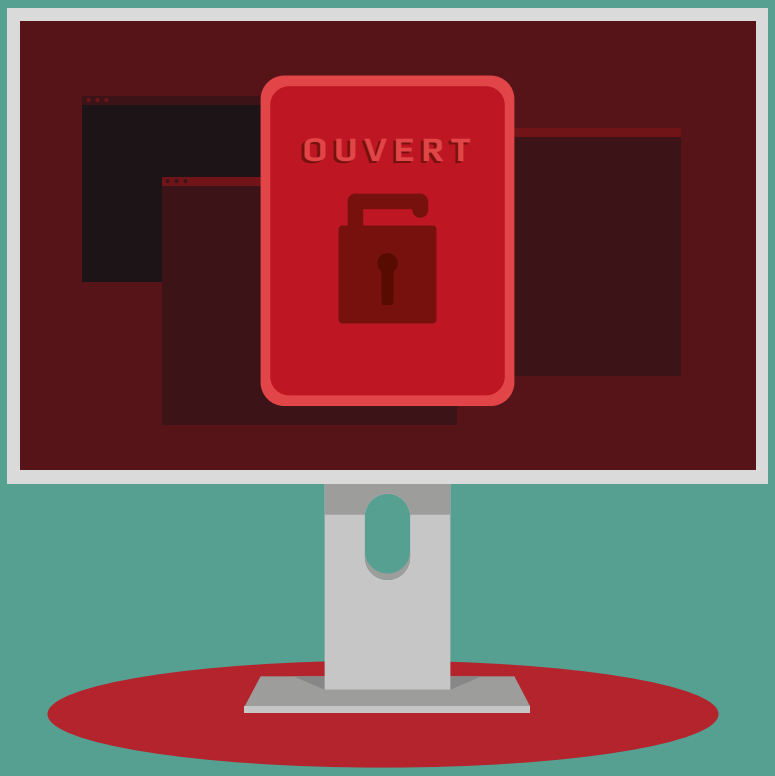
PENDANT LE CONFINEMENT, LA PORTE DE VOTRE ENTREPRISE EST FERMÉE À CLÉ, MAIS ÊTES-VOUS CERTAINS D'ÊTRE PROTÉGÉS ?



ALORS SÉCURISEZ VOS POSTES DE TRAVAIL

Le recours au télétravail est une solution face à cette situation de crise liée au COVID-19.

Ne pas s'assurer de leur sécurité c'est compromettre toute l'entreprise.

Pourtant, le télétravail peut vite devenir un danger face aux cybercriminels qui profitent de ce contexte inédit.

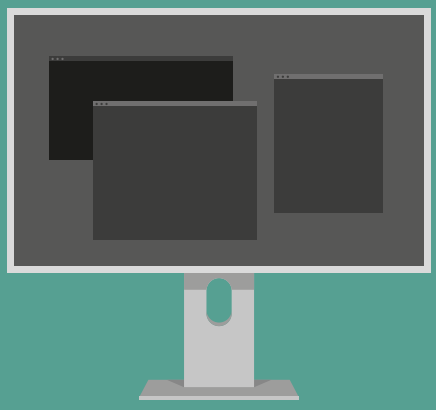
BORDEAUX

12 RECOMMANDATIONS À METTRE EN PLACE EN TANT QU'EMPLOYEUR :

1. Fournissez les équipements des télétravailleurs ou encadrez l'utilisation de leurs équipements personnels.

2. Limitez les accès extérieurs, ne permettez pas à n'importe qui d'avoir accès à vos services.

3. Sécurisez les accès extérieurs : privilégiez l'utilisation d'un VPN pour renforcer votre sécurité.



4. Ne négligez pas la force de vos mots de passe, ils doivent être suffisamment longs, complexes et uniques.

5. Faites dès que possible vos mises à jour de sécurité.

6. Sauvegardez et testez régulièrement vos données, cela pourrait être le seul moyen de les retrouver.

7. Utilisez des antivirus professionnels, ils permettent de vous protéger des attaques courantes.

8. Gardez un historique de vos activités et de vos équipements pour comprendre comment une cyberattaque a pu se produire et de pouvoir y remédier.

9. Surveillez l'activité de votre système, une anormalité peut être le signe d'une cyberattaque.

10. Sensibilisez vos collaborateurs en télétravail, une prise de conscience limitera les risques.

11. Préparez-vous à être attaqués, prévoyez un plan de crise et de communication.

12. En tant que dirigeant, montrez l'exemple !

Pour plus d'informations : https://www.cybermalveillance.gouv.fr

BORDEAUX