SÉGUR DU NUMÉRIQUE EN SANTÉ en Normandie

Accompagnement Cybersécurité

Juin 2025

https://www.esegur-normandie/

SOMMAIRE

Rappels

Micros coupés pendant le temps des interventions

Temps de questions / réponses à la fin

Questions à poser en levant la main (chat bloqué)

Session enregistrée

Ouverture du comité régional

Olivier ANGOT

Directeur
GRADeS Normand’e-Sante

Vos Contacts en région

Omar CHIBANE

Coordonnateur Collectif SI Normandie &
Référent régional Cyber ESMS

Olivier COUTANT

Coordinateur du Centre Régional
de Ressources Cybersécurité

Sensibilisation à la Cybersécurité

Introduction

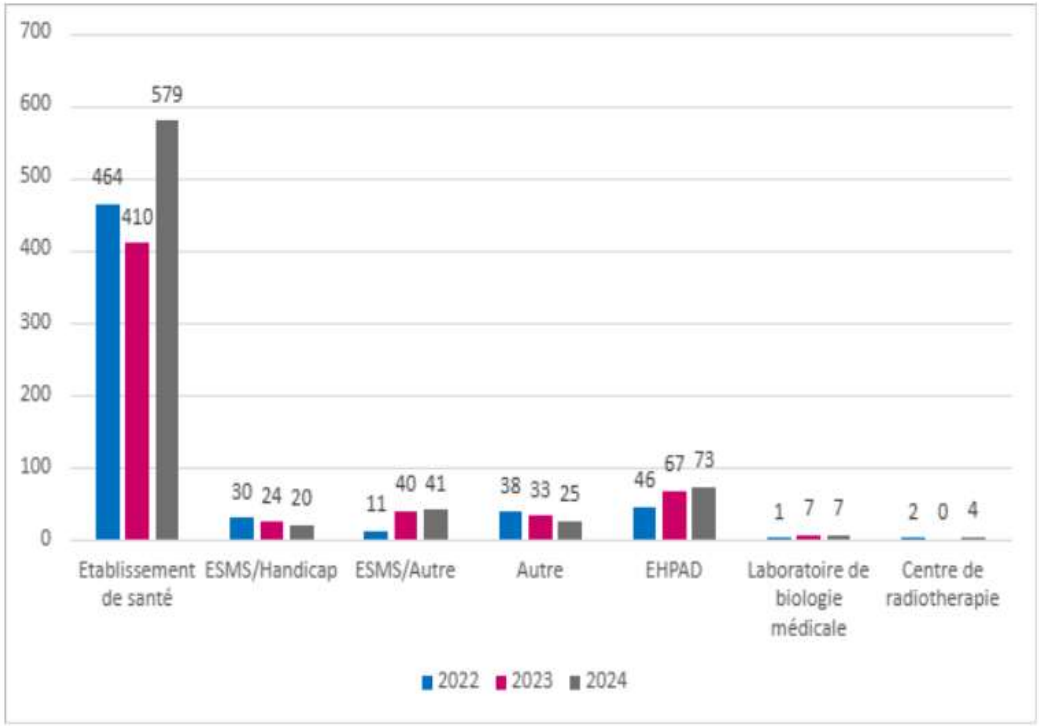
Les établissements de santé restent la principale cible des cybercriminels

Les établissements de santé sont privilégiés pour deux raisons : leur niveau de sécurité est assez faible et ils détiennent des données personnelles facilement revendables. Sur le **darknet**, un seul dossier médical se revend entre 50 et 250 euros.

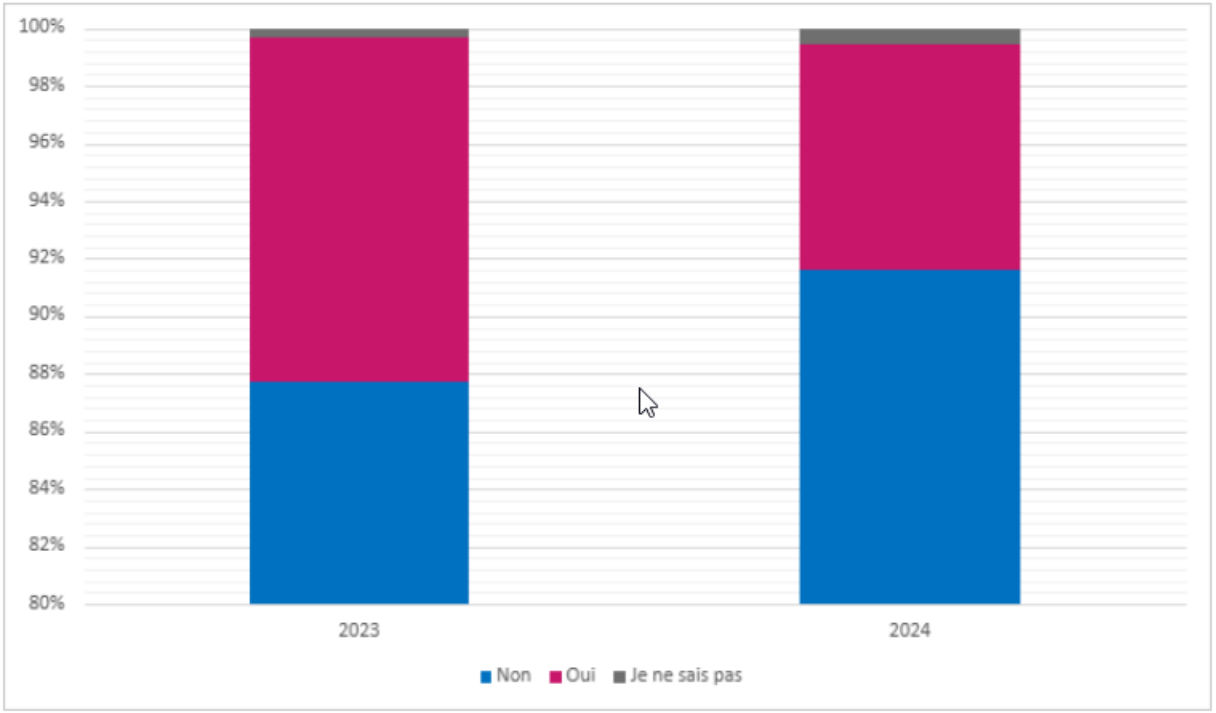
749 incidents ont été déclarés en 2024. Ce nombre est en forte augmentation par rapport à 2023 (581). Pour mémoire, 591 incidents avaient été déclarés en 2022

Les Chiffres

Répartition des signalements selon le type de structure



Mise en danger potentielle des patients



Parmi les 59 mises en danger patient potentielles de cette année 2024 (8% du nombre total d'incidents), trois incidents ont entrainé une mise en danger patient avérée.

Plan

A – Que faire face à une Cyberattaque

1) Les **conséquences**
2) Les **réactions à adopter** (dans l'urgence, la rançon)
3) La **réparation** (grâce aux sauvegardes) et la **prévention**
4) Les **mots de passe**, les **clés USB**

B - Les différentes menaces

1) **Les ransomwares**
2) **L'usurpation d'identité**
3) **L'hameçonnage**
4) **Les réseaux Wifi**
5) **Le télétravail**
6) **Le téléphone portable**

1ère PARTIE :

Que faire face à une Cyberattaque ?

COMMENT EVITER CELA ?!...

UN RANSOMWARE, C'EST QUOI ?

3. 2. Les conséquences

Impossibilité d'accéder à ses données locales ou distantes

Plus d'accès aux outils ou portails pour gérer les données de la collectivité (accueil des patients, facturation, imagerie médicale dossiers médicaux…)

E-réputation de la collectivité **entachée**

Une potentielle **fuite de données** pour un usage litigieux (usurpation d'identité…)

Une **publication de données sauvage** pour augmenter la pression sur les victimes

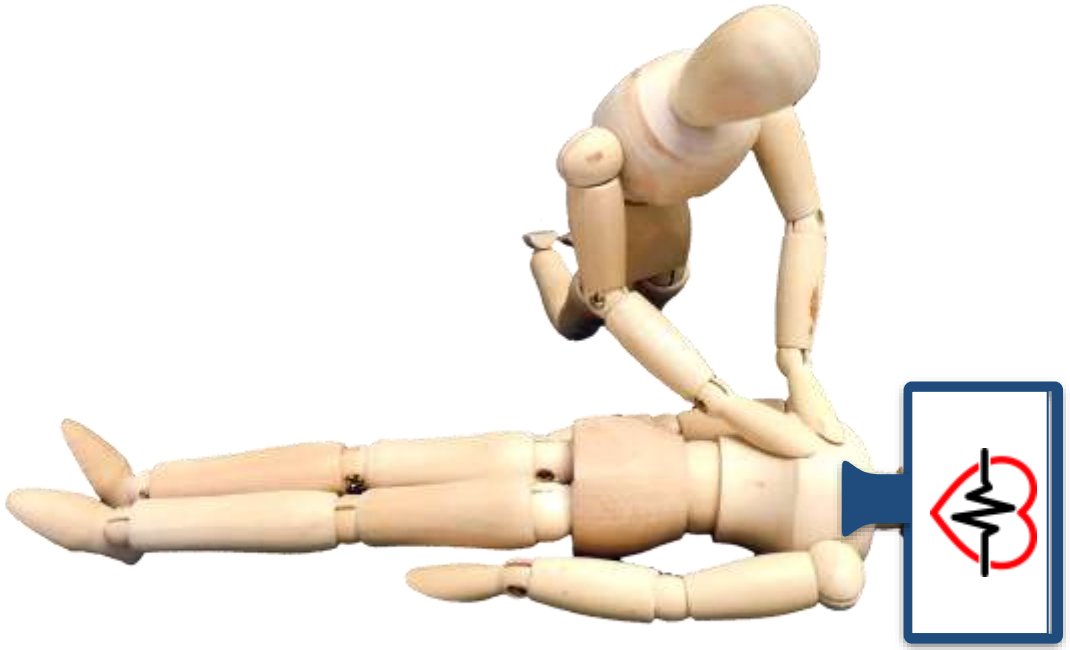
UN RANSOMWARE, C'EST QUOI ?

3. 2. Les conséquences

[1]Règlement général sur la protection des données

Dans l'urgence

Les **premiers gestes** peuvent être **DÉCISIFS**



CYBERATTAQUE : COMMENT REAGIR ?

- **Laisser les machines <u>en l'état</u>** (éteintes ou en veille)
- **Identifier tous les appareils chiffrés/infectés**

Éviter d'éteindre les machines infectées, les mettre plutôt en veille

3

Alerter immédiatement votre support informatique

4

2

Couper les connexions entrantes et sortantes de l'internet

Déconnecter les sauvegardes

5

1

Déconnecter les éléments infectés du réseau et couper les connexions sans fil.

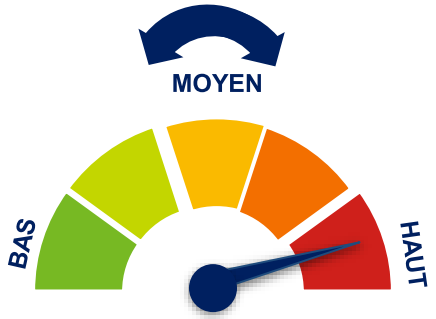
CYBERATTAQUE : COMMENT REAGIR ?

Il est fortement **recommandé de ne pas payer la rançon.**

NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

Payer la rançon revient à s'exposer à de nombreux risques



CYBERATTAQUE : COMMENT REPARER ?

L'arme fatale :
LA SAUVEGARDE

3 Trois **sauvegardes**

2 Deux **supports**

1 Un **endroit** différent

CYBERATTAQUE : COMMENT REPARER ?

L’arme fatale :
LA SAUVEGARDE

Sécurisées

Chiffrées

Régulières

Sur différents supports

Dans des **endroits différents et éloignés**

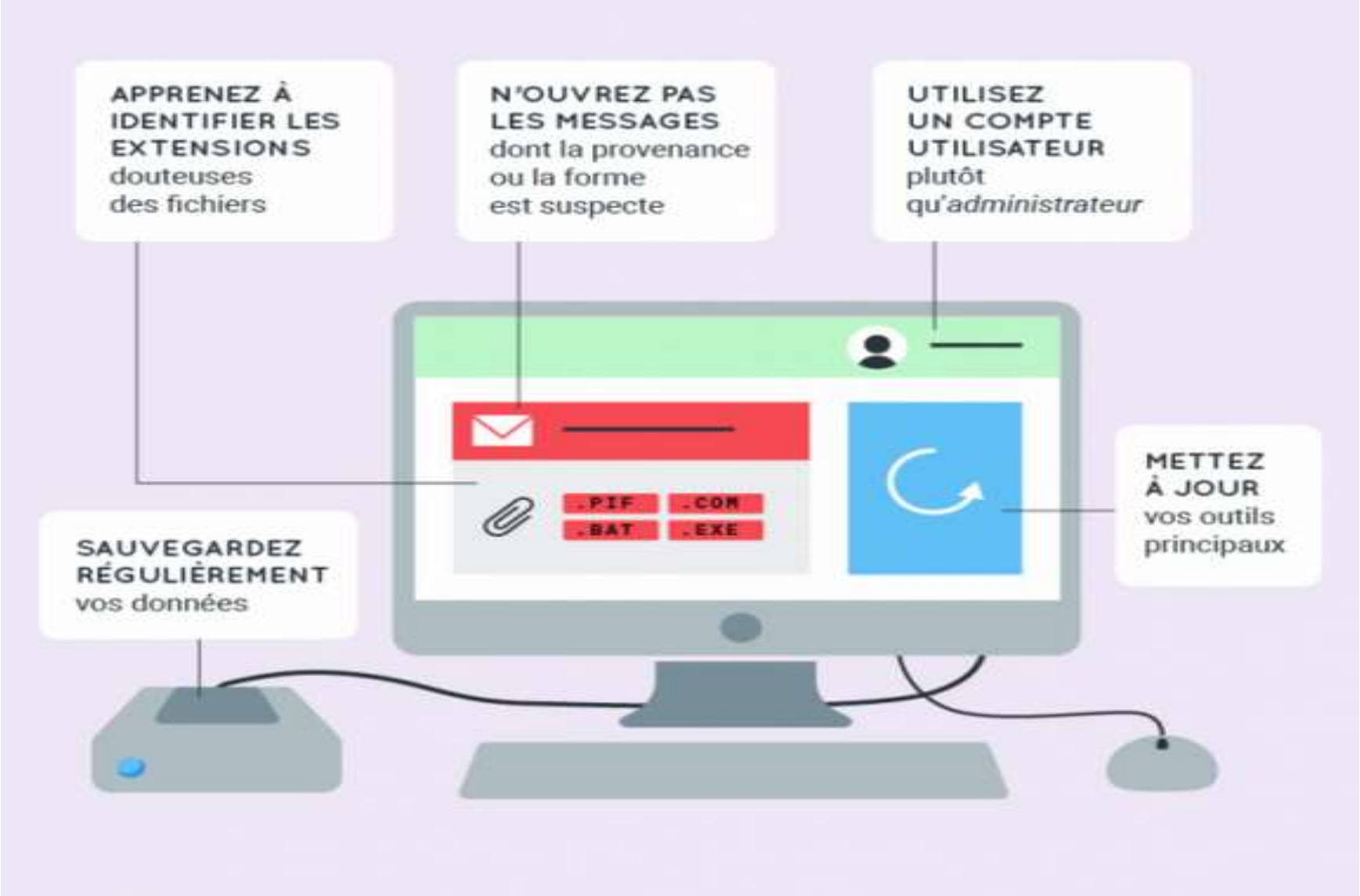
Testées régulièrement

Vérifier les clauses du contrat

LA PREVENTION

Le **risque zéro n'existe pas**, c'est pourquoi la **PRÉVENTION** est **primordiale.**

LA PREVENTION



Les mots de passe

1. Un bon mot de passe, c’est un minimum de 12 caractères, en alternant des majuscules, des minuscules, des chiffres, des caractères spéciaux.

2. Il ne dit rien sur vous.

3. Un compte, un mot de passe

4. On ne l’écrit pas (post-it, messagerie, fichier texte…)

5. On active la double authentification si le service le propose

6. Quand il y a une alerte ou un doute, on le change immédiatement.

Les mots de passe

TEMPS NÉCESSAIRE POUR CRACKER UN MOT DE PASSE EN UTILISANT L'IA CHAPGPT (2023)

Nbre de caractères	Nombre uniquement	Minuscules	Majuscule et Minuscules	Nombre, Majuscule et Minuscules	Nombre, Majuscule et Minuscules, Caractères spéciaux
4	Instantanée	Instantanée	Instantanée	Instantanée	Instantanée
5	Instantanée	Instantanée	Instantanée	Instantanée	Instantanée
6	Instantanée	Instantanée	Instantanée	Instantanée	Instantanée
7	Instantanée	Instantanée	Instantanée	Instantanée	Instantanée
8	Instantanée	Instantanée	Instantanée	Instantanée	1 seconde
9	Instantanée	Instantanée	4 secondes	21 secondes	1 minute
10	Instantanée	Instantanée	4 minutes	22 minutes	1 heure
11	Instantanée	6 secondes	3 heures	22 heures	4 jours
12	Instantanée	2 minutes	7 jours	2 mois	8 mois
13	Instantanée	1 heure	12 mois	10 ans	47 ans
14	Instantanée	1 jour	52 ans	608 ans	3k ans
15	2 secondes	4 jours	2k ans	37k ans	232k ans
16	15 secondes	2 ans	140k ans	2m ans	16m ans
17	3 minutes	56 ans	7m ans	144m ans	1bn ans
18	6 jours	1k ans	378m ans	8bn ans	79bn ans

Les mots de passe

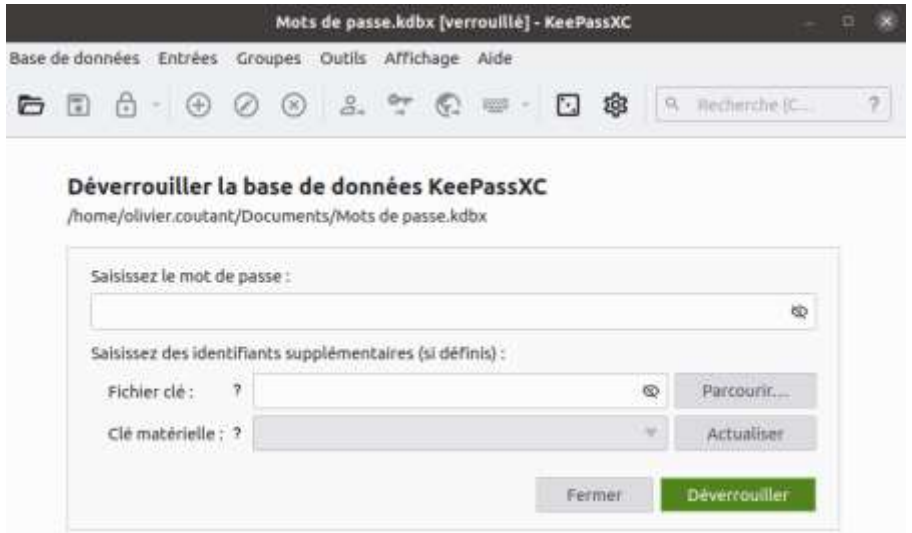
QU'EST-CE QUE KEEPASS ?

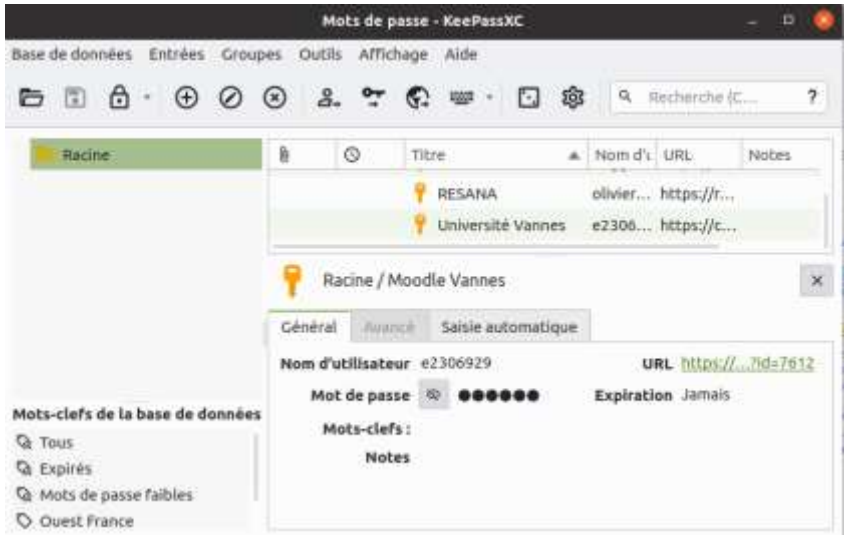
Keepass est un coffre-fort électronique permettant de gérer et stocker vos mots de passe en remplaçant avantageusement les aide-mémoires papier. Des applications mobiles compatibles existent par exemple «Keepass2Android Offline» et permettent de maitriser à tout moment ses mots de passe.

La protection de cet outil est assurée par un mot de passe d'accès qu'il conviendra de construire en respectant les règles de sécurité élémentaires (décrites dans la suite du document).

Pour éviter les pertes de données, il est vivement conseillé de l'intégrer dans un processus de sauvegarde automatisée des données.

Attention, en cas d'oubli du mot de passe d'accès il sera impossible de récupérer les informations stockées.





Séparer votre vie privée de votre vie professionnelle sur les réseaux sociaux

- Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez.

- Usages pro-perso : Ne mélangez pas votre messagerie professionnelle et personnelle.

- Maîtrisez vos propos sur les réseaux sociaux.

- Usages pro-perso : N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles.

28

Le piratage de compte

4 CONSEILS D'UTILISATION DES CLÉS USB AU TRAVAIL :

- Fournir des clés USB aux collaborateurs afin d'éviter toute menace extérieure
- Ne pas brancher une clé USB dont on ne connaît pas la provenance à un poste de travail
- Contrôler les clés USB qui n'ont pas été branchées dans un environnement sécurisé
- Brancher uniquement des clés préalablement vérifiées

Bien choisir sa clé USB, c'est aussi assurer la sécurité de votre entreprise et de votre vie privée.

Le piratage de compte

2ème PARTIE :

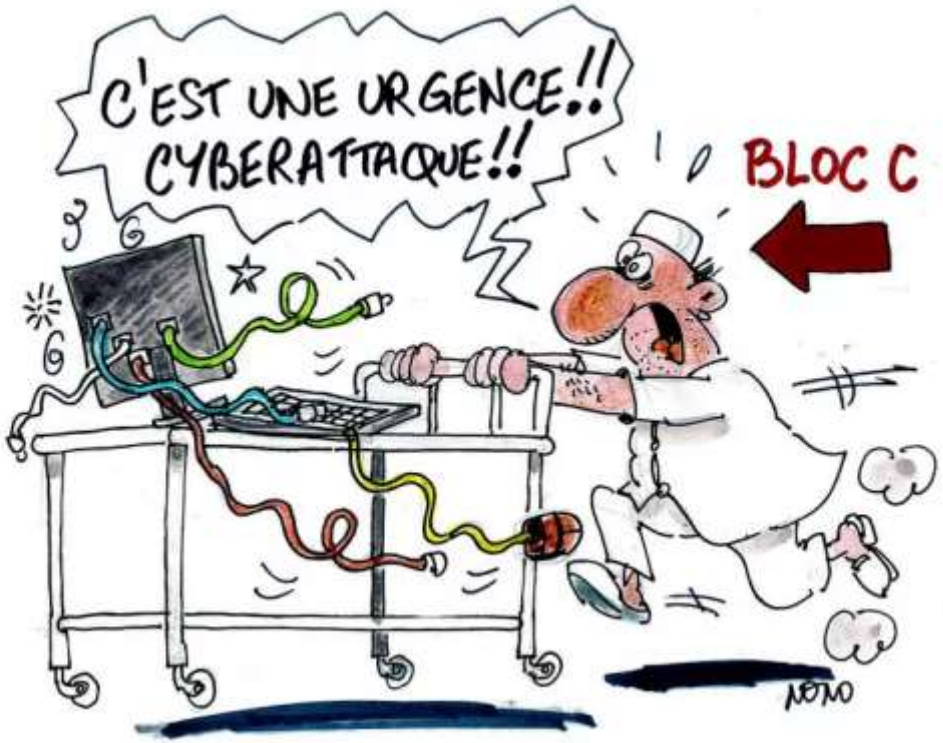
Les différentes menaces

UN RANSOMWARE, C'EST QUOI ?

- 1 attaque par rançongiciels toutes les 11 secondes dans le monde.

- 1 marché qui représente + de 1000 milliards de $ par an.

- Cyberattaques par rançongiciels en hausse de 30 % en 2023.



Action d'un rançongiciel : WannaCry.

UN RANSOMWARE, C'EST QUOI ?

- Un rançongiciel – ransomware en anglais – est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.

- Ce logiciel malveillant rend les données inaccessibles.

- Le pirate réclame une rançon pour les débloquer.
(double extorsion avec vente parfois aux enchères)

UN RANSOMWARE, C'EST QUOI ?

Le **comportement du virus varie**, il peut agir :

- aussitôt
- attendre le week-end
- attendre d'avoir infecté toutes les machines

L’usurpation d’identité

Une usurpation d'identité, c'est lorsqu'une personne se fait passer pour vous, utilise vos données personnelles sans votre accord et réalise différents actes en votre nom.

L'usurpation d'identité peut se produire via des sites Web, des e-mails, des appels téléphoniques, des SMS.

Le fraudeur va prendre votre identité par exemple pour ouvrir des comptes bancaires et souscrire des cartes de paiement, mais aussi des crédits à la consommation.

L’usurpation d’identité

Gardez la maîtrise de vos données d’identité

https://filigrane.beta.gouv.fr/

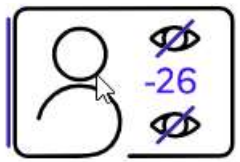
L'usurpation d'identité

Gardez la maîtrise de vos données d'identité

FRANCE IDENTITE

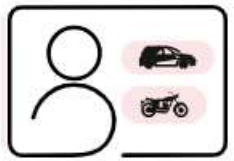
Fournir un justificatif d'identité à usage unique

Facilement, en toute sécurité, et à usage unique. Terminés les scans de carte d'identité !



Prouver votre identité ou de certains attributs...

En ligne ou pour des usages de proximité avec ou sans partage de vos données



ou encore de votre droit à conduire

Lors d'un contrôle routier ou pour louer un véhicule

L’usurpation d’identité

Gardez la maîtrise de vos données de santé

L’Application Carte Vitale

L’usurpation d’identité

L’usurpation d’identité

« L » minuscule

apple.com

apple.com

« i » majuscule

L'usurpation d'identité

OVHcloud

1 Sélectionner — 2 Options — 3 Récapitulatif

Rechercher un nom de domaine

Recherche générale

nornand-esante.fr

Entrez vos noms de domaine (jusqu'à 20) ici, avec leur extension associée. Veuillez noter que chaque nom de domaine doit apparaître sur une ligne distincte.

Rechercher

Bénéficiez d'un nom de domaine gratuit pendant un an en souscrivant à une offre d'hébergement web OVHcloud*.

Inclus avec chaque nom de domaine :

- 1 adresse e-mail personnalisée
- 1 DNSSEC (DNS sécurisé)

Résultats de la recherche

	Prix HT /1re année	
nornand-esante.fr Disponible	5,59 € puis 7,79 €/an	Acheter

Vue du moteur de recherche OVH, vérification de disponibilité

L’usurpation d’identité

Mes alias

Adresse e-mail de l'alias *

o.chibane@nornand-esante.fr

+ Ajouter un alias

L’hameçonnage

L'hameçonnage ou le phishing consiste à obtenir du destinataire d'un courriel, d'apparence légitime, qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent.
Quishing (Hameçonnage par QR code)

L'hameçonnage

Quelques exemples

ING

Chère cliente, Cher client,

Lors de votre dernier opération bancaire, nous avons remarqué une activité inhabituelle sur votre compte.

Pour réactiver votre compte Vous devez mettre à jour vos informations, une fois ces dernières validées, le compte fonctionnera normalement.

L'ensemble du processus ne prendra que 5 minutes. Vous devez agir maintenant pour résoudre le problème le plus rapidement possible.

Suivez le lien ci-dessous pour finaliser le processus et régler l'état de votre compte

Accéder à votre espace sécurisé

Nous vous remercions de votre confiance

Cordialement,

Arnaud Le Roux
Direction Qualité

L'hameçonnage

votre-conseiller@relation-clients-edf.fr

De: EDF <votre-conseiller@relation-clients-edf.fr>
Envoyé: [redacted]
À: [redacted]
Objet: Votre consommation d'électricité a évolué. Voici notre conseil.

Si vous ne visualisez pas ce message, suivez ce lien

EDF **Avec la mensualisation sans surprise, adaptez vos mensualités**

Bonjour Monsieur [redacted]

N° client : 5018456599
7 CHEMIN DE LA [redacted]

Nous constatons actuellement que votre mensualité de 64,82 € TTC ne correspond plus à votre consommation réelle.

Afin de comprendre cet écart et d'éviter une régularisation importante en fin de période, contactez-nous rapidement au **30 04** (service et appels gratuits).
Lors de cet entretien, munissez-vous également de votre relevé de compteur de gaz.

Pourquoi votre consommation a-t-elle augmenté ?

Cette évolution peut s'expliquer par :

- Des changements intervenus au sein de votre foyer (habitudes de consommation, équipements énergivores…)

Le saviez-vous ?
Le compteur communicant Linky mesure vos consommations réelles. Ainsi nous pouvons régulièrement

- Des variations de la température extérieure.

vérifier que vos mensualités sont bien adaptées

À bientôt,

Votre conseiller EDF

Pour ne plus recevoir ces alertes, rendez-vous dans votre espace client ou contactez-nous au :
3004 Service & appel gratuits

votre-conseiller@relation-clients.edf.fr

EDF & MOI

Téléchargez l'appli EDF & MOI

Téléchargez sur Google play

Téléchargez sur l'App Store

Retrouvez-nous sur :

L'énergie est notre avenir, économisons-la !

Origine 2021 de l'électricité vendue par EDF : 76,9% nucléaire, 14,5% renouvelables (dont 6,6% hydraulique), 0,8% charbon, 7,0% gaz, 0,8% autres fossiles. Origine 2021 de l'électricité vendue par EDF et indicateurs d'impact environnemental sur www.edf.fr/origine-de-lelectricite-fournie-par-edf

EDF SA au capital social de 2 000 468 641 euros, n° 552 081 317 RCS Paris, siège social 22-30 avenue de Wagram 75382 Paris Cedex 08.

Conformément à la réglementation en matière de données personnelles, vous disposez d'un droit d'accès, de rectification, d'opposition, d'effacement, de limitation et de portabilité de vos données à l'adresse électronique : mesdonnees@edf.fr en vous authentifiant ou en justifiant de votre identité.

Pour une information plus détaillée sur le traitement de vos données et vos droits, nous vous invitons à consulter notre "charte de protection des données personnelles" disponible ici.

Pour choisir quels emails recevoir, ou vous désabonner, c'est par ici

5 conseils pour identifier les e-mails frauduleux

1. Le message vient du domaine public

Aucune organisation légitime n'enverra d'e-mails en utilisant un domaine public comme les e-mails se terminant par *@gmail.com.*

2. Le nom d'affichage peut être faux

Beaucoup d'entre nous ne regardent jamais l'adresse e-mail d'où provient un message. Lorsque les escrocs créent une fausse adresse e-mail, ils sélectionnent un nom d'affichage, qui n'a pas du tout à se rapporter à l'adresse e-mail.
Par exemple : *PayPal@abc.com*

3. Noms de domaine mal orthographiés

Il existe de nombreuses façons de créer des adresses qui ne peuvent pas être distinguées de celles qui sont usurpées.
Exemple : au lieu de *m* , il y a un *rn* dans le domaine de l'arnaque

4. Les e-mails urgents ou alléchant sont une menace

Si vous recevez un e-mail avec une ligne d'objet qui invoque un sentiment d'urgence ou qui est trop beau pour être vrai.
IL FAUT SE MÉFIER!!!

5. Vérifiez avant de cliquer sur les pièces jointes ou un lien

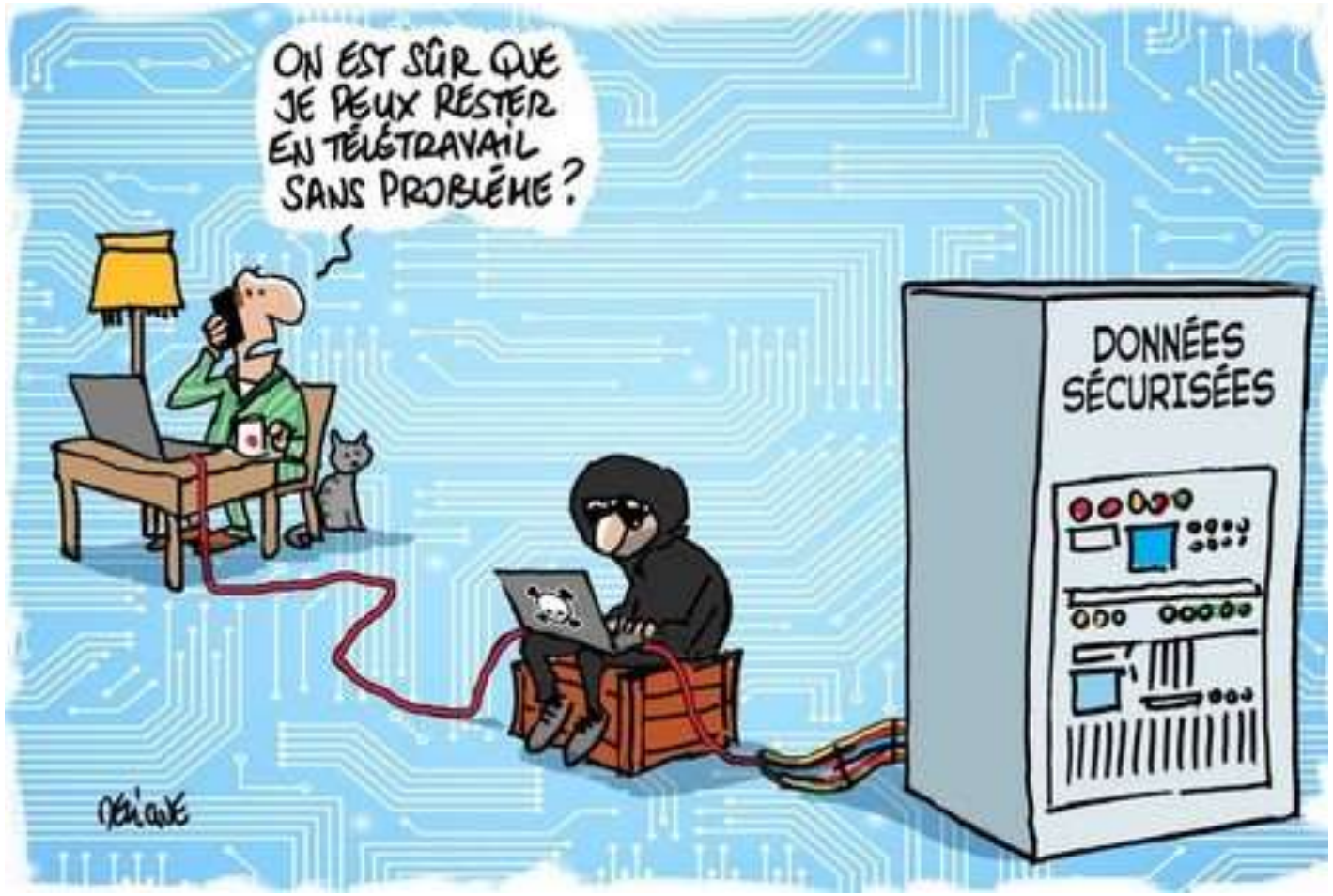
Ne cliquez jamais sur des pièces jointes que vous ne vous attendez pas à recevoir ou dont vous n'avez aucune idée. Essayez d'abord d'analyser les détails de l'e-mail comme l'adresse e-mail, le nom de domaine, les erreurs grammaticales dans le corps de l'e-mail.
Pour les liens, placez votre souris sans cliquer sur le lien.

Les réseaux Wifi

Vos mots de passe, identifiants, emails, numéros de carte de crédit… Tout ce que vous faites sur internet est visible. Pour se connecter à un Wifi public, j'active mon VPN.

Les réseaux Wifi

Le télétravail



Le Téléphone Portable

Charger votre batterie de smartphone via un port USB peut s'avérer dangereux. Les hackers peuvent voler vos fichiers, infecter votre smartphone d'un virus, ou même le rendre inutilisable.

LA SOLUTION

Vérifier les permissions des applications avant de les installer

– Appareil photo/Micro :

Prendre des photos et faire des vidéos
Enregistrer une vidéo ou un fichier audio

– Contacts/Agenda :

Consulter et modifier vos contacts
Consulter l'agenda et les données confidentielles
Ajouter ou modifier des évènements dans l'agenda et envoyés des emails aux invités à votre insu.

– Photos/Médias/Fichiers :

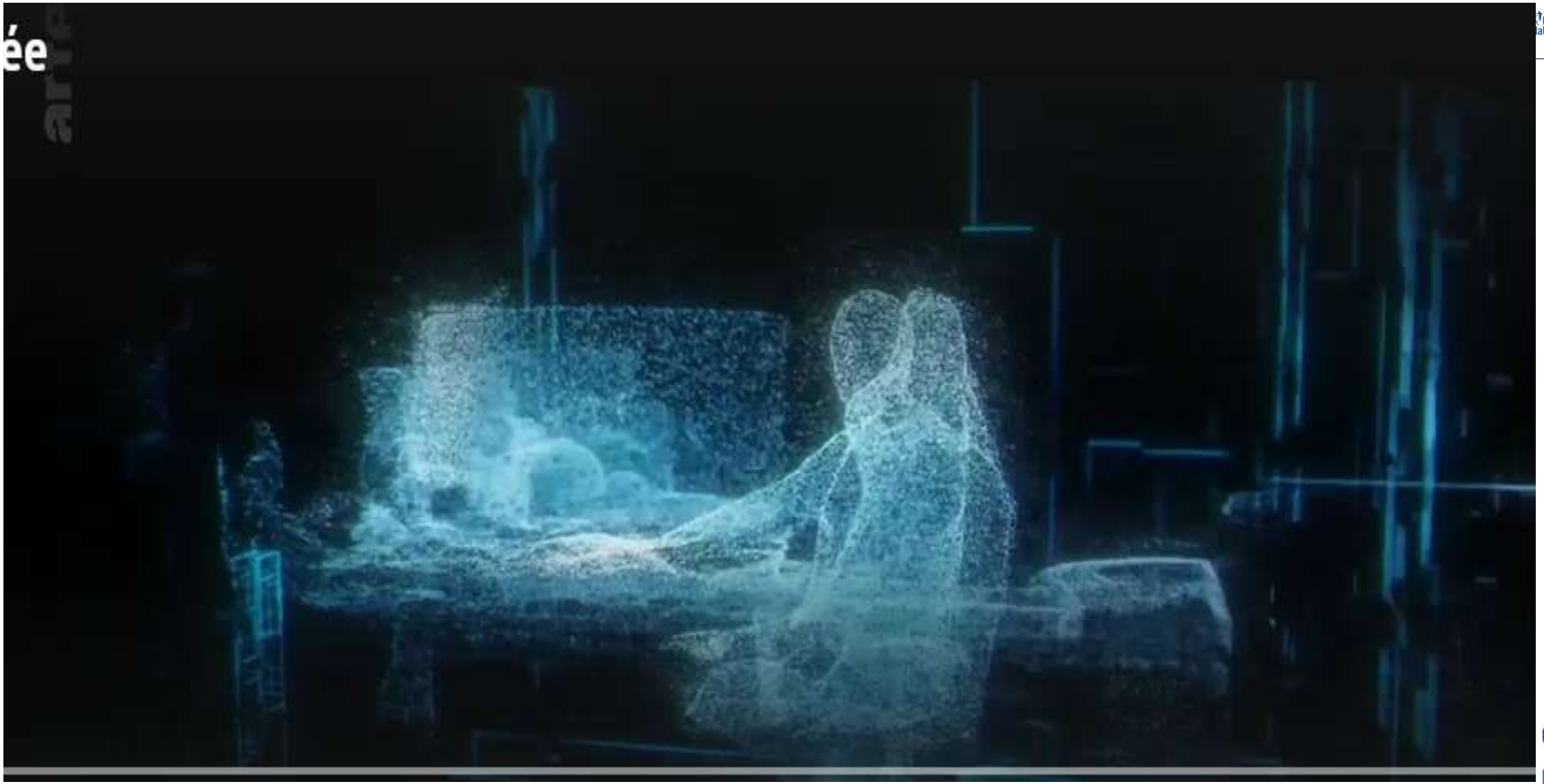
Lire, modifier ou supprimer le contenu de la mémoire de stockage, que ce soit la mémoire de stockage ou une carte SD.
Installer, désinstaller et formater la mémoire de stockage

– Autres appareils :

Consulter et écrire sur les flux de vos réseaux sociaux
Accéder aux flux auxquels vous êtes abonnés

52

CONCLUSION



CONCLUSION

« L’humain est à la fois la faille et le rempart. »

Atelier participatif

Mon Diagnostic Cyber : 10 minutes pour agir

Atelier participatif – Mon Diagnostic Cyber : 10 minutes pour agir

Mode d'emploi

1. *Chaque participant remplit un **questionnaire en ligne***

   (1 questionnaire par entité juridique)

2. *Analyse collective rapide*

3. *Plan d'action flash*

- Chaque participant sélectionne **2 actions simples et prioritaires** à lancer dans les 30 prochains jours

- Une fiche a été mise à disposition dans vos pochettes pour aider à choisir des actions concrètes et accessibles (ex. : activer le verrouillage auto des sessions, mettre à jour les mots de passe, nommer un référent cyber…)

4. *Temps d'échanges*

Scanner le QR CODE

Pause déjeuner

Reprise à 14H

La Cybersécurité en Normandie

Clôture et prochaines étapes

Merci de votre attention

contact@securnes.fr

www.securnes.fr