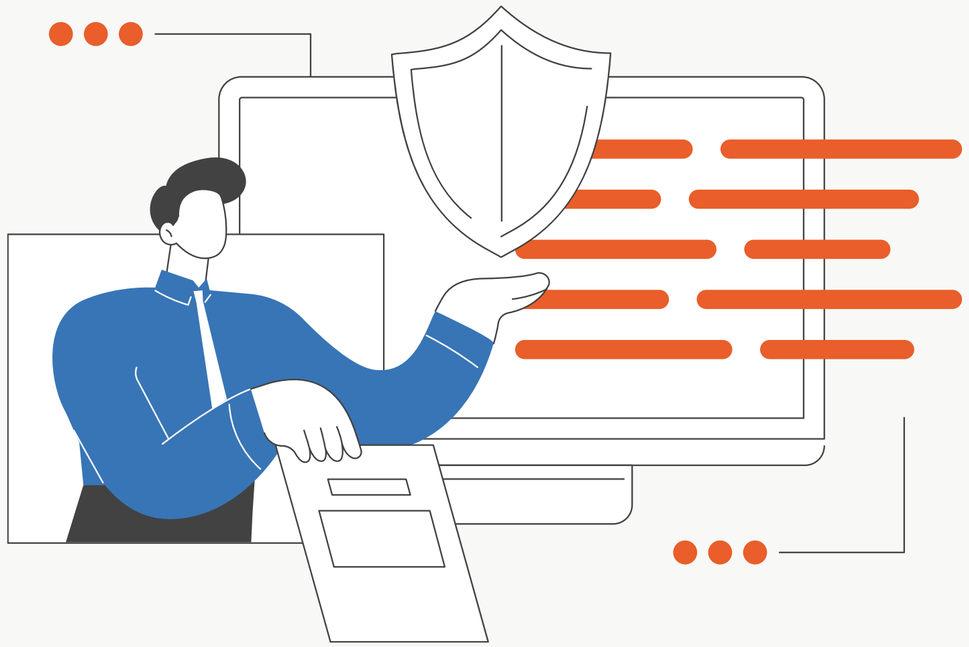
# PARLONS CPTS !

L'ÉCLAIRAGE MENSUEL SUR VOS ENJEUX QUOTIDIENS



# CPTS & CYBERSECURITE

Guichet CPTS - 2024

e-santé Occitanie
Connecter pour mieux soigner

LE GUICHET CPTS
URPS OCCITANIE

# Plan de la présentation



01 INTRODUCTION

02 NOTIONS DE CYBERSECURITE

03 BONNES PRATIQUES ET GESTION DES INCIDENTS

04 QUESTIONS / REPONSES

02

# Notions de cybersécurité

Ensemble des mesures techniques, organisationnelles et humaines, mises en place pour protéger les systèmes informatiques et les données contre les cybermenaces.

Secteur essentiel
Hautement vulnérable

Augmentation des volumes et du partage de données de santé

Ouverture des systèmes d’informations des organisations de santé

Augmentation de la valeur des données de santé

Augmentation des attaques

03

# Les bonnes pratiques

Garder la disponibilité, l’intégrité et la confidentialité des données

## SEPARATION DES USAGES

## L’OUTILLAGE ET LES PRESTATAIRES

## LES MOTS DE PASSE

## LES SAUVEGARDES

## LA PROTECTION DES DONNEES

## LES MISES A JOUR ET ANTIVIRUS

# Séparation des usages

03

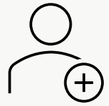
La frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse.
Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre structure que votre espace de vie privée.

## L'astuce

Utilisez des appareils distincts pour le travail et les loisirs, améliorant ainsi la sécurité et facilitant la déconnexion en dehors des heures de bureau

N'utilisez pas le même appareil pour les **usages personnels**

**Segmentez** les comptes mails/applicatifs



Créez des **comptes séparés** dans le cas de poste partagé

N'hébergez pas les **données pros** sur vos drives perso

Limitez l'utilisation de clé USBN et ne branchez que des clés dont **l'origine est connue**

N'utilisez pas de wifi public ou **non sécurisé**

# L’outillage et les prestataires

03

**TIERS - PRESTAIRES**

Votre métier vous oblige à utiliser de plus en plus d’outils. Les usages évoluent et vous devez avoir recourt à des tiers pour vous aider dans cette mission.

**LES QUESTIONS A SE POSER**

*« Ai-je vraiment besoin de l’outil ?*

*Si l’outil est payant, est-ce normal que je le trouve gratuitement ailleurs ? »*

Privilégiez les logiciels sécurisés

Utilisez des logiciels possédant une **certification** et qualification

Utilisez les logiciels fournis par les **organes nationaux** (ANS,ARS,GOUV)

S’assurer que l’outil est connu de ses pairs

Téléchargez les applications sur un site de confiance

Ne pas confier ses équipements à n’importe qui

## Les outils

**GRADeS**

Mise à disposition d’outils

**ANS**

Hébergeurs certifiées HDS

# 03

# Les mots de passe

1 Une garantie que vous seul accédez au contenu

2 L’unique protection universelle de votre identité

3 Une cible privilégiée des cybercriminels

Ne partagez pas votre mot de passe

N’utilisez pas le même mot de passe sur **différents comptes**

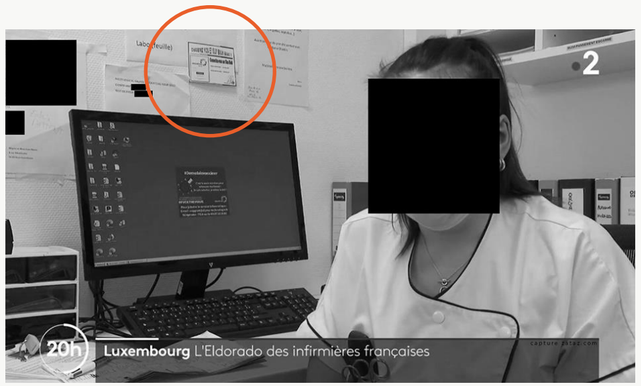
N’écrivez pas votre mot de passe sur un post-it

+ L

Verrouiller sa session dès que vous quittez votre poste

Choisissez un mot de passe robuste

Changez votre mot de passe régulièrement, même lorsque ce n’est pas obligatoire




## Les outils

**Utiliser un Coffre-fort à mot de passe**

**Utiliser Pro Santé Connect**

**Utiliser l’authentification multifactorielle**

# Les sauvegardes

03

Opération qui consiste à dupliquer et mettre en sécurité les données contenues dans un système informatique. Cela permet de pouvoir augmenter les chances de reprise d'activité après incident.

**3**
**Exemplaires des données sauvegardées**

**2**
**Supports de sauvegarde différents**

**1**
**Support déconnecté du réseau internet**

## La méthode

Identifier les données critiques à sauvegarder
Appliquer la règle du « 3-2-1 »
Chiffrer les données sensibles

## L'outils

Hébergements Cloud, les outils cloud peuvent être pertinents, cependant il faut s'assurer que l'hébergeur soit certifié HDS

# La protection des données

03

## LE CYCLE DES DONNÉES

Compte tenu de la sensibilité des données, il est important de mettre en place des mesures de sécurité pendant tout le cycle de vie de la donnée.

1. Ne partagez pas d'informations sur des médias
2. Utiliser le média adapté à la sensibilité de l'information
3. Appliquez votre devoir de discrétion même pendant vos échanges oraux
4. Voyagez léger : Ne vous déplacez pas avec vos sauvegardes et l'intégralité de vos données
5. Munissez-vous d'un filtre de confidentialité lors de vos déplacements
6. Détruisez les données sensibles que vous n'utilisez plus

## LES QUESTIONS A SE POSER

1. *Est-ce le bon outil pour l'information ?*
2. *Est-ce que la personne est légitime pour recevoir ce type d'information ?*
3. *Est-ce que la personne nécessite de connaitre l'information ?*

MSSanté

medimail

SPICO DISCUSSIONS

# 03

# Mises à jour & antivirus

Il n’est pas évident de se protéger au quotidien contre les cyberattaques, en plus des bonnes pratiques et de l’hygiène informatique, il est important de s’appuyer sur des dispositifs et mécanismes techniques dédiés.

Mettre à jour **régulièrement** les systèmes et applications

Utilisez un **Antivirus** et vérifiez la bonne mise à jour de la base virale

Ne pas ignorer les **messages d’alerte** de vos équipements

Ne désactiver pas le **pare-feu** de vos équipements

Activez l’application des mises à jour automatique sur vos applications

Téléchargez les mises à jour depuis les magasins **d’applications officiels**

## Astuce

Planifier vos mises à jour pendant vos périodes d’inactivités depuis l’outils de gestion des mises à jour Windows

1

**Isolation réseau de l’équipement**

2

**Suspendre mes activités sur le poste**

3

**Je demande de l’assistance à un prestataire qualifié**

4

**Je sacralise les sauvegardes**

5

**Je déclare l’incident auprès des autorités**

# En cas d’incident de sécurité ?

Tout événement ou activité suspecte, non autorisée ou anormale qui compromet l'intégrité, la confidentialité ou la disponibilité des systèmes informatiques, ou des données.

# Déclarer un incident

03

1 **Incident de sécurité**

2 **Portail de signalement des évènements indésirables**

https://signalement.social-sante.gouv.fr

Si malveillant

3 **Signalement à la Police / Gendarmerie**

Déposer une plainte

Si fuite de données suspectée ou effective

3 **Déclaration à la CNIL**

https://notifications.cnil.fr/notifications/index

Délai de 72h pour la déclaration

**Communiquer aux concernés**