RÉGION DE GENDARMERIE AUVERGNE – RHÔNE-ALPES

Bulletin d'information Entreprises

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Semaine 16 - Avril 2020 – N° 2

TÉLÉTRAVAILLER EN TOUTE SÉCURITÉ

Recommandations pour les dirigeants et les salariés

Pour les cybercriminels, la crise sanitaire actuelle représente une aubaine. A l'heure où la moitié de la population mondiale est confinée, le télétravail s'est imposé, parfois après mûre réflexion, mais le plus souvent dans la précipitation. Si ce mode d'activité est actuellement considéré comme étant LA SOLUTION, il n'est toutefois pas sans risque et pose de nombreux problèmes de cybersécurité. Pour s'en prémunir, il convient donc de mettre en place un peu de TECHNOLOGIE, mais surtout de faire preuve de beaucoup de BON SENS.

Risques

Informations

06/04/2020 : Un salarié en télétravail reçoit un mail sur sa boîte professionnelle émanant d'un service enquêteur, l'informant qu'il fait l'objet d'une enquête judiciaire. La victime aurait été ciblée en raison d'une activité pornographique soutenue sur les réseaux sociaux. N'ayant rien à se reprocher et la contexture du mail étant plus que suspecte (*présence de nombreuses fautes d'orthographe et de syntaxe*), l'intéressé signale les faits.

11/04/2020 : La secrétaire d'une PME reçoit un courriel semblant provenir du service client d'un transporteur ayant pour sujet : «*Suivez vos expéditions XXX Express pendant l'éclosion de covid-19*». Le message indique qu'un colis a été retourné à l'expéditeur et que la somme de 50 € doit être réglée au plus vite via un lien ne correspondant pas au nom de domaine du transporteur. Suspectant une escroquerie, la salariée ne donne pas suite et avise sa hiérarchie.

07/04/2020 : Une société étrangère propose par mail à un commercial en télétravail d'acheter des produits de protection individuelle (*masques, gel hydroalcoolique et gants stériles*). Une commande est passée et un virement de près de 140 000 € est réalisé. Rapidement, la banque de l'entreprise victime signale le caractère douteux de la transaction. Une plainte est immédiatement déposée auprès de la gendarmerie. La coopération judiciaire européenne permet le blocage rapide des fonds sur un compte hongrois. L'enquête est en cours.

Prévention

MATÉRIEL ET LOGICIELS

- **N'utiliser que le matériel informatique et les logiciels mis à disposition par l'entreprise.**
- **Privilégier des moyens de communication sécurisés pour les échanges de documents professionnels** *(mise en place de VPN)*.
- **Sécuriser la connexion WI-FI** (*mais privilégier le partage de connexion avec un téléphone portable ou l'usage d'une clé 4G*).
- **Mettre à jour régulièrement l'ensemble des logiciels utilisés.**
- **Activer pare-feu et antivirus.**
- **Ne pas télécharger de logiciels provenant de sources non vérifiées.**
- **Effectuer régulièrement des sauvegardes externalisées ou sur support(s) externe(s) et faire régulièrement des essais de restauration pour en vérifier la viabilité.**

MESURES DE BON SENS

- **Respecter à la lettre les prescriptions de la charte informatique de l'entreprise.**
- **Utiliser des mots de passe forts (*12 à 17 caractères*) et un mot de passe différent pour chaque application et les services en lignes.**
- **Fermer sa session dès lors qu'on quitte son poste de travail.**
- **Faire preuve d'une vigilance accrue sur les réseaux sociaux et lors de la réception de mails. Attention aux pièces jointes et aux liens. (*Risque ransomware élevé*).**
- **Ne communiquer aucune information confidentielle demandée par une personne non identifiée.**
- **Ne pas utiliser le matériel professionnel à des fins personnelles.**

Pour accéder à l'ensemble des recommandations de sécurité informatique pour ***« le télétravail en situation de crise »*, cliquez sur l'icône ci-dessous :**

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Sites à consulter régulièrement

https://www.ssi.gouv.fr/
https://www.cybermalveillance.gouv.fr
https://www.ene.fr/
https://ma-solution-numerique.fr/
Formation gratuite à la cybersécurité
https://secnumacademie.gouv.fr/

Sécurité économique territoriale
Auvergne - Rhône-Alpes

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP - Tél. : 04.37.85.21.15
rgra+intel-eco@gendarmerie.interieur.gouv.fr

Bulletin d'information Entreprises N° 2

BIEN AGIR

(*à afficher à proximité du poste de travail*)

Les 4 principaux risques cyber

- L'hameçonnage (*phishing*)
- Les rançongiciels (*ransomware*)
- Le vol de données
- Les faux ordres de virement (FOVI/BEC)

RECOMMANDATIONS DE SÉCURITÉ LIÉES AU TÉLÉTRAVAIL POUR LES EMPLOYEURS

Tous ces conseils en détail sur **www.cybermalveillance.gouv.fr**

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

ÉQUIPEZ VOS COLLABORATEURS DE MOYENS MAÎTRISÉS

FILTREZ ET CLOISONNEZ VOS ACCÈS EXTÉRIEURS

SÉCURISEZ VOS ACCÈS EXTÉRIEURS (VPN, 2FA…)

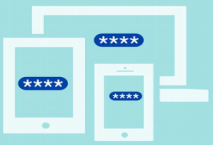
RENFORCEZ VOTRE POLITIQUE DE GESTION DE MOTS DE PASSE

AYEZ UNE POLITIQUE STRICTE DE DÉPLOIEMENT DES MISES À JOUR DE SÉCURITÉ

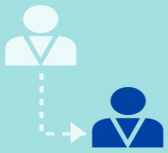
DURCISSEZ LES SAUVEGARDES DE VOS DONNÉES

UTILISEZ DES SOLUTIONS ANTIVIRALES PROFESSIONNELLES

JOURNALISEZ L'ACTIVITÉ DE VOS ÉQUIPEMENTS

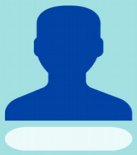


SUPERVISEZ L'ACTIVITÉ DE VOS ACCÈS EXTERNES ET SYSTÈMES SENSIBLES



SENSIBILISEZ ET APPORTEZ UN SOUTIEN RÉACTIF À VOS COLLABORATEURS EN TÉLÉTRAVAIL

PRÉPAREZ-VOUS À AFFRONTER UNE CYBERATTAQUE



DIRIGEANTS : IMPLIQUEZ-VOUS ET MONTREZ L'EXEMPLE !

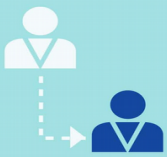
Pensez à faire adapter vos contrats d'assurance afin de couvrir les risques physiques et le matériel informatique professionnel mis à disposition des télétravailleurs.

Il est également conseillé de rédiger une charte d'utilisation du matériel informatique, d'internet et des réseaux sociaux en l'adaptant aux conditions particulières imposées par le télétravail.

RECOMMANDATIONS DE SÉCURITÉ POUR LES TÉLÉTRAVAILLEURS

Tous ces conseils en détail sur **www.cybermalveillance.gouv.fr**

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique



SI VOUS DISPOSEZ D'ÉQUIPEMENTS PROFESSIONNELS, SÉPAREZ VOS USAGES

APPLIQUEZ STRICTEMENT LES CONSIGNES DE SÉCURITÉ DE VOTRE ENTREPRISE

NE FAITES PAS EN TÉLÉTRAVAIL CE QUE VOUS NE FERIEZ PAS AU BUREAU

APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS ÉQUIPEMENTS CONNECTÉS

VÉRIFIEZ QUE VOUS UTILISEZ BIEN UN ANTIVIRUS ET SCANNEZ VOS ÉQUIPEMENTS

RENFORCEZ LA SÉCURITÉ DE VOS MOTS DE PASSE

SÉCURISEZ VOTRE CONNEXION WIFI

SAUVEGARDEZ RÉGULIÈREMENT VOTRE TRAVAIL

MÉFIEZ-VOUS DES MESSAGES INATTENDUS

N'INSTALLEZ VOS APPLICATIONS QUE DANS UN CADRE «OFFICIEL» ET ÉVITEZ LES SITES SUSPECTS