

FICHE PRÉVENTIVE

Comment se prémunir des cyberattaques ?

Les attaques ciblent nos identifiants, nos sujets et nos outils.
La vigilance individuelle est la première barrière de protection du service public

Liste non exhaustive des différentes cybermenaces :

HAMEÇONNAGE (PHISHING)

Des acteurs malveillants usurpent l'identité d'un tiers de confiance pour diffuser un message frauduleux contenant une pièce-jointe piégée ou un lien vers un site frauduleux dans le but d'obtenir des informations confidentielles ou d'installer un logiciel malveillant.

DÉNI DE SERVICE OU DENIAL SERVICE (DDoS)

Une attaque par déni de service consiste à inonder un serveur de requêtes pour le faire tomber en panne et le rendre inaccessible. L'attaque donne l'impression que l'attaquant a pu accéder aux données. Ce n'est pas toujours le cas : un serveur peut être saturé sans qu'il y ait eu violation de données.

RANÇONGICIEL (RANSOMWARE)

Un rançongiciel est un logiciel malveillant qui chiffre des fichiers ou bloque l'accès à un appareil afin d'exiger une rançon. L'infection survient généralement après l'ouverture d'un contenu frauduleux, la visite d'un site compromis ou une intrusion dans le système.

ARNAQUE AU FAUX SUPPORT TECHNIQUE

Des usurpateurs affichent de fausses alertes ou appellent pour faire croire à un problème grave et se faire passer pour un support officiel. Ils cherchent à faire payer un faux dépannage ou à installer des logiciels nuisibles.

ADOPTONS LES BONS GESTES NUMÉRIQUES

Nous sommes tous et toutes un maillon essentiel : la cybersécurité repose sur la vigilance de chacun

J'adopte les bons réflexes de prévention pour minimiser les risques de cybermenace

LES MOTS DE PASSE : première barrière de protection contre les accès non-autorisés



- Adopter un mot de passe fort (14 caractères combinant lettres majuscules, minuscules, chiffres et symboles).
- Activer la double-authentification (l'accès aux données est sécurisé par une double vérification de l'identité) dès que possible.
- Ne jamais partager son mot de passe, même avec un collègue, un ami ou un parent.
- Changer immédiatement en cas de doute (mail suspect, connexion anormale, appareil perdu). Informer le service informatique de la préfecture.
- Ne pas noter les mots de passe sur un papier ou en clair sur un fichier.
- Utiliser un gestionnaire de mots de passe fourni ou validé par le service informatique.

LES SAUVEGARDES DE DONNÉES : préservent le fonctionnement du service et atténuent les effets d'un incident cyber



- Effectuer des sauvegardes de données régulières, dont la fréquence et les modalités varient en fonction du niveau de criticité des données. Se référer aux recommandations du service informatique.
- Réaliser des sauvegardes locales (supports validés et fournis par les services informatiques).
- Réaliser des sauvegardes en ligne (*cloud* sécurisé mis en place par les services de l'Etat ou serveur interne de la préfecture).

LES MISES À JOUR : protègent les données, préviennent les cyberattaques

- Se conformer aux consignes de périodicité du service informatique.
- Activer les mises à jour automatiques si possible.
- Installer les mises à jour dès qu'elles sont disponibles.
- Redémarrer son poste après chaque mise à jour pour son optimisation.



ADOPTONS LES BONS GESTES NUMÉRIQUES

Nous sommes tous et toutes un maillon essentiel : la cybersécurité repose sur la vigilance de chacun

J'adopte une démarche prudente face aux tentatives de cyberattaques

LES COMMUNICATIONS SUSPECTES : risque de vol des données ou d'infection des systèmes informatiques

- Ne jamais cliquer sur des liens non-sécurisés, ouvrir ou transférer des pièces jointes douteuses (courriel ou SMS).
- Vérifier l'expéditeur, le contacter par un autre biais et signaler immédiatement toute communication suspecte.
- Ne pas avoir une confiance spontanée dans le nom de l'expéditeur du message. Au moindre doute, contacter l'expéditeur par un autre biais.



LES INTRUSIONS PHYSIQUES : toute intrusion physique non signalée peut compromettre les postes informatiques et les données



- Verrouiller son poste en s'absentant, même pour quelques minutes.
- Protéger les supports physiques contenant des données sensibles (clés USB, disques durs, documents imprimés), en les mettant dans une armoire ou un tiroir sécurisé.
- N'utiliser que des supports sécurisés pour transférer ou stocker des données (clé USB et/ou disque dur approuvé par le service informatique).
- Ne pas utiliser de supports personnels ou inconnus susceptibles de contenir des virus ou faciliter des fuites de données.
- Signaler immédiatement tout vol ou perte de matériel dès sa constatation ;

L'INTELLIGENCE ARTIFICIELLE (IA) : Une utilisation imprudente peut ouvrir la porte aux cyberattaques



- Ne jamais partager d'informations sensibles ou confidentielles avec des outils IA non sécurisés.
- Se conformer aux règles internes et aux obligations légales ; protéger les données traitées en adoptant des mesures de cybersécurité qui permettent de garantir leur confidentialité et leur intégrité. (RGPD - règlement général sur la protection des données ; CNIL - Commission nationale de l'informatique et des libertés).

ADOPTONS LES BONS GESTES NUMÉRIQUES

Nous sommes tous et toutes un maillon essentiel : la cybersécurité repose sur la vigilance de chacun

Je reste un acteur de la cybersécurité même en dehors de mon lieu de travail

LE TÉLÉTRAVAIL : accroît les risques cyber lorsqu'il est pratiqué sans vigilance ni bonnes pratiques de sécurité



- Maintenir les outils de travail à jour (système, navigateur et antivirus).
- Wi-Fi domestique sécurisé (mot de passe fort : Il doit comporter au minimum 14 caractères mélangeant les majuscules, les minuscules, des chiffres et des caractères spéciaux).
- Aucun télétravail sur un Wi-Fi public ou non-sécurisé.
- Ne pas utiliser un partage de connexion non autorisé ou avec son téléphone personnel, ou le téléphone d'un tiers.
- Ne pas exporter de documents professionnels sur mon courriel personnel et supports de stockages privés, et inversement.
- Vérifier que l'écran est à l'abri des regards (famille, visiteurs, etc.).
- Aucun échange entre l'usage personnel et professionnel du matériel.

EN DÉPLACEMENT : le risque cyber augmente car le matériel et les connexions sont plus exposés



- Protéger le Wi-Fi : éviter les réseaux publics ; privilégier le partage de connexion sécurisé.
- Ne jamais laisser son équipement sans surveillance (train, hôtel, salle d'attente, etc.).
- Verrouiller l'écran dès qu'on s'en éloigne.
- Ne pas parler de sujets sensibles en public (train, cafés, etc.).
- Ne pas utiliser de clé USB inconnue ou personnelle.
- Signaler immédiatement tout vol ou perte de matériel dès sa constatation ;