RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONSIGNES EN CAS DE CYBERATTAQUE

1 DÉBRANCHEZ LA MACHINE D'INTERNET OU DU RÉSEAU INFORMATIQUE

Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.

2 N'ÉTEIGNEZ PAS L'APPAREIL

Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.

3 ALERTEZ AU PLUS VITE VOTRE SUPPORT INFORMATIQUE

Votre support pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.

4 N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS

Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.

5 PRÉVENEZ VOS COLLÈGUES DE L'ATTAQUE EN COURS

Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.

CIRTEL
INFORMATIQUE - RÉSEAUX - TÉLÉCOM

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

ALSACE RHIN BRISACH
PLACE À L'AUDACE!

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CYBERATTAQUE
Consignes pour les collaborateurs

Toute entreprise, association, collectivité ou administration, quelle qu'en soit la taille, peut être la cible d'une cyberattaque. Une situation qui peut avoir de graves conséquences pour l'organisation qui en est victime : techniques, financières, réputationnelles, juridiques ou encore humaines.

Une cyberattaque peut se produire à tout moment et, parfois, ce sont les collaborateurs de l'organisation visée qui en sont les premiers témoins : fichiers chiffrés, difficultés ou impossibilité d'accès aux logiciels ou systèmes informatiques, etc.

Ce document synthétique vise à fournir aux collaborateurs les consignes d'urgence à appliquer pour réagir en cas de cyberattaque et ainsi aider l'organisation à répondre au plus vite à l'incident pour améliorer ses chances d'y faire face.

Ces mesures opérationnelles peuvent faire l'objet d'un affichage dans vos locaux et à proximité de chaque poste de travail.

CIRTEL
INFORMATIQUE - RÉSEAUX - TÉLÉCOM

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

ALSACE RHIN BRISACH
PLACE À L'AUDACE !

V230419