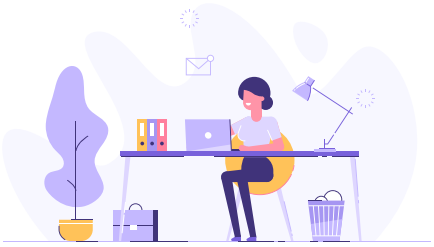
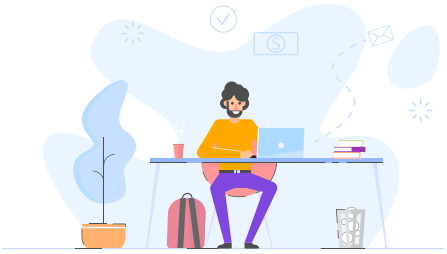
MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité





LE TÉLÉTRAVAIL AU MINISTÈRE DES ARMÉES

1 RISQUES ET MENACES

Pendant la crise du Covid-19, la résilience du ministère repose notamment sur celle de ses systèmes d'information. Dans le domaine de la cyberdéfense, une vigilance renforcée est nécessaire du fait :

- de l'augmentation des risques liés au télétravail pouvant porter atteinte à la confidentialité, à la disponibilité et l'intégrité des données :
  - non-respect des règles de sécurité lors des transferts de données entre réseaux de nature et classification différentes,
  - perte ou vol d'équipements lors des trajets ou au domicile,
  - utilisation des ordinateurs, tablettes ou smartphones personnels et des accès domestiques ou public au réseau Internet à des fins professionnelles ;
- des cyberattaques spécifiques liées à la crise : email de hameçonnage (phishing) avec pièce jointe ou lien Internet piégé, recherche de renseignement lié à la défense ou de données personnelles, désinformation.

A titre d'illustration, plusieurs incidents Cyber liés à la crise Covid-19 sont rapportés en sources ouvertes :

- le 12 mars, Google Play a retiré une application permettant à ses utilisateurs de déterminer, grâce à une série de questions, s'ils présentaient des symptômes du Covid-19. Cette application jouait sur la peur de l'épidémie pour recueillir des numéros de téléphone et des données de géolocalisation en temps réel.
- Le 6 mars, une campagne d'hameçonnage a été détectée en Italie. Les courriels frauduleux contenaient en pièce jointe un document Word censé fournir des précautions contre le Covid-19. Il installait en réalité le malware trickbot, étape préalable à des actions de cybercriminalité.
- Sous le prétexte de permettre d'utiliser l'application « Coronavirus map » qui recense les cas en temps réel dans le monde, des attaquants ont incité de nombreux utilisateurs à télécharger un malware permettant de dérober leurs données et d'accéder à leurs nom, mots de passe et numéros de cartes de crédit.
- L'hôpital universitaire de Brno en République tchèque a été victime d'une cyberattaque le 12 mars, qui a entrainé le report des interventions chirurgicales les plus urgentes et un transfert de patients vers un autre établissement.

2 CE QUI EST AUTORISÉ DANS LE CADRE DU TÉLÉTRAVAIL

Le traitement et l'échange des données de niveau NON PROTEGE sont autorisés sur tous types de réseaux, Internet et applications de messagerie inclus. Toutefois, il est rappelé que la collecte et la mise en perspective de plusieurs informations non protégées peuvent permettre, par corrélation, d'obtenir des informations sensibles.

Le traitement et l'échange des données de niveau DIFFUSION RESTREINTE sont autorisés uniquement sur les ordinateurs portables SMOBI équipés d'une clé (« **token** ») pour se connecter à Internet, les tablettes SMOBI ou les smartphones SMOBI.

3 CE QUI EST INTERDIT DANS LE CADRE DU TÉLÉTRAVAIL

Le traitement et l'échange de données classifiées de défense, en position de télétravail à domicile, sont interdits.

Sur un poste Intradef, tenter d'installer ou de lancer des programmes ou fichiers exécutables non référencés par la DIRISI est interdit.

L'élaboration, le stockage et le traitement de données de niveau DIFFUSION RESTREINTE sur un ordinateur personnel, un smartphone ou une tablette reliés à Internet, hors SMOBI, sont interdits.

Les applications de messagerie chiffrées comme Whatsapp, Protonmail, Signal, etc. ne constituent pas des plateformes d'échange de données de niveau DR.

L'utilisation de supports amovibles (clés USB) pour le transfert de fichiers est interdite en l'absence de sas antivirus ou station blanche fournis par la DIRISI. Il est en particulier interdit de brancher sur son poste de travail des supports amovibles personnels.

4 BONNES PRATIQUES ET RECOMMANDATIONS

Le personnel du ministère placé en position de télétravail a le devoir de rendre compte immédiatement dès lors qu'une situation anormale est constatée sur son poste de travail professionnel. Exemple : alerte déclenchée par l'antivirus, observation de prise en main à distance (déplacement incontrôlé du curseur de la souris), réception de mail douteux, défacement d'un site du ministère, etc.

Les comptes-rendus doivent remonter par la chaine SSI, dont le premier maillon est le correspondant SSI d'organisme (CSSI ou OSSI), préalablement identifié.

Le site Internet institutionnel cybermalveillance.gouv.fr a émis des recommandations spécifiques liées à la crise Covid-19.

Il est recommandé de mettre à jour les antivirus des ordinateurs et moyens personnels.

Le passage au SAS antivirus des supports amovibles avant connexion à un réseau du ministère est obligatoire.

Les données enregistrées sur le disque dur (dans le répertoire Mes documents) du poste de travail professionnel doivent être sauvegardées régulièrement sur les disques durs partagés en réseau ou les portails collaboratifs.