

COLLOQUE SENSIBILISATION RGPD

Le numérique sans les clichés

Comprendre la cybersécurité et adopter les bons réflexes au quotidien



Casser le mythe du cinéma

- **Le cliché hollywoodien** : L'image populaire du hacker génial en sweat à capuche dans le noir.
- **La réalité du terrain** : Des attaques automatisées, banales et très souvent opportunistes.
- **L'enjeu réel** : La cybersécurité n'est pas réservée aux experts, elle concerne chacun de nous.



Le piège : "Je n'ai rien à cacher"

1. Une approche automatisée

Les cybercriminels ne ciblent pas votre identité précise. Leurs robots testent en continu des millions de connexions au hasard pour détecter la moindre porte mal fermée sur Internet.

2. La vraie valeur de vos données

Votre adresse e-mail, votre numéro ou votre ordinateur ont une valeur : réinitialiser vos accès, arnaquer vos proches en votre nom, ou relayer des attaques automatisées.

L'analogie du quotidien : La maison

- **Nos réflexes physiques** : Fermer la porte à clé le matin, vérifier les fenêtres et ne pas ouvrir à un inconnu suspect.
- **Une question de bon sens** : Ces réflexes évidents dans le monde réel doivent le devenir dans le monde numérique.
- **Le manque de repères** : On utilise des outils puissants sans toujours avoir appris le manuel de sécurité.



Objectifs de la conférence



Comprendre

Saisir le fonctionnement des pièges les plus courants du quotidien sans aucun jargon technique.



Repérer

Identifier facilement les tentatives d'escroqueries reçues par e-mail, SMS ou téléphone.



Agir

Repartir avec 4 ou 5 réflexes très simples pour mettre efficacement sa vie numérique à l'abri.

Partie 1

Les menaces du quotidien

Le Phishing (ou Hameçonnage)

- **L'attaque n°1** : Le principe classique de la pêche : un appât numérique pour piéger la victime.
- **Usurpation de confiance** : Des messages imitant l'Assurance Maladie, la Poste, votre banque ou les impôts.
- **Les leviers psychologiques** : Jouer systématiquement sur l'urgence ("sous 24h") ou une opportunité de gain.



Le Phishing (ou Hameçonnage)



ESPACE CLIENT ▾

PORTAL TV ET ▾

SERVICES PLUS POUR VOUS ▾

Facture impayée (N°72937438)

Chère Cliente, Cher Client,

Nous sommes au regret de vous informer que le prélèvement mensuel dû au règlement de votre facture a été refusé par votre établissement.

Dans l'attente d'une suite favorable, nous vous invitons à régler les frais de votre abonnement dans les plus brefs délais dans un de nos magasins ou sur votre espace client en cliquant sur le lien ci-dessous

<http://www.bouyguestelecom.fr/mon-compte/suivi-conso/factures>

Vous disposez de 48h pour régler votre facture, dans le cas où votre facture n'est toujours pas réglée, votre abonnement sera automatiquement résilié.

Nous vous remercions de votre confiance.

S'IDENTIFIER

L'arnaque au "Faux Conseiller"

Le mécanisme du piège

Un appel reçu depuis le numéro officiel de votre banque (falsifié à l'affichage). Un interlocuteur très courtois simule une fraude en cours pour vous stresser.

La règle d'or à retenir

On vous demande un code SMS pour "annuler" l'achat. En réalité, ce code valide le paiement du pirate. **Aucun organisme officiel ne vous demandera un code par téléphone.**



Mots de passe : Notre faiblesse



Le réflexe courant : Utiliser un mot de passe simple et identique sur plusieurs sites pour ne pas l'oublier.



Le risque d'effet domino : Le piratage d'un petit site secondaire donne accès à tous vos autres comptes (mails, banque, réseaux).



L'analogie de la clé unique : Avoir le même mot de passe partout revient à ouvrir sa maison, sa voiture et son bureau avec la même clé.



Pas de panique !



Partie 2

Les 4 "Gestes Barrières" numériques

1. Mots de passe solides & uniques

- **Le gestionnaire de mots de passe** : Un coffre-fort numérique sécurisé qui retient et génère vos accès complexes à votre place.
- **Une seule clé à retenir** : Vous n'avez plus qu'un seul mot de passe maître à mémoriser pour l'ensemble de vos accès.
- **Alternative "Phrase de passe"** : Associer plusieurs mots simples (ex: *JadoreLesCroissantsAuBeurreLeMatin!*) impossibles à deviner.



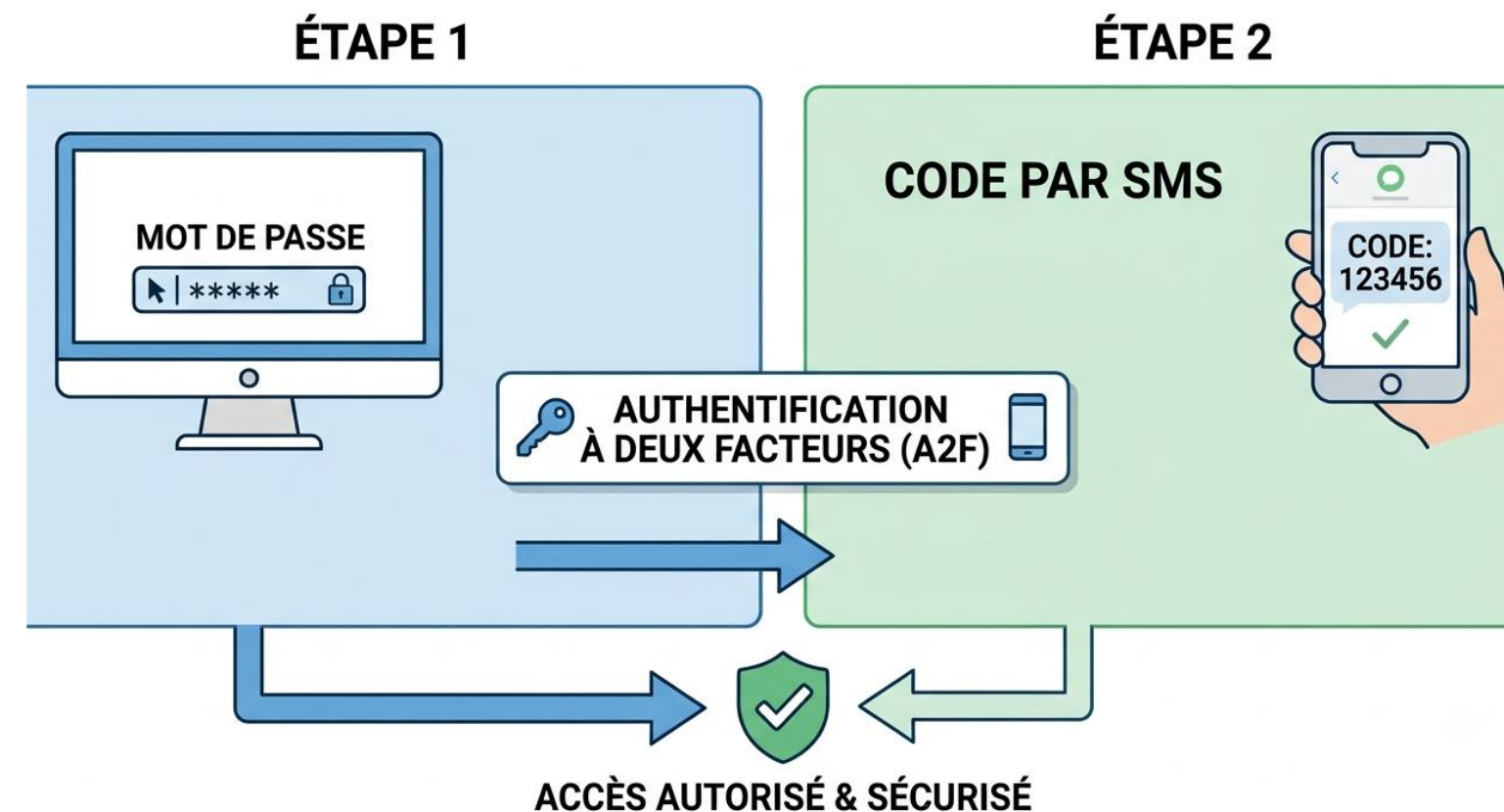
2. La double authentification

Qu'est-ce que la 2FA ?

En plus de votre mot de passe, un second code temporaire est demandé (SMS ou application). C'est le même principe que pour valider vos achats bancaires en ligne.

Un verrou infranchissable

Même si un pirate à l'autre bout du monde trouve votre mot de passe, il reste bloqué à la porte car il ne possède pas votre téléphone physique.



3. Les mises à jour système

- **Réparer les serrures** : Une mise à jour corrige les failles de sécurité découvertes dans vos logiciels et applications.
- **Ne pas repousser** : Cliquer sur "Me le rappeler demain" revient à laisser une serrure cassée sans la réparer.
- **La bonne habitude** : Activer les mises à jour automatiques pendant la nuit pour laisser la technologie travailler seule.



MISE À JOUR...



4. La sauvegarde externe

- **Protection anti-rançongiciel** : En cas de virus qui bloque votre ordinateur, la sauvegarde rend le chantage inefficace.
- **La méthode simple** : Copier régulièrement vos photos et documents sur un disque dur externe, puis le débrancher.
- **La roue de secours** : Un réflexe qu'on espère ne jamais utiliser, mais essentiel le jour où un incident survient.



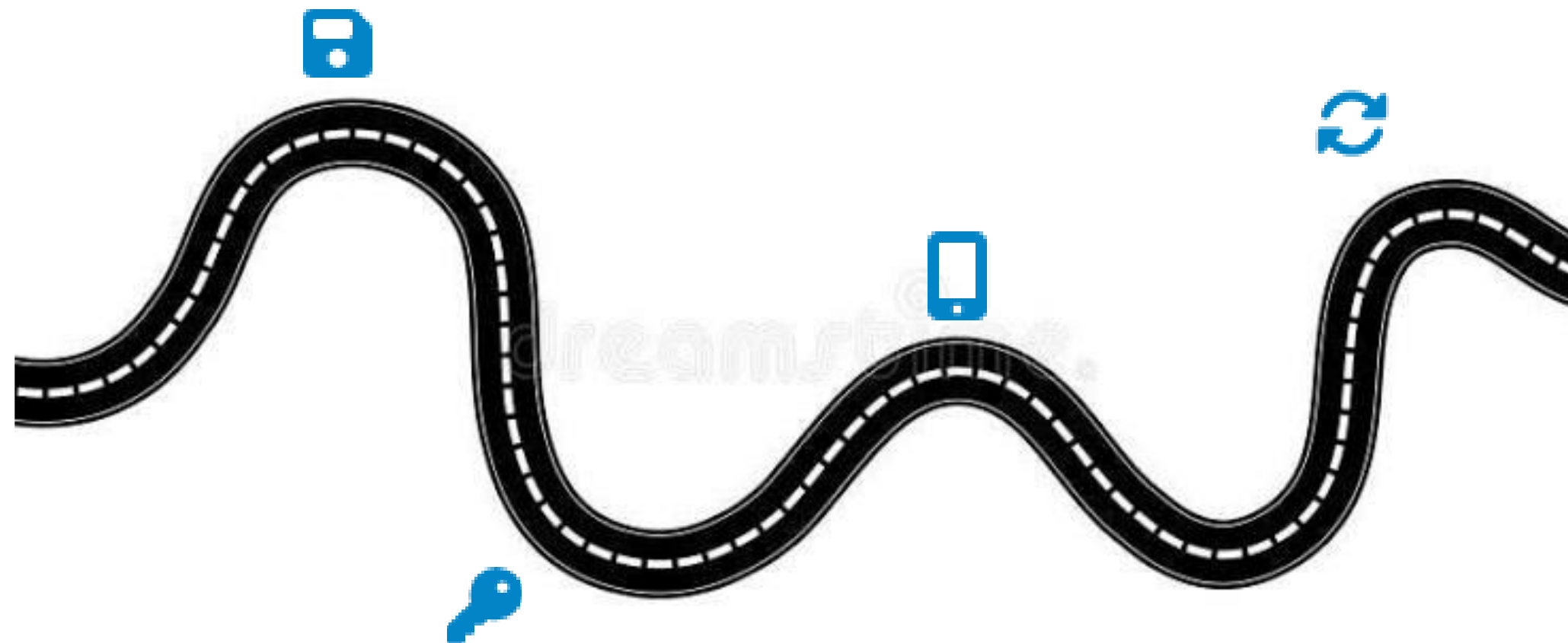
Que faire en cas d'attaque ?

- Agir vite
- Le protocole **ASAP** : Arrêter l'attaque, Signaler, Annoter, Protéger
- En cas de doute : Appliquez quand même le protocole ASAP



La feuille de route essentielle

-  **1. Double verrou** : Activez la double authentification sur votre boîte mail principale et vos comptes clés.
-  **2. Clé unique** : Utilisez une phrase de passe ou adoptez un gestionnaire de mots de passe.
-  **3. Serrures réparées** : Programmez l'installation automatique des mises à jour système.
-  **4. Roue de secours** : Sauvegardez vos souvenirs et fichiers importants sur un disque déconnecté.



La cybersécurité est humaine

- **L'humain au cœur du sujet** : Les attaques ciblent la fatigue, l'inattention ou la curiosité, plutôt que la technologie elle-même.
- **Le meilleur outil, c'est vous** : La seconde de réflexion avant de cliquer sur un lien suspect est votre protection absolue.
- **En cas de doute** : Prenez le temps de vérifier l'expéditeur ou contactez directement l'organisme officiel.



Les offres de l'ADIT

1. Bilan et sensibilisation

- Réalisation de bilans personnalisés
- Conseils et accompagnement à la mise en place de méthodes et de pratiques informatiques sécurisées
- Sensibilisation des agents et des élus à la cybersécurité

2. Des outils pour vous accompagner

Fourniture de dispositifs de sécurisation

- Messagerie professionnelle,
- Coffre-fort de mot de passe,
- Sauvegarde de vos données
- Antivirus à analyse comportementale

Questions & Échanges

Merci pour votre attention et votre participation !

Plateforme officielle d'assistance : www.cybermalveillance.gouv.fr