Numenantes

Vous propose

SENSIBILISATION CYBERSÉCURITÉ GRAND PUBLIC

40’ pour sécuriser Votre vie numérique

De la Box Internet au Smartphone, en passant par votre montre connectée et/ou votre voiture :

Apprenez à fermer les portes aux hackers.

Nantes – aout 2026

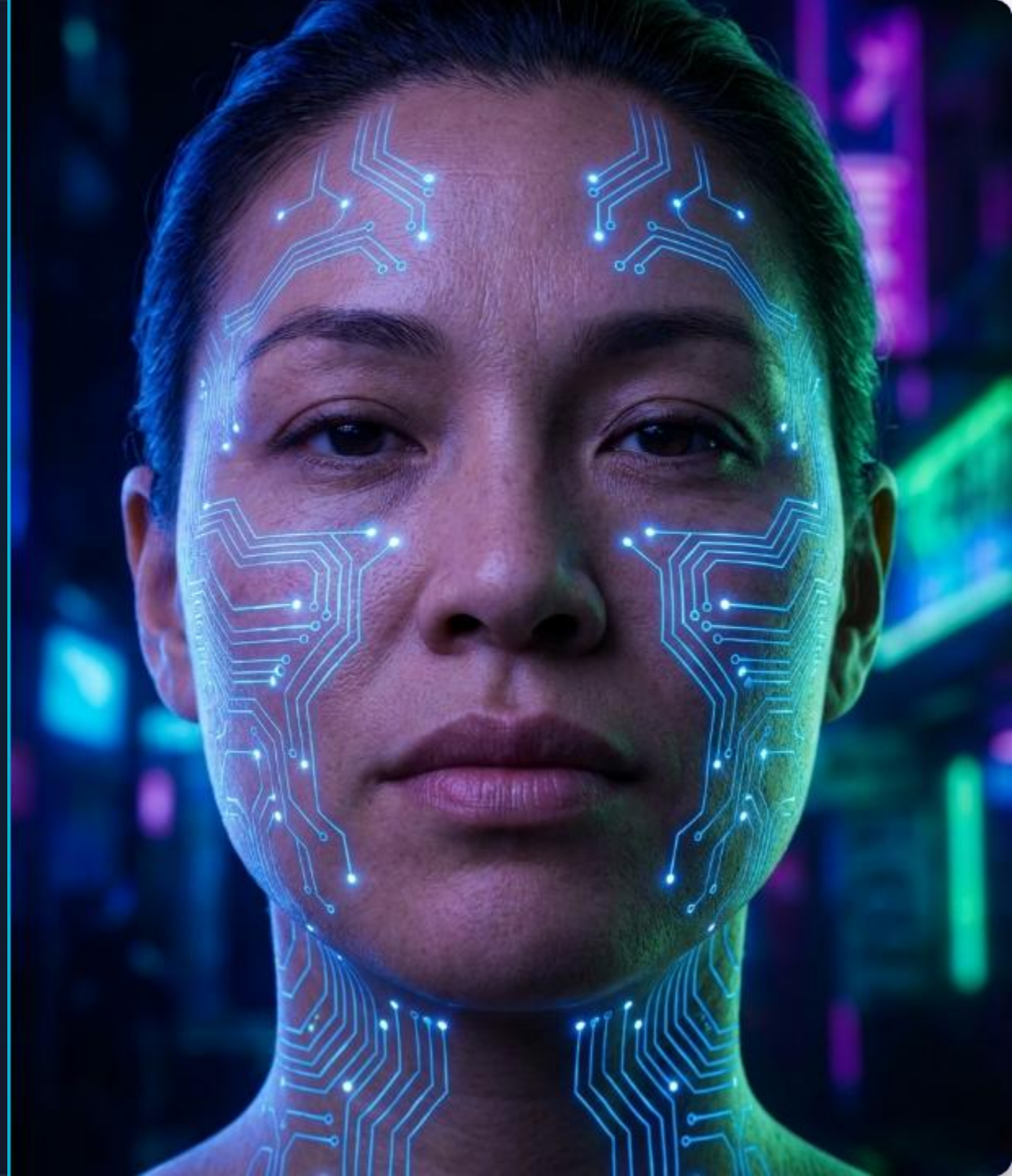
Le Mythe

L'Illusion de la Sécurité

Nous pensons souvent que les cyberattaques ne ciblent que les grandes entreprises, les banques ou les gouvernements.

La réalité est vertigineuse : **Vous** êtes la cible principale. Votre smartphone est le coffre-fort de votre vie entière, et les attaquants le savent.

Numenantes



Prise de conscience :
Vos données Personnelles

Aujourd'hui, **91%** des piratages visent les particuliers via des objets du quotidien sans qu'ils ne s'en aperçoivent.

L’industrialisation du Crime Mondial

L'année écoulée marque un tournant historique :

l'intégration massive de **l'Intelligence Artificielle** générative par les syndicats du crime a fait **exploser la vitesse et le volume des attaques** à l'échelle planétaire.



L'Effondrement du Temps (L'effet IA)

- ⏱️ **29 minutes chrono** : C'est le temps moyen qu'il faut à un pirate mondial pour prendre le contrôle total d'un réseau une fois qu'il a réussi à y poser un pied. C'est une baisse de 65 % du temps nécessaire par rapport à 2024.
- ⚡ **27 secondes** : C'est le record mondial absolu d'intrusion automatique mesuré cette année par les experts de CrowdStrike. Les humains ne peuvent plus lutter manuellement contre la vitesse des algorithmes

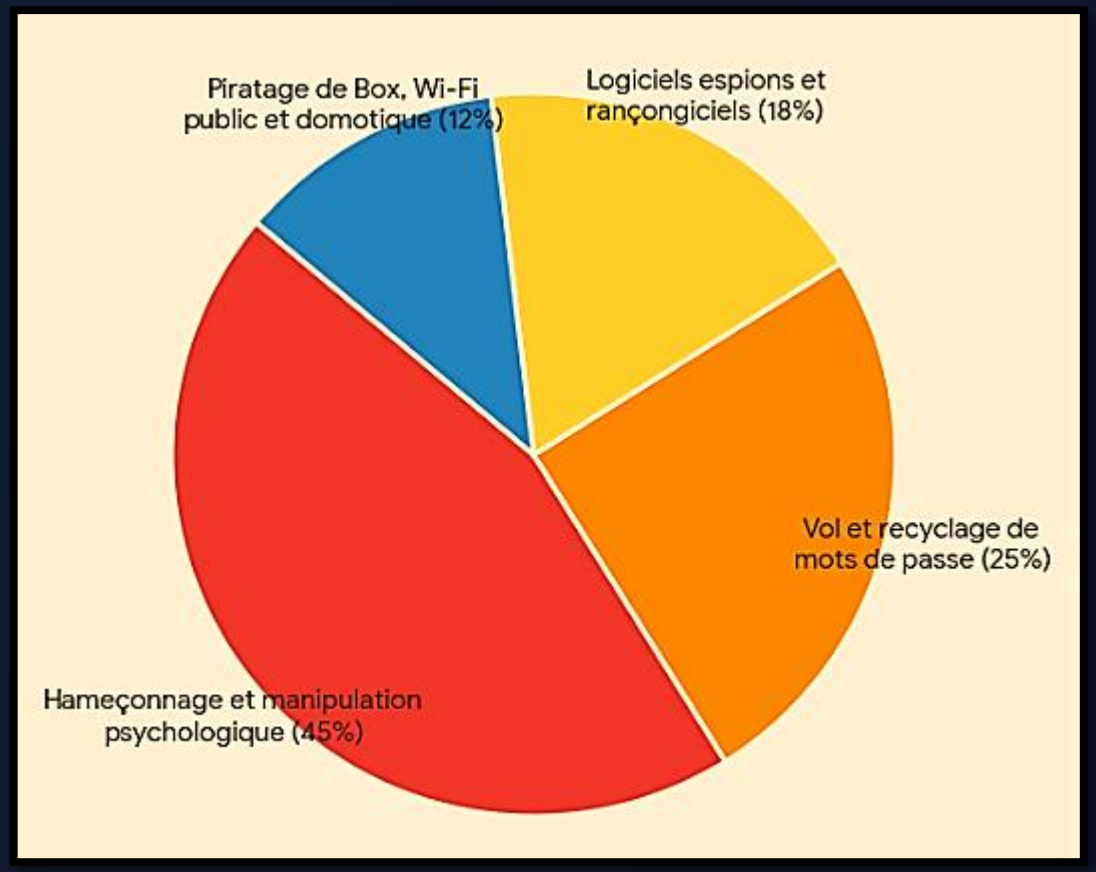
Les Chiffres Chocs Globaux

- 📈 **+18 % d'augmentation** du volume global des cyberattaques dans le monde par rapport à la même période l'année dernière.
- 📡 **2 086 attaques par semaine** : c’est la moyenne ahurissante d'assauts numériques subis par *chaque entreprise ou organisation* dans le monde en 2026.
- 💰 **4,99 millions de dollars** : c’est désormais le coût financier moyen mondial d'une seule fuite de données pour une structure touchée.
- 🚨 **+87 % de victimes de rançongiciels** (ransomwares) en un an (bilan arrêté à l'été 2026)

Répartition mondiale : Comment les pirates entrent-ils chez vous ?

« Quand vous regardez ce graphique, vous comprenez immédiatement la stratégie du crime organisé en 2026. La somme du jaune et du bleu — c'est-à-dire la technique pure, le piratage informatique difficile — **ne représente que 30 % des attaques.**

Les 70 % restants (le rouge et l'orange), c'est ce qu'on appelle l'attaque humaine : des pirates qui exploitent vos mots de passe réutilisés ou qui vous manipulent au téléphone. Retenez bien ceci pour ce soir : les pirates ne forcent plus nos systèmes, ils se connectent simplement à nos vies parce que nous leur laissons les clés. C'est pour cela que nos fiches réflexes vont tout changer. »



Le choc des données : « Regardons la réalité en France »

Les Chiffres Clés (Actualisés août 2026)

43,4 millions de comptes français ont été compromis et se retrouvent dans des bases de données criminelles rien qu'au premier semestre 2026.

9 Français sur 10 ont déjà subi une fuite de leurs données personnelles en ligne.

Une personne moyenne en France a vu ses données fuiter **5 à 6 fois** via des piratages de plateformes tierces.

L'Hameçonnage (Phishing) dopé à l'Intelligence Artificielle générative reste la cybermenace numéro 1 sur les particuliers.

43,4

Millions de Français



https://frenchbreaches.com/

https://bonjourlafuite.eu.org/

Le choc des données : « Attaques en France/ Impact famille»

Date	Cible Réelle	Ce qui a été volé ou bloqué	L'Arnaque concrète chez vous
Automne 2025	Hôpitaux Régionaux	Dossiers médicaux et numéros de Sécurité Sociale.	Un faux conseiller de l'Assurance Maladie vous appelle, connaît vos soucis de santé et vous réclame de l'argent.
Décembre 2025	Ministère de l'Intérieur	Fichiers d'identité confidentiels.	Vos documents sont utilisés pour créer de faux profils de vente (ex: sur Leboncoin) pour arnaquer d'autres personnes en votre nom.
1er Janvier 2026	La Banque Postale	Serveurs bloqués le jour de l'An (Pas de vol).	Panique des clients. Les pirates en profitent pour envoyer un faux SMS : *"Le site bug, cliquez ici pour voir votre solde"*.
Janvier 2026	L'URSSAF & Chasseurs	Données de 1 million de chasseurs et de salariés.	Mails de chantage ou fausses amendes hyper réalistes envoyés directement dans votre boîte aux lettres.

Regardez la logique implacable des pirates sur ces 12 derniers mois. Ils ont commencé par voler vos données de **santé** fin 2025.

Début 2026, ils ont bloqué les **banques**.

Au printemps, ils ont volé les **cartes d'identité** et ciblé les **enfants** à l'école.

Date	Cible Réelle	Ce qui a été volé ou bloqué	L'Arnaque concrète chez vous
Mars 2026	FICOBA (Bercy)	RIB et coordonnées bancaires de 1,2 million de Français.	De petits prélèvements discrets de 4,99 € par mois apparaissent sur votre compte sans que vous ne l'ayez autorisé.
Avril 2026	L'ANTS (Cartes d'identité)	Papiers d'identité de **11,7 millions** de citoyens.	**L'Usurpation d'identité.** Des criminels achètent votre carte d'identité sur internet pour contracter des crédits à votre nom.
Avril 2026	ÉduConnect & CROUS	Profils et adresses de **3,5 millions d'élèves**.	Les pirates contactent vos enfants sur WhatsApp en se faisant passer pour un prof afin de leur voler les codes de la maison.
Juillet 2026	Éducation Nationale	Fichiers nominatifs des agents et profils.	Campagnes massives de faux e-mails de virement ou de changement de mutuelle reçus sur les messageries des enseignants.
Août 2026 *(Aujourd'hui)*	Le Fisc (DGFiP) Scalingo / BlgCloud	Revenus et données de **678 000 contribuables** et clients Cloud.	**L'arnaque ultime.** Le faux conseiller bancaire vous appelle au téléphone : il connaît votre revenu fiscal exact pour vous mettre en confiance.

Et ce mois-ci, en août 2026, ils ont récupéré les déclarations d'**impôts**.
En un an, ils ont patiemment réuni toutes les pièces du puzzle de votre vie privée.

Ils savent tout de vous.

Voilà pourquoi l'ancien mot de passe de votre enfance ou le mot de passe unique pour tous vos sites ne suffit pas





Le Piratage du Cerveau : ingénierie Sociale



L'Urgence

L'attaquant crée un sentiment d'urgence absolue ("Votre compte sera supprimé dans 2h"). Sous stress, le cerveau zappe l'esprit critique.



La Cupidité

Les fausses promesses d'argent facile, de gains inattendus, de crypto-monnaies gratuites ou de subventions étatiques exceptionnelles.



L'Autorité

Se faire passer pour les Impôts, la Police, l'ANTAI ou votre banquier. On obéit naturellement et par réflexe à une figure d'autorité.

Le marché du Dar Web : Votre prix

Combien valent vos données personnelles pour un cybercriminel en 2026 ?

« Vous pensez peut-être que votre vie privée vaut de l'or. Sur le Dark Web, **votre identité complète s'achète pour le prix d'un ticket de restaurant**. Pourquoi ? Parce que les pirates ne vendent pas vos données une par une. Ils piratent des serveurs entiers et revendent des packs de 500 000 profils d'un coup.

Pour l'escroc qui achète ce pack, vous n'êtes qu'une ligne statistique. S'il achète vos coordonnées 20 €, mais qu'il réussit à vous piéger avec l'arnaque du "Faux Conseiller Bancaire" pour vous voler 3 000 €, son investissement est rentabilisé au centuple. C'est l'abondance de ces données pas chères qui rend les cyberattaques si faciles et si fréquentes. »

Les Tarifs du Marché Noir (Données d'individus)

Type de donnée volée	Prix moyen constaté	Risque principal pour la victime
Dossier Médical Complet	**230 € à 280 €** ($250-$310)	**Le plus cher.** Un dossier de santé ne peut pas être modifié ou annulé comme une carte bancaire. Idéal pour le chantage ou la fraude à l'assurance.
Accès Banque en Ligne (Vérifié)	**180 € à 900 €** ($200-$1000)	Vidage direct des comptes ou blanchiment d'argent. Le prix varie selon le solde disponible.
Identité Complète ("Fullz") *(Nom, adresse, numéro de Sécu, date de naissance)*	**18 € à 90 €** ($20-$100)	Crédits à la consommation souscrits en votre nom, création de faux papiers, usurpation d'identité à long terme. Une identité française basique se négocie parfois dès 32 €.
Compte E-commerce actif *(Amazon, AliExpress avec carte enregistrée)*	**15 € à 180 €+**	Achats massifs de matériel et revente par le pirate avant que vous ne bloquiez votre carte.
Carte Bancaire avec crypto-visuel (CVV)	**9 € à 36 €** ($10-$40)	**Très bon marché.** L'abondance des cartes volées fait chuter les prix. Une carte française standard coûte environ 12 €.
Compte Réseaux Sociaux / Divertissement *(Facebook, Netflix, Spotify)*	**1 € à 40 €**	Usurpation de votre messagerie pour arnaquer vos proches ("Arnaque à l'urgence").

Les 3 pièges du quotidien



Le Wi-Fi Gratuit

Se connecter au réseau sans mot de passe du café permet à un attaquant d'intercepter tout votre trafic non chiffré. Utilisez toujours votre 4G/5G ou un VPN.



Le "Quishing"

Scanner un QR code collé sur un horodateur peut vous rediriger vers un faux site de paiement. Vérifiez toujours physiquement l'autocollant.



Le Faux Colis (Smishing)

"Votre colis a été bloqué. Payez 1,99€ de frais." L'objectif n'est pas les 2 euros, mais d'aspirer le numéro complet de votre carte bancaire.

Êtes vous compromis ? (Exercice)

Étape 1 : Prenez votre téléphone

Nous allons faire un test en direct et en toute sécurité.
Ouvrez votre navigateur internet sur votre smartphone.



Étape 2 : Vérifiez votre email

Allez sur le site https://haveibeenpwned.com/
et entrez votre adresse email personnelle. Regardez les résultats.



*Le rouge signifie que vos données ont fuité lors d'un piratage d'un site que vous utilisez.

Mon mot de passe est t'il véloce ?

Étape 1 : Un volontaire

(Consignes)

- Pensez à un mot de passe, ne pas écrire un mot passe actif, mais s'y rapprochant en algorithme
- Tapez-le
- Lisons le résultat

Étape 2 : Vélocité du mot de passe

Allez sur le site

https://www.security.org/how-secure-is-my-password/

Appliquons les consignes

Regardez les résultats



Le secret de la vélocité en 2026, ce n'est pas la complexité, c'est la LONGUEUR.
Plus votre code est long, plus le robot ou l'IA fatigue et abandonne.

La règle d’or en cas de doute

🚨 "Le test des 3 secondes"

Avant de cliquer sur un lien dans un SMS, un e-mail, ou d'installer une mise à jour sur votre PC, appliquez la méthode **A.R.T.** :

- **A**nalyser l'expéditeur : L'adresse mail se termine-t-elle par `@impots.gouv.fr` ou par un texte bizarre comme `@impots-securite-2026.com` ?
- **R**epérer l'urgence : Si le message dit *"Votre compte va être bloqué dans 24h"* ou *"Votre colis est bloqué, payez 1,99€"*, c'est une arnaque. La peur fait commettre des erreurs.
- **T**éléphoner à la source : Ne cliquez jamais sur le lien du message. Fermez tout, allez sur le site officiel par vous-même (ou appelez l'organisme) pour vérifier l'information. Regardez la Pup-Pop (Lecture) en survolant le lien

La Box Internet : La Porte du Foyer

Pièges Classiques

Mot de passe d'usine & Wi-Fi Invité

Laisser le mot de passe Wi-Fi par défaut au dos de la box ou partager le réseau principal avec tous vos invités permet à n'importe quel appareil infecté de rebondir sur votre réseau.

Actions Immédiates

Sécurisation en 3 Clics

1. Changez le mot de passe d'administration de la Box.
2. Activez le **Wi-Fi Invité** pour les visiteurs.
3. Désactivez le protocole obsolète WPS et l'administration à distance.

Smartphone Neuf : Sorti du Carton

Danger

Autorisations excessives

Dès le premier allumage, les applications demandent accès à la géolocalisation, aux contacts et au micro sans justification réelle.

Infiltration

Applications hors store

Installer des fichiers APK ou scanner des liens suspects installe des faux claviers qui enregistrent vos codes bancaires (Keyloggers).

Réflexe Cyber

Configuration initiale

Activez les mises à jour automatiques du système, le verrouillage par code fort (pas 0000 !) et refusez le suivi publicitaire systématique.

Montre & Écouteurs Bluetooth

Le Bluetooth : Une Faille dans la Poche

Les montres connectées et écouteurs Bluetooth diffusent en continu des identifiants (beaconing). Un pirate à proximité peut bombarder votre smartphone de faux messages d'appairage ou intercepter votre position exacte.

Règle d'or : Désactivez le Bluetooth dans les lieux publics denses (transports, gares) quand vous ne l'utilisez pas !



Numenantes

🚗 Voiture Connectée & Supports Mobile

Quand le véhicule devient un espion

- **Supports USB de recharge publics :** Risque de *Juice Jacking* (vol de données via le câble de recharge USB).
- **Synchronisation Bluetooth de location :** Laisser son répertoire téléphonique enregistré dans le système GPS de bord !
- **Clés de voiture mains-libres :** Relay-attack permettant de déverrouiller la voiture devant chez vous à distance.



Numenantes

QR Codes Frauduleux : Le Quishing

+300%

D'attaques par QR Code collé sur les horodateurs et avis de livraison

L'arnaque invisible au premier coup d'œil

Les pirates collent un nouvel autocollant QR Code au-dessus du vrai QR Code officiel (parking, borne de recharge, carte de restaurant). Vous pensez payer 2 € de stationnement, vous donnez vos coordonnées bancaires à un faux site miroir !

Conseil : Toujours vérifier l'URL complète avant de valider une saisie sur smartphone.

Numenantes

Pratiques Dangereuses vs Réflexes Cyber

Équipement / Usage	Pratique à Risque	Réflexe de Protection
Box Internet	✗ Garder le code Wi-Fi sous la box et/ou d'origine	✓ Wi-Fi Invité + Mot de passe admin modifié
Mots de passe	✗ Mêmes identifiants partout	✓ Gestionnaire de Mots de passe + MFA (Authentification Multi-facteur)
Smartphone neuf	✗ Accepter toutes les permissions	✓ Filtrer localisation et micro au cas par cas
Bluetooth / Montre	✗ Bluetooth visible H24	✓ Couper le Bluetooth hors appairage nécessaire

Audit Express de votre Téléphone

Sortez vos smartphones : Ouvrez immédiatement le menu *Paramètres > Confidentialité / Gestionnaire de permissions*.

Vérifiez la Localisation : Regardez quelles applications accèdent à votre position *"Toujours autoriser"*. Désactivez toutes les applications non indispensables.

Activer la Double Authentification (2FA) : Sur WhatsApp, Google ou vos e-mails, ajoutez la validation sur un 2ème appareil.

Désactiver la Connexion Automatique aux Wi-Fi publics : Empêchez votre téléphone de se connecter seul aux réseaux non sécurisés.

Numenantes

Le Piège du Café : Votre téléphone parle aux inconnus

"Wi-Fi PIÈGE"

« Nous sommes tous pareils : quand on attend le train à la gare, qu'on est assis dans un café ou à l'hôtel, le premier réflexe est d'allumer son téléphone et de chercher un réseau Wi-Fi gratuit pour économiser son forfait

« Lorsque vous vous installez dans un café ou une gare, votre téléphone cherche à vous simplifier la vie. S'il capte un réseau au nom très commun (comme "SNCF_Gare", "Air France Lounge" ou "Starbucks_Guest") auquel vous vous êtes déjà connecté par le passé, il s'y reconnecte automatiquement, sans vous demander votre avis.

Imaginez un pirate informatique assis à côté de vous. Avec un petit boîtier à 50 €, il diffuse un Wi-Fi gratuit portant exactement l'un de ces noms. Votre téléphone s'y connecte instantanément. Le pirate intercepte alors votre connexion : il peut tenter de vous rediriger vers des fausses pages de connexion (phishing) ou d'analyser vos données. »

L'attaque "Evil Twin" (Le Jumeau Maléfique)

Le mythe : Aujourd'hui, les smartphones modernes (iOS/Android) ne diffusent plus en clair le nom de votre box de maison dans la rue pour des raisons de confidentialité.
La réalité du danger : En revanche, ils gardent en mémoire les réseaux Wi-Fi publics et non sécurisés (sans mot de passe).

Le piège : Le pirate configure sa fausse borne avec le nom exact d'un Wi-Fi public courant. Le smartphone, croyant reconnaître une borne familière, s'y associe automatiquement. Même si le chiffrement moderne (HTTPS) protège mieux vos mots de passe, le pirate contrôle votre accès au réseau et peut bloquer vos applications ou tenter de pirater votre appareil.

Les bonnes pratiques

Désactiver la connexion automatique aux réseaux Wi-Fi ouverts/publics dans les paramètres du téléphone.

Oublier le réseau ("Supprimer ce réseau") dans les réglages dès que vous quittez un lieu public.

Utiliser un VPN (Réseau Privé Virtuel) lors de chaque connexion à un Wi-Fi public pour chiffrer l'intégralité du trafic de bout en bout.

Numenantes

Plan d'Actions : Ce Soir à la Maison

1. La Box

Activer le réseau Wi-Fi Invité et changer le mot de passe admin.

2. Les Comptes

Activer la 2FA sur l'e-mail principal et la banque.

3. Le Mobile

Purger les applications inutilisées et les autorisations.

4. Le Bluetooth

Supprimer les jumelages enregistrés dans la voiture de location.

Numenantes

LES BULLES DE SECOURS 🛡️ : Vous n'êtes pas seuls face aux pirates

- Les 3 réflexes officiels à mémoriser pour protéger votre foyer.

1. 💻 **Le reflexe Numérique** : **CYBERMALVEILLANCE.GOUV.FR** : Cybermalveillance.gouv.fr.

   Usage : C'est le Samu du numérique. Pour faire un diagnostic gratuit, nettoyer un appareil ou être guidé pour porter plainte en ligne.

2. 📞 **Le Réflexe Chantage ou Vol de Papiers**

   APPELEZ LE 17

   Usage : Si vous êtes victime d'une usurpation d'identité confirmée, d'une extorsion de fonds ou d'un chantage à l'écran bloqué.

3. 💳 **Le Réflexe Bancaire**

   LE NUMÉRO AU DOS DE VOTRE CARTE

   Usage : Si vous avez un doute après un appel ou si vous pensez avoir validé une fausse opération. Ne cherchez pas le numéro sur internet, utilisez uniquement celui gravé sur votre propre carte bancaire.

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

17 CYBER
Mon assistance en ligne



Numenantes

Continuer à vous former 💻 : Devenez gardien de votre foyer

1. Le SecNumAcadémie (Le cours officiel de l'État)
C'est la formation incontournable lancée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
Le Site : secnumacademie.gouv.fr

Pour qui ? Les adultes et les séniors qui veulent comprendre les bases sans jargon technique.
Le contenu : Un parcours en 4 modules ludiques (le mot de passe, la navigation web, la sécurité du smartphone, l'ordinateur au quotidien). C'est entièrement gratuit et vous obtenez une attestation de réussite officielle à la fin.

🛡️ 2. Pix (Le service public de la culture numérique)
La plateforme de l'État utilisée par les collégiens, les lycéens, mais aussi accessible à tous les adultes en France.
Le Site : pix.fr



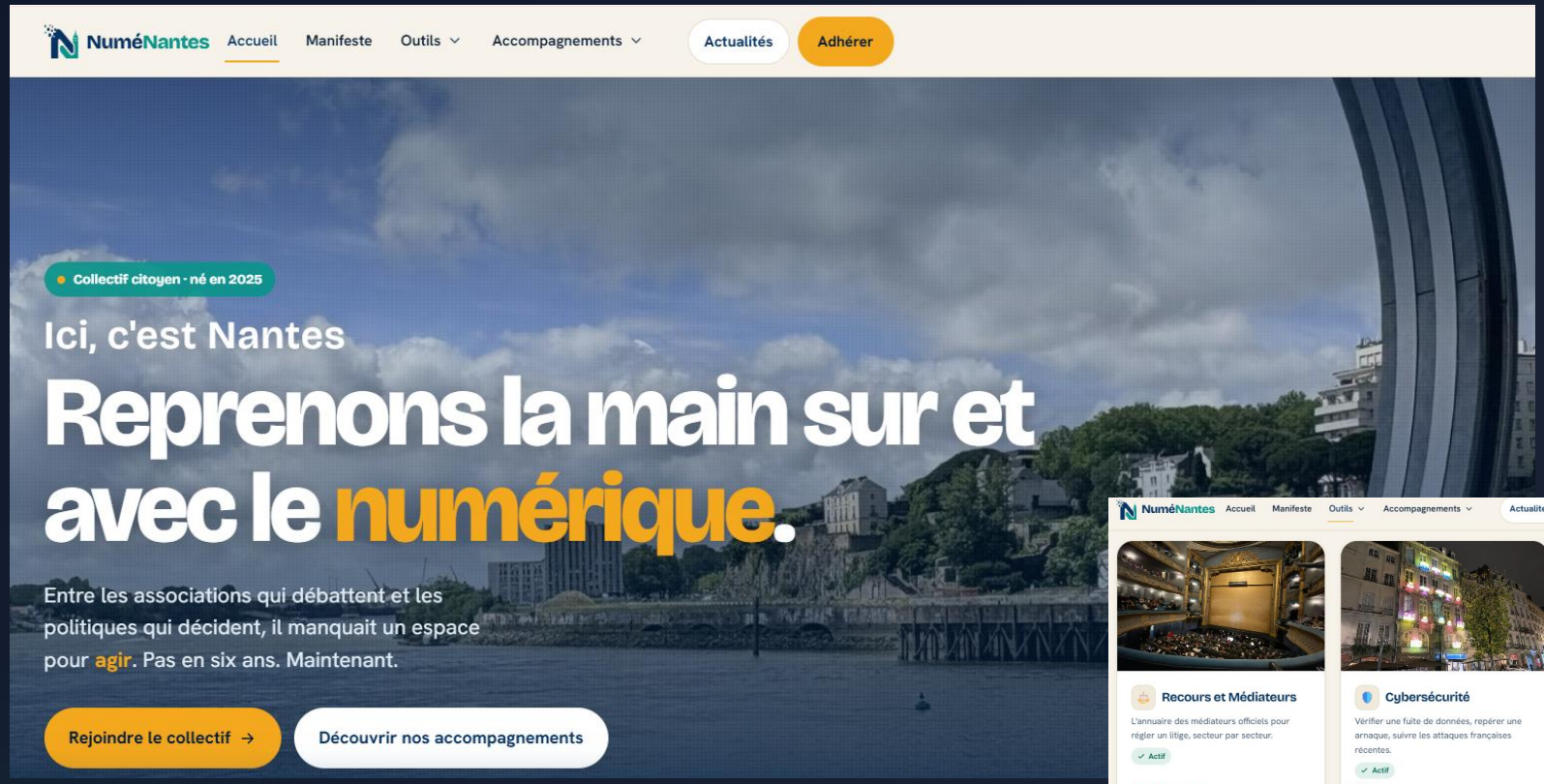
Pour qui ? Idéal pour les familles, à faire avec ses enfants ou petits-enfants.
Le contenu : Des défis interactifs et des mini-jeux pour tester vos connaissances réelles. La catégorie "Sécurité numérique" vous apprend concrètement à repérer un piège, protéger vos données et sécuriser vos comptes de manière très concrète.

📦 3. Le Kit de Sensibilisation de Cybermalveillance
La boîte à outils indispensable créée spécifiquement pour le grand public.
Le Site : cybermalveillance.gouv.fr/tous-nos-contenus

Pour qui ? Pour ceux qui préfèrent lire ou regarder de courtes vidéos plutôt que de suivre des cours.
Le contenu : Des fiches thématiques très simples, des bandes dessinées pédagogiques pour les enfants et des fiches mémos (ex: "Sécuriser ses achats", "L'arnaque au faux conseiller"). Tout est téléchargeable et imprimable gratuitement.

Continuer à vous former 💻 : Devenez gardien de votre foyer

https://www.numenantes.fr/



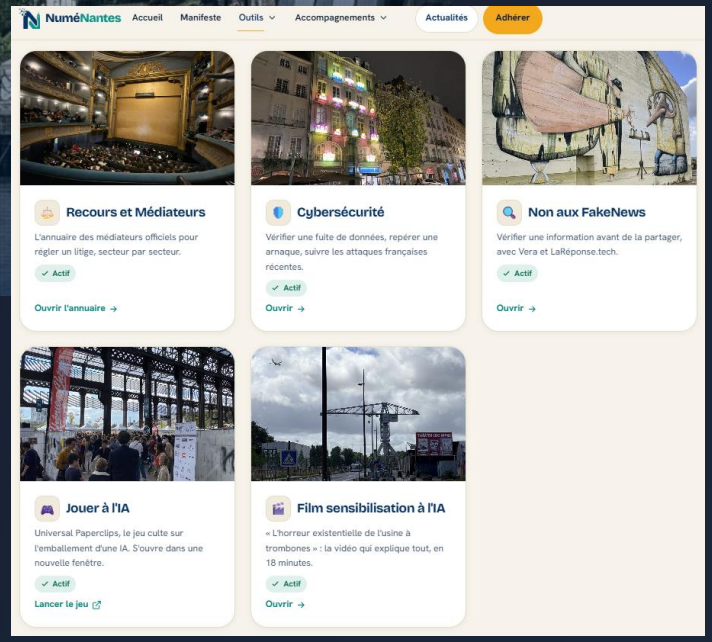
77 127
Facebook · vues

8 708
TikTok · vues

37 320
Instagram · vues

1 244
X · vues

https://www.numenantes.fr/axe-cybersecurite.html



Numenantes

https://www.numenantes.fr/outils.html

BRAVO POUR VOTRE VIGILANCE

Des Questions ?

N’oubliez pas de récupérer le lien pour recevoir :

Cette présentation incluant

- 10 Fiches reflexes
- Un Quiz Cybersécurité

Protégez vos proches : partagez ces bons réflexes autour de vous !

« Le numérique reste une chance formidable pour garder le lien avec nos enfants, nos petits-enfants et simplifier nos vies. Ne laissons pas la peur nous priver de ces outils. Être en sécurité, ce n'est pas être un expert en informatique, c'est simplement avoir du bon sens et appliquer ces quelques verrous. Les fiches que nous vous distribuons maintenant contiennent tout ce que nous avons vu ensemble. Prenez 10 minutes ce soir pour sécuriser votre box et vos mots de passe.

Merci à tous pour votre écoute et bonne fin de journée ! »

Numenantes

La sécurité numérique ne consiste pas à renoncer à la technologie, mais à en reprendre le contrôle.

— Guide de Bonnes Pratiques de Sensibilisation