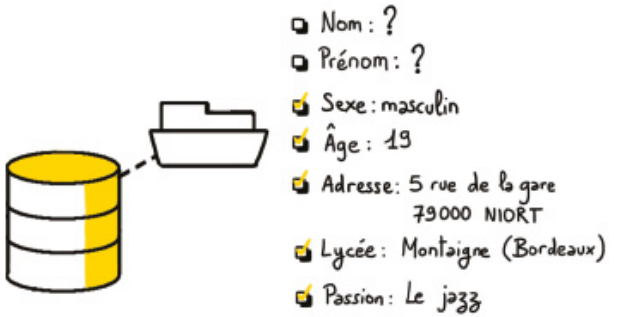
Cybermenaces et le règlement général sur la protection des données (RGPD)

21 octobre 2022

Sommaire :

→ **Cybercriminalité :** Définition , Prévention et Action

→ **RGPD** : Définition, obligations et étapes à réaliser pour les CPTS



CYBERCRIMINALITE

Définition , Prévention et Action !

JACQUES WEMAERE

SOURCES : Réserviste de la Police - la police Nationale -le réseau des référents Cyber Menace

« Ce n’est pas si mais quand! »

Quelques chiffres ….

71% Attaques - Motivation FINANCIERE

10 Attaques - cabinet dentaire en 2021

27 nombre d'établissement attaqués en 2021

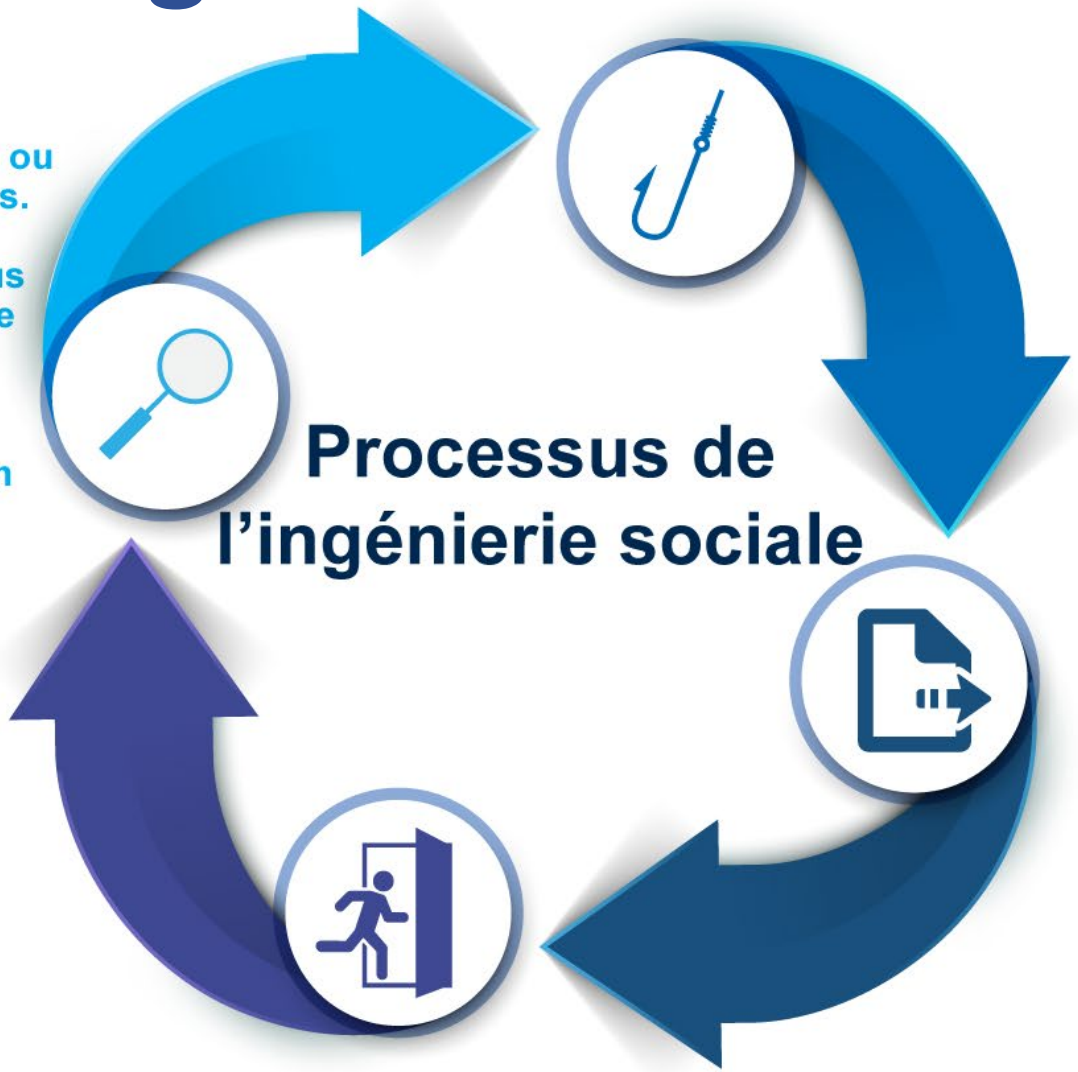
94% Attaques - à partir d'un email

85% des incidents - origine d'un erreur Humaine

Ingénierie Sociale

1 Recherche

- Choisir un événement d'actualité ou d'intérêt collectif, comme la pandémie ou la date limite de déclaration de revenus.
- Cerner les cibles potentielles (individus ou entreprises) et le meilleur moyen de les aborder.
- Recueillir des renseignements sur les victimes de diverses sources (p. ex, en ligne ou dans les déchets).



2 Prétexte

- Aborder les cibles avec une histoire fausse mais vraisemblable.
- Bâtir une relation ou établir le contrôle.
- Pousser les cibles à agir sous l'influence de la peur.
- Motiver les cibles à agir.

3 Extraction

- Obtenir des renseignements personnels ou financiers de façon frauduleuse.
- Convaincre les cibles à envoyer de l'argent par transferts électroniques, cartes cadeaux, etc.

4 Clôture

- Mettre fin à la relation.
- Décourager les cibles de parler.
- Brouiller les pistes.

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Ingénierie Sociale
Les 7 attaques les plus courantes

- Phishing
- spear Phishing
- Vishing
- Pretexting
- Baiting
- Talonnage
- Quiproquo

Prévenir les cyberattaques

→ Choisir avec soin ses mots de passe

→ Mettre à jour régulièrement vos logiciels

→ Effectuer des sauvegardes régulières

→ Sécuriser l’accès Wifi de vos cabinets

→ Être prudent lors de l’utilisation de sa messagerie

→ Être vigilant lors d’un paiement sur internet

→ Séparer les usages personnels des usages professionnels

→ Être aussi prudent avec son smartphone ou sa tablette

En cas d'attaque …

Si le système est compromis :

→Mettre en quarantaine les équipements en déconnectant les appareils du réseau (ne pas les éteindre) :

→Évaluer l'étendue de l'intrusion et collecter les preuves.

→Déposer plainte

Après avoir réalisé une analyse antivirale complète, réinstaller le système :

→ Changer les mots de passe d'accès et mettre à jour les logiciels et équipements avant la remise en système du service.

→Notifier l'intrusion à la CNIL en cas de violation de données à caractère personnel

Le règlement général sur la protection des données (RGPD) des CPTS

RGPD : définition et obligation

→ Le RGPD encadre le traitement des données personnelles et **s'applique à toute organisation, publique et privée**, qui traite des données personnelles, **quelle que soit sa taille.**

→ Qu'est-ce qu'une donnée personnelle ?

- Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».
- Une personne peut être identifiée :
  - directement (exemple : nom, prénom)
  - ou indirectement (exemple : par un identifiant (n° RPPS), un numéro (de téléphone), plusieurs éléments spécifiques propres à son identité physique, physiologique, économique, culturelle ou sociale, mais aussi la voix ou l'image (photos des élus).

RGPD : définition et obligation des CPTS

→ Qu'est-ce qu'un traitement de données personnelles ?

- Une opération, ou ensemble d'opérations, portant sur des données personnelles (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion…).
- Un traitement de données doit avoir un objectif, une finalité :
  - nous ne pouvons pas collecter ou traiter des données personnelles simplement au cas où cela nous serait utile un jour.
  - A chaque traitement de données doit être assigné un but, qui doit être légal et légitime au regard des missions de la CPTS.

Données sensibles : de quoi s’agit-il ?

Les données sensibles forment une catégorie particulière des données personnelles.

→ Informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

→ **Il est interdit de recueillir et d'utiliser ces données.** Sauf dans certains cas précis (article 9 du RGPD) et si la personne concernée a donné son **consentement exprès** (écrit, clair et explicite) ;

Les 4 grandes étapes pour la mise en conformité avec les règles de protection des données

1 - Identifiez et listez les activités de votre CPTS qui nécessitent la collecte et le traitement de données

Pour cela, vous pouvez vous appuyer sur le modèle de registre proposé par la CNIL.

2 - Faites le tri dans les données

La constitution du registre permet de s'interroger sur les données dont votre structure a réellement besoin et de vérifier :

- Que vous ne traitez pas de données sensibles (ex : données de santé), ou, si c'est le cas,
- Que vous avez bien le droit de les traiter ;
- Que seules les personnes habilitées ont accès aux données ;
- Que vous ne conservez pas les données au-delà de ce qui est nécessaire.

Les 4 grandes étapes pour la mise en conformité avec les règles de protection des données

3 - Respecter le droit des personnes : informez-les !

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données. L'information des personnes doit comporter la finalité, le fondement juridique du traitement, la mention des personnes ayant accès aux données, la durée de conservation ainsi que les modalités selon lesquelles les personnes peuvent exercer leurs droits.

4- Sécurisez les données

Vous devez prendre toutes les mesures nécessaires pour garantir au mieux la sécurité des données.

Les outils à votre disposition

Memento

Cybermenaces

et professionnels de santé libéraux

Comment les prévenir ?
Que faire en cas d'attaque ?

Les exemples de cyberattaques dans le domaine de la santé ne manquent pas. Du fait de leur accès à des données sensibles, les professionnels de santé de ville sont une cible pour les hackers…

Si vous êtes victime d'une cyberattaque, la police judiciaire propose un point d'entrée unique pour la Nouvelle-Aquitaine : ***cybermenaces-bordeaux @interieur.gouv.fr***

Adopter les bonnes pratiques :

- Protéger les accès avec des **mots de passe** robustes et différents sur tous les équipements.
- Sauvegarder les données régulièrement et conserver une **copie des sauvegardes** sur un support externe.
- Appliquer les **mises à jour** sur tous vos appareils. Les télécharger uniquement à partir des sites officiels.
- Utiliser un **antivirus** et faire régulièrement des analyses (scans) pour vérifier l'absence d'infection.
- Séparer les **usages personnels et professionnels**. Par exemple, il est conseillé d'éviter de mélanger la messagerie personnelle avec la professionnelle, ainsi que d'utiliser ses appareils professionnels pour un usage personnel (et inversement).
- Maîtriser ses **réseaux sociaux** : protéger l'accès à ses comptes et vérifier les paramètres de confidentialité. Avant de publier un message, penser à l'utilisation qui pourrait en être faite.
- **Relayer** les informations à ses équipes et les **former** aux risques de cybermenaces.

Pour se faire assister par des professionnels spécialisés : ***www.cybermalveillance.gouv.fr***

Conduite à tenir en cas d'attaque :

- Après avoir suspecté ou reconnu les signes d'un système compromis (impossibilité de se connecter, fichiers disparus, ralentissement du système…), **mettre en quarantaine** les équipements en déconnectant les appareils du réseau (ne pas les éteindre).
- **Évaluer** l'étendue de l'intrusion et collecter les preuves.
- Déposer plainte
- Après avoir réalisé une **analyse antivirale** complète, réinstaller le système.
- **Changer les mots de passe** d'accès et **mettre à jour** les logiciels et équipements avant la remise en système du service.
- **Notifier l'intrusion à la CNIL** en cas de violation de données à caractère personnel (www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles) et informer de la situation les personnes concernées par ces données personnelles.

Agora Lib Nouvelle-Aquitaine

Petit mémento sur le Règlement Général sur la Protection des Données (RGPD) à l'usage des CPTS

Le RGPD encadre le traitement des données personnelles et **s'applique à toute organisation**, publique et privée, **qui traite des données personnelles**, quelle que soit sa taille.

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Quatre principales actions à réaliser pour débuter la mise en conformité :

1- **Identifiez et listez les activités de votre CPTS qui nécessitent la collecte et le traitement de données**
Pour cela, vous pouvez vous appuyer sur le modèle de registre proposé par la CNIL.

2- **Faites le tri dans les données**
La constitution du registre permet de s'interroger sur les données dont votre structure a réellement besoin et de vérifier :
   - Que vous ne traitez pas de données sensibles (ex : données de santé), ou, si c'est le cas, que vous avez bien le droit de les traiter ;
   - Que seules les personnes habilitées ont accès aux données ;
   - Que vous ne conservez pas les données au-delà de ce qui est nécessaire.

3- **Respecter le droit des personnes : informez-les !**
Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données. L'information des personnes doit comporter la finalité, le fondement juridique du traitement, la mention des personnes ayant accès aux données, la durée de conservation ainsi que les modalités selon lesquelles les personnes peuvent exercer leurs droits.

4- **Sécurisez les données**
Vous devez prendre toutes les mesures nécessaires pour garantir au mieux la sécurité des données.

Dans certains cas, vous pourrez être conduits à désigner un délégué à la protection des données. Vous trouverez toute l'information sur les cas de désignation obligatoire ainsi que sur les compétences du délégué à la protection des données sur le site Internet de la CNIL : https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo

Pour aller plus loin :

- Le site Internet de la CNIL recense toutes les informations et les actions à réaliser pour se mettre en conformité.
- La CNIL a également mis en place un MOOC pour s'initier au RGPD et débuter la mise en conformité de votre CPTS : https://atelier-rgpd.cnil.fr/
- Vous pouvez également accéder au guide de sensibilisation au RGPD pour les petites et moyennes entreprises créé conjointement par la CNIL et BPI France.
- Le modèle de registre proposé par la CNIL.
- Concernant la sécurité des données, le site gouvernemental https://www.cybermalveillance.gouv.fr/ vous propose de l'aide en ligne.