



Paris, le 25 octobre 2019

Dans sa com', la DG supprime ... déjà les droits indirects !

La Direction Générale (DG) s'est fendue dernièrement d'une adresse aux agents sur la sécurité informatique. Dans le prospectus diffusé dans ses espaces collectifs, il y est question de « reconnai[ssance] » et de « préven[tion] des menaces » (voir numérisation ci-contre).

Jusque là, rien que de très normal. Cela s'inscrit dans une certaine « pro-activité ». Le visuel explicite et la mise en page dénotent également un certain professionnalisme.

C'est pourquoi nous sommes profondément troublés par la signature du document : Direction Générale des Douanes (DGD). Et non Direction Générale des Douanes et Droits Indirects (DGDDI) !

Est-ce une anticipation du devenir de la DGDDI ? Une préparation des esprits à s'habituer à sa dénomination future ?

Surinterprétation ? À corriger donc ! Et d'indiquer « et Droits Indirects ». Les agents de la DGDDI en sauront gré à leur Direction Générale.

Menaces informatiques
Ne vous mettez plus en danger

1. RECONNAÎTRE LES MENACES

- 1 La destabilisation**
Attaques visant à porter atteinte à l'image de la douane ou à un de ses agents.
- 2 L'espionnage**
Recherche d'informations par des moyens secrets ou illicites à des fins de renseignement ou de fraude.
- 3 Le sabotage**
Destruction, la perturbation ou mise hors service intentionnelle d'un équipement, d'un matériel ou d'une installation.
- 4 La cybercriminalité**
Attaques essentiellement dans un but lucratif, de type «rançongiciel» (ransomware) et d'«hameçonnage» (phishing) bloquant l'accès aux données.

2. PRÉVENIR LES MENACES

- Je ne tente pas de modifier les paramètres de sécurité de mon équipement (poste de travail, smartphone).
- Je suis attentif à mon matériel pour éviter le vol ou les pertes.
- Je suis vigilant sur le contenu des mails reçus et je vérifie l'identité de mes interlocuteurs.
- Je suis discret sur mon activité en dehors du cadre de travail.
- Je me méfie des cadeaux (clé usb, smartphone) et des objets connectés. Ils pourraient être infectés ou piégés.
- Si j'ai le moindre doute, je contacte le TSI.

3. RÉAGIR EN CAS D'ATTAQUE

JE CONTACTE LE TSI :

En cas de vol, de perte de matériel ou de données, de soul informatique ou de sollicitation par un inconnu.

En cas de suspicion d'attaque par un virus informatique, je déconnecte le câble réseau et je laisse le poste de travail allumé.

**Direction Générale des Douanes
Bureau Satisfaction des utilisateurs**

Direction Générale des Douanes
Bureau Satisfaction des utilisateurs

Pour défendre l'intégrité du réseau, 2 rendez-vous !

→ **Jeudi 14 novembre 2019 :**
mobilisation DGFIP-DGDDI

→ **Jeudi 5 décembre 2019 :**
mobilisation interprofessionnelle

Annexe : 2^{ème} prospectus diffusé dans les services (avec la même signature en bas de page...)



Sécurité informatique

Quelques règles à respecter



SUR MON POSTE DE TRAVAIL

- Je définis un mot de passe Windows sécurisé (minimum 8 caractères, comportant des majuscules, des minuscules, des chiffres et caractères spéciaux).
- J'effectue des sauvegardes régulières de mes documents de travail importants, en privilégiant si possible le serveur réseau mis à ma disposition.
- J'utilise un dossier «données privées» créé sur mon poste pour mes données personnelles.
- Si les mises à jour Windows et antivirus de mon poste de travail ne sont pas effectuées, je contacte le TSI.
- Je ne connecte sur mon poste de travail que des équipements fournis ou validés par le TSI (clé usb...).
- Je quitte ou je verrouille ma session en fin d'utilisation.



MA CONNEXION À LA MESSAGERIE MERCURE

- Je ne me connecte jamais sur Mercure depuis un poste inconnu (cybercafé...).
- Je consulte ma messagerie à l'abri des regards.
- Je suis attentif aux messages reçus et à leurs émetteurs afin d'éviter le phishing.
- Je déconnecte ma session en fin d'utilisation.



EN DÉPLACEMENT

- Avant de partir, je vérifie si besoin avec le TSI le verrouillage automatique de mes équipements (ordinateur portable, smartphone).
- Je vérifie la sensibilité des données contenues dans mes équipements. Si nécessaire, je demande un moyen de chiffrement au TSI.
- Je ne laisse jamais mes équipements sans surveillance.
- Je privilégie la connexion à des réseaux maîtrisés ou de confiance.



MA PRÉSENCE SUR LES RÉSEAUX SOCIAUX

- Je suis discret sur ma situation et mon activité professionnelles.
- Je reste vigilant sur le contenu diffusé.
- Je n'utilise pas mon adresse mail professionnelle, y compris sur LinkedIn.
- Je privilégie les pseudos sur les réseaux non professionnels.



Direction Générale des Douanes
Bureau Satisfaction des utilisateurs