VIVRE DANS UN MONDE DE CYBERMENACES

Jeudi 9 avril 2026
Rencontre régionale URPS Pharmaciens

e•Santé Centre-Val•de•Loire

Êtes-vous une autruche ?

- Remettre à plus tard la stratégie cyber
- Déléguer sans vérifier (confiance aveugle)
- Penser que « ça n'arrive qu'aux autres »

En vérité, le risque n'est pas QUE technique :

- Manque de structure et d'organisation
- PCA/PRA ??

- Qui décide quoi ?
- Quoi faire dans les 4 premières heures ?
- Quels sont vos systèmes critiques ?

Si votre SI tombe demain matin à 8h, que feriez-vous dans l'heure qui suit ?

La cybersécurité, c’est quoi ?

L’ensemble des moyens déployés pour protéger les systèmes d’information (SI) : PSSI, PC, serveurs, mobiles, réseaux, données systèmes électroniques,... **contre les intrusions et attaques malveillantes .**

- **PRÉVENIR :**
  - **Sensibilisation, sauvegardes…**
- **CONTRÔLER :**
  - **Audits, scan des systèmes, surface d’exposition, vulnérabilités…**
- **DÉTECTER :**
  - **Pare-feu, antivirus, SIEM, EDR/XDR…**
- **RÉAGIR ET REMEDIER :**
  - **Gestion de crise, assistance incidents, reconstruction des systèmes**

La cybersécurité, c’est quoi ?

- **Qu’avez-vous à protéger au sein de votre SI ?**
  - Les données de vos patients (sensibles et onéreuses)
  - Les données des collaborateurs (identifiants et accès)
  - Informations confidentielles (santé)
  - Les logiciels métiers (LGO, CRM…)
  - Vos sauvegardes (3 2 1 -> 3 2 1 1 0)

- **Une sensibilisation primordiale**
  - L’humain est le premier rempart à toute forme d’attaque cyber. C’est le maillon fort !

(90% des cyberattaques sont liées à une erreur humaine. Source IBM Institute 2024)
Selon l'ANSSI, *plus de 80 % des cyberattaques débutent par un email frauduleux*.

Un monde de cybermenaces

- **Les types de cybercriminels :**
  - Etats nations
  - Cybercriminels
  - Hacktivistes
  - Groupes terroristes
  - Script Kiddies
  - Menace interne
- **Leurs objectifs :**
  - Gains financiers
  - Vol de données
  - Nuisance / Vengeance
  - Espionnage
- **Les principales cyberattaques :**
  - Malwares (Ransomware)
  - Phishing – Smishing – Quishing (SE)
  - Vol de données
  - DDOS

Un monde de cybermenaces

- **Les signes probables d’une cyberattaque**
  - Des applications qui ne fonctionnent plus (enfin plus comme d’habitude)
  - Des ralentissements réseau extrêmes
  - Des imprimantes qui crachent des notes de rançons
  - Un nouveau fond d’écran super stylé, mais quelque peu anxiogène.
  - Altérations/suppressions de fichiers (file.txt.hacked)

- **Les conséquences d’une cyberattaque**
  - Perte financière
  - Interruption totale ou partielle d’activité
  - Indisponibilité du SI
  - Vol de données
  - Réputationnel
  - Juridique

La menace cyber en santé

- **l'IA au service du crime**
  - Spear Phishing - Deep Fakes
  - Usurpation d'identité et chantage
  - Sophistication accrue

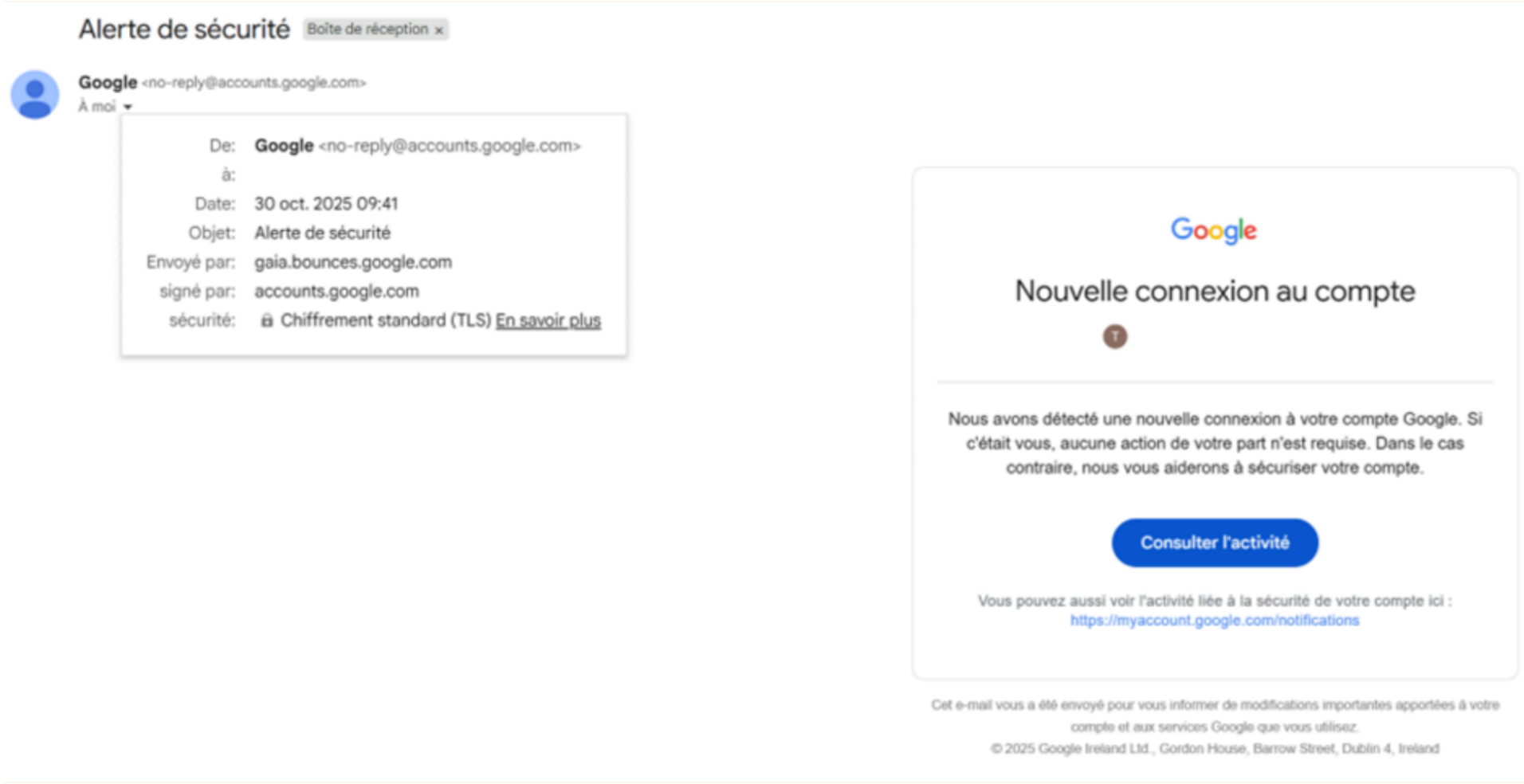
- **Pourquoi la santé ?**
  - Valorisation d'un dossier médical.
  - Données sensibles

- **Des précédents qui nous obligent à réagir**
  - ARS, GRADeS, CH, EHPAD...
  - CEGEDIM
  - 37 alertes en région CVL sur 2025 dans le domaine de la santé

- Un dossier médical vaut 250$ dollars sur le dark web.
- 1 français sur 4 s'est fait pirater ses données médicales rien qu'en 2025.
- 15,8 millions de dossiers volés
- 1500 cabinets médicaux piratés

Phishing ou pas phishing ?

Phishing ou pas phishing ?



Phishing ou pas phishing ?

Réagir en cas de cyberattaque

1ère étape : arrêter l'hémorragie

- Isolement de la machine infectée (quarantaine) en débranchant les câbles réseau et le Wi-Fi.
- N'éteignez surtout pas les ordinateurs (empreintes numériques)

2ème étape : alerter le 17 cyber : https://17cyber.gouv.fr/

- Réponse technique avec des mesures réflexes selon l'incident.
- Disponible 24h/24 et 7j/7

3ème étape : Faites appel à des spécialistes :

- En cas de virement suspect : appeler votre banque, exiger un rappel de fonds.
- Appeler votre prestaire informatique pour la remédiation. Ne surtout rien effacer (copier les preuves avant de tout réinstaller), trouver l'origine de l'intrusion.

On respire,
paniquer ne sert a rien !

Réagir en cas de cyberattaque

4ème étape : dépôt de plainte

- Avec les forces de l'ordre (Police ou Gendarmerie), il y a des cellules cyber dans chaque département.

NE JAMAIS PAYER LA RANÇON !

5ème étape : Si fuite de données

- Alerter la CNIL sous 72h.
- Informer également vos clients/fournisseurs si vol d'informations personnelles.

LA QUESTION N’EST PLUS

« est-ce que cela peut vous arriver ? »

MAIS PLUTÔT

« êtes-vous prêts si cela arrive ? »

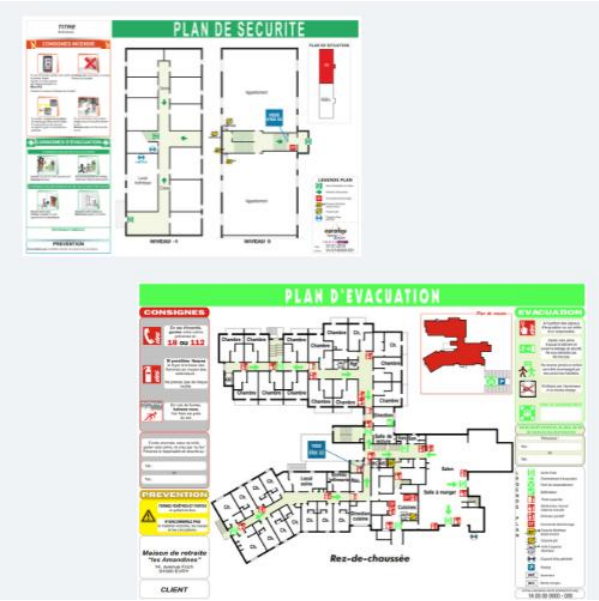
Se préparer à la menace cyber

- 3 principes de base en cybersécurité
  - Moindre privilège
  - Droit d'en connaître
  - Défense en profondeur

- Diagnostic cybersécurité

MonAide Cyber
INNOVATION ANSSI

Se préparer à la menace cyber



Se préparer à la menace cyber

- Fini les post-it ! On utilise un gestionnaire de mot de passe (keepass…). Mot de passe = mouchoir
- On verrouille sa session en cas d'absence
- Anonymiser les données si utilisation de l'IA
- Bannir les adresses Google/Yahoo/Hotmail… si envoi de documents confidentiels. MSS…quoi?
- Activer le MFA, le vrai, le TOTP clé physique ou MS Authenticator
- Mettre à jour les équipements
- Avoir des sauvegardes, testées, et qui peuvent être déconnectées (règle du 3 2 1 1 0)
- Méfiez-vous des messages inattendus et des comportements suspects ! On signale.
- Vigilance avec les supports amovibles (rubber ducky)

MIEUX VIVRE DANS UN MONDE DE CYBERMENACES

Ugo SCHURIG
Chargé de mission Cybersécurité

e•Santé Centre-Val•de•Loire