CYBER#365
LA CYBERVIGILANCE TOUTE L'ANNÉE

QUE FAIRE EN CAS D'ATTAQUE DE RANSOMWARE ?

Un **ransomware** (ou "logiciel de rançon") est un logiciel malveillant qui s'installe sur votre ordinateur **à votre insu**. Toutes vos données sont alors prises en otage par les hackers qui promettent de vous les rendre en échange d'une rançon.

COMMENT SE PROTÉGER ?

PHISHING	Liens, expéditeurs, pièces jointes... un seul clic peut suffire !
MOTS DE PASSE	Uniques et robustes : minuscules, majuscules, chiffres et symboles.
MATÉRIEL	Verrouillez votre session lorsque vous n'êtes pas là, ne laissez pas votre matériel sans surveillance.
WIFI + USB	Ne vous connectez pas à n'importe quel réseau, ne branchez pas votre matériel sur n'importe quelle prise.
PROCÉDURES	Faites confiance à votre DSI. S'ils mettent en place des procédures de sécurité, c'est pour vous protéger, vous et l'entreprise !

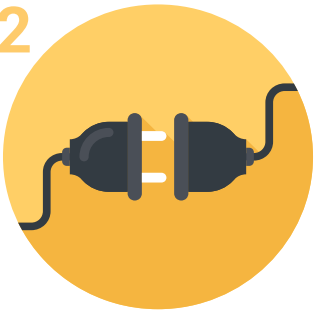
ET SI ÇA ARRIVE QUAND MÊME ?

1



Ne payez pas !
Rien ne garantit que les hackers vous rendent vos données.

2



Déconnectez-vous !
Sans Internet, le ransomware ne peut pas se propager.

3



Prévenez votre DSI !
Plus vite vous levez l'alerte, plus ils pourront gérer la crise efficacement.

© Dæsign - Ces contenus sont protégés par le droit d'auteur. Leur reproduction est interdite sans l'accord préalable de Dæsign. La reproduction sur un support papier demeure autorisée aux conditions suivantes : usage non commercial, respect de l'intégrité des documents reproduits (ni modifications, ni altérations), citation claire et lisible du copyright Dæsign.