FICHE 19

QUELS SONT LES PREMIERS RÉFLEXES À ADOPTER EN MATIÈRE D'USAGES NUMÉRIQUES ?

Une fois les services numériques en place, vous devez les utiliser de manière adaptée à vos besoins tout en réduisant l'exposition à des risques de sécurité (intrusion informatique, fraude, etc.).

VÉRIFIER LES FACTURES DE VOS FOURNISSEURS

Vos factures réunissent de nombreuses données (nombre, typologie et durée des appels et des SMS/MMS, options et services souscrits, remises, services supplémentaires facturés, etc.).

Il est important de vérifier l'exactitude de vos factures, en particulier les premières émises après la signature du contrat.

ADAPTER LES SERVICES À VOS BESOINS

Si vous souhaitez réduire vos coûts liés aux communications électroniques, vous devrez vous assurer de la **réalité de votre besoin et évaluer les bénéfices de chacun des services souscrits au regard de leurs coûts associés.**

Par exemple, le transfert d'un appel d'une ligne fixe vers une ligne mobile est pratique mais peut se révéler coûteux : vous payez le prix de la communication entre la ligne sur laquelle le renvoi est activé et le téléphone mobile destinataire du renvoi. Une mesure simple consiste à utiliser les services de restriction d'appel en fonction de vos besoins métier : communications internationales, option d'itinérance sur les mobiles, communications vers les numéros surtaxés, etc.

L'évolution de vos besoins peut également vous conduire à modifier les points de vigilance et les paramètres de restrictions.

Le suivi de la consommation par la lecture détaillée de vos factures permet **d'identifier l'usage réel des moyens de communication que vous utilisez :** vous pouvez alors faire évoluer votre offre de façon à ce qu'elle soit adaptée à vos besoin réels.

Les opérateurs et certains fournisseurs spécialisés proposent des outils d'analyse des données de facturation et de trafic permettant d'en extraire des graphiques et des tableaux synthétiques qui facilitent la compréhension des usages à l'échelle de tous vos utilisateurs. Cela vous permet d'identifier facilement des services sous ou non-utilisés.

En ce qui concerne les mobiles, donnez à vos employés des conseils pour éviter la casse, la perte ou le vol de leur terminal et communiquez-leur les procédures à suivre lorsque de tels événements se produisent (vous trouverez plus de précision dans la partie dédiée ci-dessous « perte et vol d'équipement mobile »). Vous pouvez aussi fournir des équipements de protection pour prévenir la dégradation du matériel. Enfin, en cas d'usage intensif d'un terminal mobile, privilégiez les équipements à faible DAS[1] (débit d'absorption spécifique), c'est-à-dire qui émettent moins d'ondes électromagnétiques, et incitez à l'utilisation d'un kit main libre (pour en savoir plus : 🌐 Les bons gestes pour limiter son exposition).

Communiquez, auprès de vos salariés, sur les bonnes pratiques pour la maîtrise des dépenses de communications électroniques (par exemple lors des déplacements à l'étranger).

1. Les termes surlignés sont définis dans le glossaire en page 122.

DIFFUSER LES BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ

Les moyens de communications électroniques constituant un des principaux liens vers l'extérieur, ils vous exposent à des risques en matière de sécurité : fraude, vol de données, etc. Ce risque s'est par ailleurs accru avec la convergence entre les communications électroniques et l'informatique classique.

Il est important de sensibiliser vos différents utilisateurs aux bonnes pratiques en matière de sécurité :

- **pour les personnes chargées de la gestion du parc et du support informatique :**
  - **connaissance du parc informatique,** des actifs métiers, des accès existants aux locaux et des accès aux ressources physiques et informatiques de l'entreprise ;
  - **identification et interdiction des usages à risque** (par exemple, analyse des pièces jointes ou des liens dans les courriers électroniques) ;
  - **changement régulier des mots de passe** d'accès aux interfaces d'administration et aux équipements réseau (serveurs, etc.) ;
  - **utilisation de mots de passe avec des contraintes fortes,** différents pour chaque service et lorsque c'est possible, de l'authentification à double facteur (clé d'accès, etc.) ;
  - **déploiement et mise à jour des logiciels de sécurité** (pare-feu, antivirus, etc.), sauvegarde des données les plus sensibles, chiffrement des disques ;
  - **vigilance sur l'utilisation des appareils électroniques** (vol ou espionnage d'un équipement, prêt d'un téléphone, etc.) ;
  - **définition de procédures adaptées en cas d'incident :** qu'il s'agisse du vol d'un téléphone mobile, de la compromission d'un mot de passe, ou de la détection d'un virus ;
  - **sauvegardes régulières,** a minima quotidiennement, des données importantes pour votre entreprise ;
  - **mise en oeuvre d'une application de mobile device management** qui permet de gérer une flotte d'appareils mobiles et assure que les salariés ont des terminaux à jour et correctement sécurisés ;
  - **sensibilisation régulière des salariés** aux problématiques de sécurité et aux procédures de signalement ;
  - fourniture et formation des salariés à l'utilisation d'un **gestionnaire de mots de passe** (Keepass, etc.) ;
  - **tester régulièrement** la propension des salariés à cliquer sur des liens de phishing ou à ouvrir des pièces jointes contenant des logiciels malveillants ;
  - **faire de la pédagogie** sur les types d'appels ou messages les plus susceptibles de présenter des risques pour la sécurité de l'entreprise ;
  - **fournir un filtre de confidentialité** pour les écrans des postes utilisés dans des lieux publics;
  - **sensibiliser sur les mauvaises pratiques dans les lieux publics :** ne pas laisser d'équipements ou de documents sans surveillance ; ne pas discuter (par exemple des conversations en groupe ou au téléphone) d'informations sensibles (par exemples des données personnelles ou des informations pouvant dévoiler des failles de sécurité) ; éviter certains usages lorsque connecté à un réseau Wi-Fi public.
- **pour les autres salariés :**
  - **changement régulier des mots de passe** d'accès aux services et aux équipements ;
  - **utilisation de mots de passe avec des contraintes fortes,** différents pour chaque service et, lorsque c'est possible, de l'authentification à double facteur (clé d'accès, etc.) ;
  - séparation des équipements (téléphone, ordinateur, etc.) entre usages privé et professionnel ;
  - **vigilance lors de l'utilisation des appareils électroniques** (espionnage d'un équipement dans les transports en commun, utilisation de connexions non sécurisées, usages dans des pays hors de de l'Union européenne, etc.) ;
  - **vigilance lors de la réception d'appels,** SMS/MMS ou courriers électroniques frauduleux ;
  - **connaissance et respect des procédures adaptées** définies par les personnes chargées de la gestion du parc et du support informatique en cas d'un incident.

Des prestataires (notamment opérateurs, intégrateurs/installateurs, cabinets de conseil) peuvent aussi vous accompagner dans cette démarche.

Vous pouvez vous référer à des guides de bonnes pratiques existants en matière de cybersécurité. Les systèmes téléphoniques étant également susceptibles d'être l'objet de piratage, certaines règles sont à suivre afin de les sécuriser.

→ 🌐 **Guide de l'ANSSI sur la cybersécurité pour les TPE/PME**

PERTE ET VOL D'ÉQUIPEMENTS PORTABLES

Les équipements portables, en particulier les smartphones et les ordinateurs, présentent un risque particulier de perte et de vol. Or, ils peuvent contenir des données importantes pour l'entreprise.

Donnez des consignes de sécurité pour protéger l'accès aux données (exemple : retour automatique en veille avec code de sécurité pour réactiver le téléphone mobile, verrouillage des ordinateurs lorsque les utilisateurs s'en éloignent, fourniture de cadenas pour accrocher les ordinateurs portables des salariés, etc.). Le cas échéant, n'oubliez pas vos obligations de notification vers les autorités compétentes (ANSSI si vous manipulez des données classifiées ou si vous disposez d'un statut particulier[2], CNIL en cas de violation de données personnelles[3], etc.).

Donnez à vos employés la procédure à suivre en cas de perte ou de vol pour en faire la déclaration dans les meilleurs délais, auprès de l'opérateur ou du responsable de la flotte dans l'entreprise en fonction de l'organisation retenue.

Pour davantage d'informations vous pouvez consulter la page dédiée sur le site de l'Arcep : 🌐 **Que faire en cas de vol de mon téléphone mobile ?**

🔍 **Bon à savoir :**

- L'opérateur est en mesure de bloquer la carte SIM et de rendre la ligne inaccessible si vous lui communiquez le code IMEI. Il est donc recommandé d'identifier et de sauvegarder ce code IMEI à la réception du nouveau terminal (information transmise dans la documentation à la livraison). Vous pouvez également récupérer ce code en appelant gratuitement le *#06# avec votre téléphone.

  ⚠ **Attention,** si vous avez perdu la documentation fournie à la livraison et que votre mobile a été perdu ou volé, vous ne pourrez plus récupérer ce code, anticipez donc le plus possible la récupération de cette référence.

- Si vous déposez plainte auprès des services de police ou de gendarmerie, l'opérateur disposera d'un délai de 4 jours ouvrés à compter de la réception de la déclaration officielle de vol pour bloquer l'utilisation du téléphone volé.
- Il est possible, avec certains mobiles ou certains logiciels dits de « mobile management », de faire bloquer le mobile, de le localiser et même dans certains cas d'effacer les contenus professionnels à distance.

DROITS ET OBLIGATIONS EN MATIÈRE D'INTERNET OUVERT

Depuis 2015, le 🌐 **Règlement établissant des mesures relatives à l'accès à un internet ouvert** garantit au sein de l'Union européenne la neutralité du net c'est-à-dire l'égalité de traitement et d'acheminement de tous les flux d'information sur internet, sans discrimination ni restriction, indépendamment de l'origine, de la destination ou du contenu des communications.

En tant qu'utilisateur, vos accès à une connexion à internet sont ainsi pourvus d'un certain nombre de droits vis-à-vis de votre fournisseur d'accès à internet (FAI). Le texte européen prévoit notamment le droit pour tous les utilisateurs européens d'accéder et de diffuser les contenus de son choix en ligne : cela signifie que votre FAI ne peut bloquer ni ralentir l'accès à des services ou applications spécifiques, sauf dans des cas limités et définis (ex : obligations légales, mesure de gestion de trafic temporaire, service spécialisé). Il doit aussi fournir des informations claires sur les caractéristiques de votre connexion. En cas d'anomalie, une alerte peut être transmise à l'Arcep, via sa plateforme de signalement « J'alerte l'Arcep ».

Si vous offrez une connexion à internet, gratuite ou payante, ouverte au public (par exemple un réseau Wi-Fi dans vos locaux ouverts à vos clients), vous devez également vous conformer aux mêmes exigences en tant que fournisseur d'accès à internet. Il s'agit en particulier de s'abstenir de bloquer ou ralentir l'accès à certains sites ou applications, en dehors des situations prescrites par la loi ou de mesures de gestion de trafic exceptionnel pour préserver l'intégrité et la sûreté du réseau ou pour prévenir les risques de congestion. L'ouverture d'un réseau Wi-Fi public ne nécessite pas de déclaration au préalable auprès de l'Arcep.

→ 🌐 **Le règlement internet ouvert (UE) 2015/2120**

→ 🌐 **Les obligations en matière de conservation des données de trafic**

2. 🌐 https://cyber.gouv.fr/notifications-reglementaires
3. 🌐 Notifier une violation de données personnelles