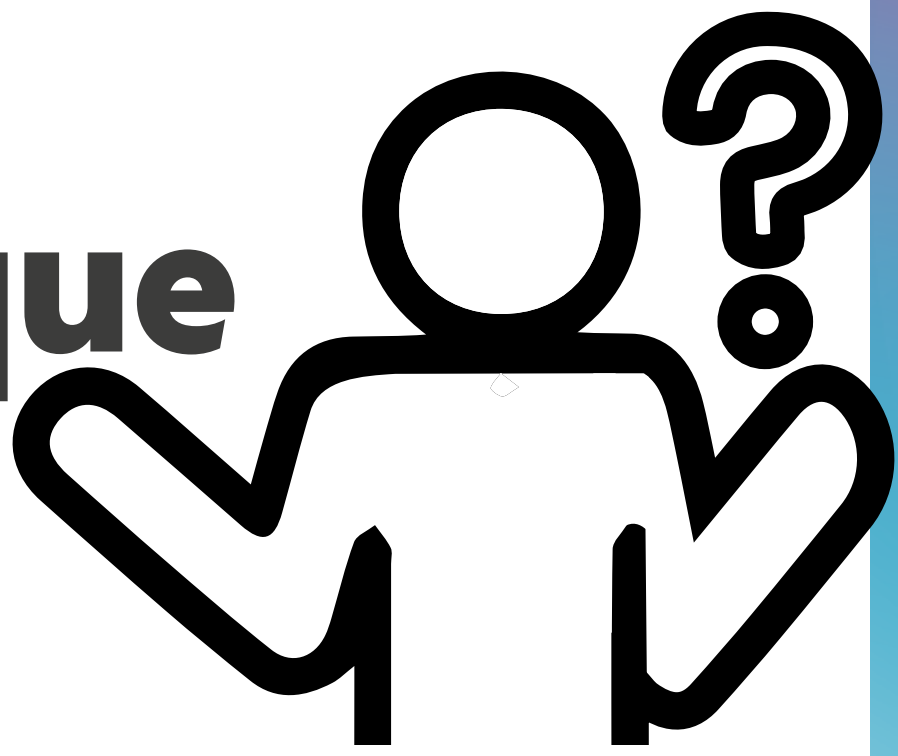
Mercr. 26 oct. 2022

Information

Cyberattaque



L'hôpital Pierre Rouquès - Les Bluets a été victime d'une cyberattaque le dimanche 9 octobre 2022.

A ce jour, la situation est totalement rétablie, tant du point de vue des soins que de la sécurité des données.

Certaines données ayant fuité au moment de l'attaque, nous vous conseillons la prudence si vous recevez des mails suspects.

Les vignettes suivantes détaillent la situation. Si vous n'y trouvez pas la réponse à vos questions, vous pouvez contacter notre Déléguée à la Protection des Données (DPO) en écrivant à **dpo.bluets@asso-croizat.org**

Mercr. 26 oct. 2022

Les principaux risques

L'hameçonnage (phishing)

L'hameçonnage consiste à vous envoyer un courriel ou SMS paraissant officiel pour vous inciter à communiquer des données personnelles et/ou bancaires.

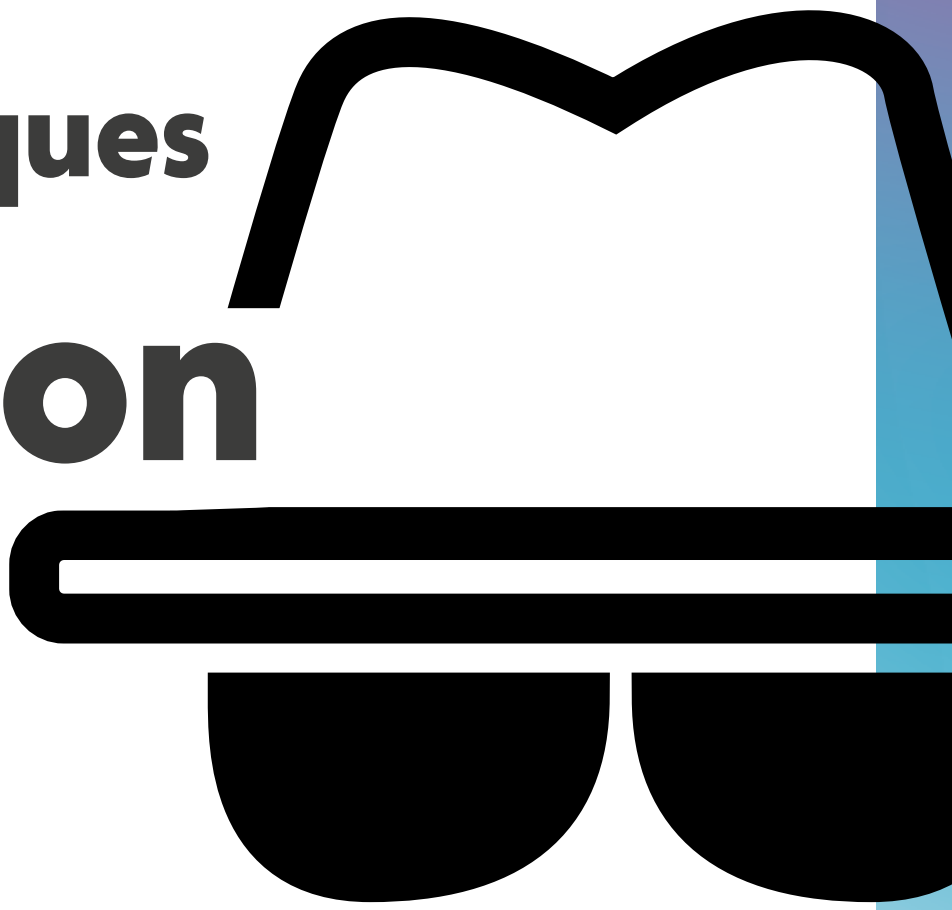
> Ce message ou cet appel paraîtra réaliste du fait de l'utilisation des données récupérées vous concernant : un soi-disant courriel de votre médecin ou de la sécurité sociale par exemple.

> Il peut s'agir : d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Mercr. 26 oct. 2022

Les principaux risques

L'usurpation d'identité



Vos informations personnelles peuvent être utilisées pour réaliser des actions frauduleuses. Ces éléments doivent vous alerter :

> Une activité suspecte sur vos comptes bancaires ou réseaux sociaux

> Des notifications de connexion inhabituelles ou de modification d'informations personnelles

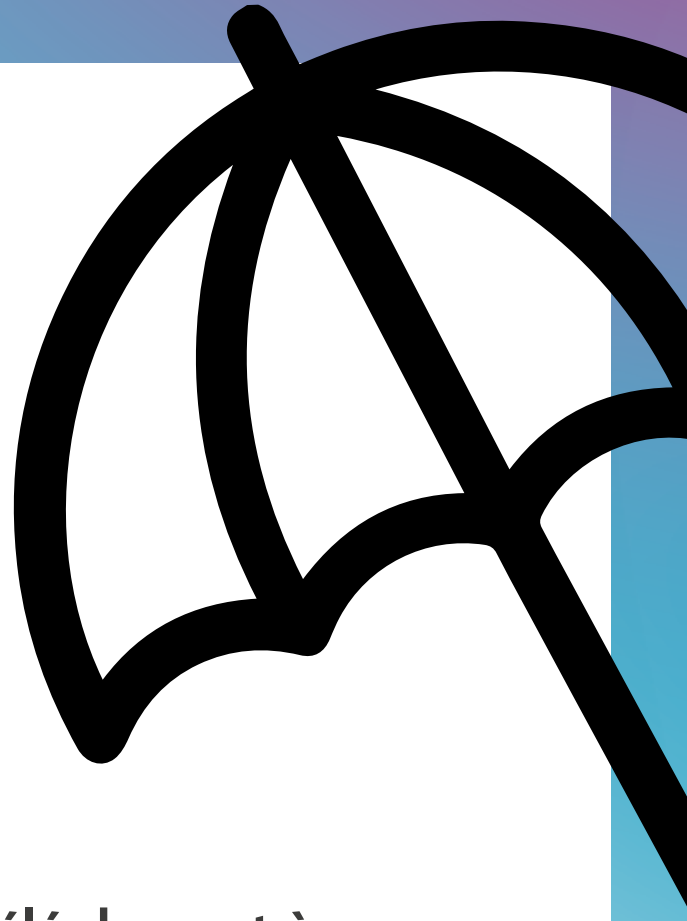
> Des relances, amendes ou condamnations inattendues

> Réception de nouveaux contrats de prêts ou crédit dont vous n'êtes pas à l'origine

Mercr. 26 oct. 2022

Se protéger

Que faire ?



Victime de phishing ?

> Vérifiez que **votre interlocuteur·rice est légitime**, en **téléphonant à l'entreprise** concernée

> Ne fournissez **pas d'informations confidentielles**

> N'ouvrez pas les pièces jointes d'un message suspect, elles peuvent potentiellement être piégées et **ne cliquez pas sur un hyperlien**.

> Changez vos mots de passe (accès bancaires, sécurité sociale, etc.)

Suspicion d'usurpation d'identité ?

> Rendez-vous sur le site cybermalveillance.gouv.fr pour obtenir des conseils pour vous prémunir d'usurpation.

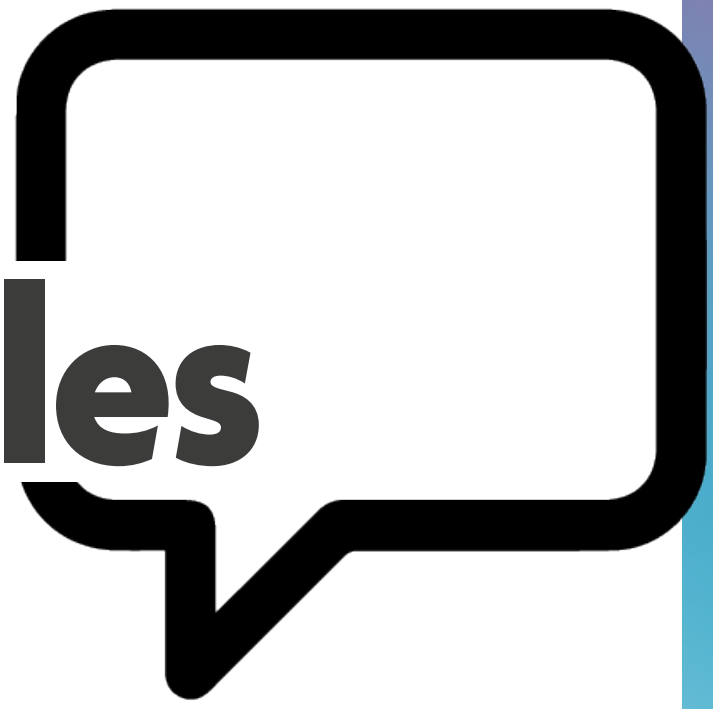
> Si l'usurpation est confirmée, **demandez auprès des services de la CNIL une consultation du fichier des comptes bancaires** (FICOBA) afin de savoir si des comptes ont été ouverts à votre nom par l'escroc.

> Nous vous encourageons à porter plainte pour «divulgation illégale volontaire de données à caractère personnel nuisibles».

Mercr. 26 oct. 2022

Se protéger

Adresses utiles



> Pour toute question, écrivez à **dpo.bluets@asso-croizat.org**.

> Vous pouvez **faire une notification auprès de la CNIL** https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

> Pour en savoir plus, **consultez ces bonnes pratiques de vigilance** informatique : https://cybermalveillance.gouv.fr/bonnes-pratiques