observez les détails : Les contours du visage peuvent paraître flous ou "vibrer" lorsque la personne bouge la tête.

• Le son et l'image : Vérifiez si les mouvements des lèvres sont parfaitement synchronisés avec les paroles.

Étape 2 : Déjouer le clonage de voix

C'est l'une des menaces les plus impressionnantes : l'escroc utilise un logiciel pour imiter la voix d'un de vos proches (votre enfant, votre petit-enfant ou un ami).

• Le scénario classique : Vous recevez un appel d'un numéro inconnu. La voix ressemble à celle d'un proche qui prétend être en urgence absolue (accident, vol de téléphone, garde à vue) et demande de l'argent.

• L'émotion : L'arnaqueur joue sur la panique pour vous empêcher de réfléchir.

• Le réflexe de sécurité : Raccrochez immédiatement et tentez de joindre votre proche sur son numéro habituel ou contactez un autre membre de la famille pour vérifier l'information.

Étape 3 : Instaurer un "Mot de Passe" familial

Puisque la voix et l'image peuvent être imitées, il faut une preuve que l'on ne peut pas copier.

• Le concept : Convenez d'un mot secret ou d'une question personnelle simple avec vos proches (ex: "Quel était le nom de notre premier chien ?").

• L'usage : Si quelqu'un vous appelle en prétendant être un proche en détresse, demandez-lui ce mot secret.

• La règle d'or : Si l'interlocuteur ne peut pas répondre, c'est une arnaque, peu importe la ressemblance de la voix.

Étape 4 : S'informer régulièrement sans effort

La vigilance n'est pas une peur constante, c'est une habitude à prendre. Pour rester informé des nouvelles ruses, utilisez des sources fiables.

• Les sites officiels : Consultez de temps en temps le site Cybermalveillance.gouv.fr, qui liste les menaces actuelles.

• Les médias : Écoutez les chroniques "consommation" à la radio ou à la télévision ; elles parlent souvent des dernières vagues d'arnaques.

• Le doute systématique : Si une demande semble trop urgente ou trop belle pour être vraie, partez du principe que c'est un piège jusqu'à preuve du contraire.

LE CONSEIL PRO : Ne vous laissez jamais presser par le temps. L'urgence artificielle est l'outil n°1 des arnaqueurs. Si on vous demande d'agir "maintenant ou jamais", c'est presque toujours un signe de fraude. Prenez 5 minutes pour respirer et vérifier l'information.

Chapitre 10

La Routine de l'Internaute Serein : 5 minutes par jour pour une sécurité totale

La Routine de l'Internaute Serein : 5 Minutes pour votre Sécurité

La sécurité sur internet ne demande pas d'être un expert en informatique. C'est une question de bonnes habitudes, comme fermer sa porte à clé en partant de chez soi.

En suivant ces trois étapes simples chaque jour, vous réduisez de plus de 90 % les risques de vous faire pirater ou arnaquer.

Étape 1 : Le Réveil Numérique - Les Mises à Jour (2 minutes)

Les logiciels et les applications que vous utilisez sont comme des boucliers. Parfois, ces boucliers présentent des failles que les pirates utilisent pour entrer. Les mises à jour servent à boucher ces trous.

• Vérifiez si votre ordinateur ou votre smartphone vous demande d'installer une mise à jour système.

• Ouvrez votre "Store" (App Store ou Play Store) pour voir si vos applications (WhatsApp, Facebook, Banques) ont besoin d'être actualisées.

• N'attendez jamais "à demain" : une mise à jour faite immédiatement est une porte fermée au nez des escrocs.

• Activez, si possible, les mises à jour automatiques dans les réglages de vos appareils.

Étape 2 : Le Tour de Garde - Vos Alertes de Connexion (2 minutes)

La plupart des services modernes (Google, Facebook, Mail, Banques) vous envoient un message si quelqu'un tente de se connecter à votre compte depuis un nouvel appareil.

• Consultez rapidement votre boîte mail pour voir si vous avez reçu une alerte de sécurité ou de "nouvelle connexion".

• Si vous recevez un code par SMS que vous n'avez pas demandé, ne le transmettez jamais à personne, même si on vous le demande poliment au téléphone.

• Vérifiez vos notifications sur vos réseaux sociaux : un message du type "Une connexion a été détectée à Paris" alors que vous êtes chez vous doit vous alerter.

• En cas de doute, la règle d'or est simple : changez votre mot de passe immédiatement sans cliquer sur les liens du mail suspect (allez directement sur le site officiel).

Étape 3 : Le Relais de Sécurité - Informer son Entourage (1 minute)

Les arnaqueurs comptent sur l'isolement de leurs victimes. Briser le silence, c'est désarmer l'escroc. L'éducation est votre meilleure arme.

• Partagez une astuce simple avec un proche, un enfant ou un parent (ex: "Attention, j'ai entendu parler d'un faux SMS de livraison de colis").

• Prenez des nouvelles d'un proche moins à l'aise avec la technologie pour savoir s'il a reçu des messages étranges.

• En parlant de sécurité une minute par jour, vous créez un cercle de protection autour de vous et de votre famille.

LE CONSEIL PRO : Ne voyez pas la sécurité comme une contrainte, mais comme une hygiène de vie. Tout comme vous vérifiez que vos plaques de cuisson sont éteintes avant de dormir, vérifiez vos notifications avant de commencer votre journée. Un internaute serein est un internaute attentif mais pas stressé.

FIN

Merci d'avoir lu "Le Guide Des Arnaques"

Une œuvre écrite par Fusianima Expert

Lire la version interactive et commenter

Découvrir les autres œuvres de l'auteur