ASSISTANCE INFORMATIQUE
911@unc.nc
290 911

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

UNIVERSITÉ de la NOUVELLE-CALÉDONIE

CYBER MOIS

CYBERSÉCURITÉ

Le hameçonnage ou phishing

ALERT PHISHING ALERT PHISHING ALERT PHISHING

Comment reconnaitre ?

Les tentatives d'hameçonnage prennent généralement **la forme d'un mail, d'un texto ou d'une personne sur les réseaux sociaux** contenant dans le message un **hyperlien** à **cliquer** ou **une pièce jointe inconnue** à **télécharger**. Un **contexte d'urgence** est souvent établi dans le message afin de vous **inciter à agir rapidement.** Un **ton menaçant** peut également être utilisé.

Son objectif ?

Voler des informations personnelles ou **professionnelles** (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Des chiffres ?

En 2022, Le dispositif **Cybermalveillance.gouv.fr** vient de publier que la fréquentation du site a **augmenté de 53 %**, avec près de 3,8 millions de visiteurs.

Comment réagir ?

- **Ne communiquez JAMAIS** d'informations sensibles (identité, adresses, comptes, données bancaires...) suite à un message ou un appel téléphonique.
- **Ne cliquez sur aucun lien.**
- **Au moindre doute, contactez directement** l'organisme concerné pour confirmer.
- Faites **opposition immédiatement** en cas d'arnaque bancaire.
- **Changez immédiatement vos mots de passe** si vous avez malencontreusement communiqué votre mot de passe, ainsi que sur tous les autres sites ou services sur lesquels vous utilisiez ce mot de passe compromis.

ALERT PHISHING ALERT PHISHING ALERT PHISHING

ASSISTANCE INFORMATIQUE
911@unc.nc
290 911

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

UNIVERSITÉ de la NOUVELLE-CALÉDONIE

CYBER MOIS

CYBERSÉCURITÉ

Le rançongiciel ou ransomware

ALERT RANSOMWARE ALERT RANSOMWARE ALERT RANSOMWARE

Comment reconnaitre ?

Les rançongiciels sont des **logiciels malveillants** qui **bloquent l'accès** à l'ordinateur ou à des fichiers en les chiffrant et qui **réclament à la victime** le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être **infectée après l'ouverture** d'une pièce jointe, après avoir **cliqué sur un lien malveillant** reçu dans vos mails, parfois en **naviguant sur des sites compromis**, ou suite à une intrusion sur le système.

Son objectif ?

Extorquer de l'argent à la victime en échange de la promesse **(pas toujours tenue)** de retrouver l'accès aux données corrompues. **Certaines attaques** visent parfois simplement à **endommager le système** de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

Des chiffres ?

En 2022, d'après les données de cybermalveillance.gouv.fr, les ransomwares ont ciblé 66 % des professionnels.

Comment réagir ?

- **Débranchez** la machine **d'Internet** et du **réseau local.**
- **Ne payez pas la rançon.** Même si vous réglez le montant de la rançon, **rien** ne vous assure que vos fichiers seront déchiffrés ou que votre ordinateur sera de nouveau accessible. De plus, **vous alimentez** un système et démarrez un cercle vicieux : après avoir payé, vous risquez d'être identifié comme « **bon payeur** » par les cybercriminels.
- **Déposez plainte.**
- **Identifiez l'origine** de l'infection (lien, mails...).
- **Faites-vous assister** au besoin par des professionnels qualifiés.

ALERT RANSOMWARE ALERT RANSOMWARE ALERT RANSOMWARE