L'ESSENTIEL DU MOIS DE LA CYBERSÉCURITÉ

LA CHARTE INFORMATIQUE

SÉCURITÉ ET RGPD

La charte engage les collaborateurs dans l'utilisation du SI à des fins professionnelles, d'une manière déontologique, dans le respect du RGPD, de la vie privée et des bonnes pratiques de sécurité.

PROPRIÉTÉ INTELLECTUELLE

- L'installation, l'utilisation ou la copie de logiciels non acquis par l'employeur est interdite.
- Utilisez des logiciels, bases de données, images, textes, sons, vidéos, après avoir vérifié qu'ils sont libres de droits, sous licence libre ou avec consentement de son auteur.

LES BONNES PRATIQUES

VIGILANCE

Verrouillez votre session quand vous quittez votre poste de travail

RACCOURCI CLAVIER

PRINCIPE DE PRUDENCE

Assurez-vous d'utiliser les ressources informatiques d'une manière raisonnable en faisant preuve de prudence (navigation sur internet, ouverture de mails suspects, téléchargement de pièce jointe...)

UN PROBLÈME ?

Signalez de manière pro-active toute anomalie constatée ou tout problème compromettant la sécurité (clic sur un lien ou pièce jointe suspects, partage non sécurisé de mot de passe...)

LE TÉLÉTRAVAIL

UTILISEZ LE VPN

C'est un outil qui crée un tunnel sécurisé entre l'agence et le poste informatique et qui sécurise de bout en bout la connexion

USAGES PRO ET PERSO

- Segmentez vos usages et votre matériel.
- Ne laissez pas votre ordinateur et/ou téléphone pro ouvert sans surveillance, même à la maison (invités, enfants, etc.)

SOURIEZ, VOUS ÊTES FILMÉS !

Une journalisation (surveillance des activités sur le réseau et le web) est mise en place à des fins de prévention et d'investigation en cas de problème et de non-respect de la charte.

AGATE
AGENCE ALPINE DES TERRITOIRES

L'ESSENTIEL DU MOIS DE LA CYBERSÉCURITÉ

ÉVITER DE TOMBER DANS LE PIÈGE DU HAMEÇONNAGE

LE HAMMEÇONNAGE KESAKO ?

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (phishing en anglais) !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel
- Au moindre doute, contactez directement l'organisme concerné pour confirmer

COMMENT LE REPÉRER ?

7 POINTS DE CONTRÔLE QUI DOIVENT VOUS ALERTER :

- Une notification de la messagerie ou de l'antivirus
- Un nom d'émetteur inhabituel
- Une adresse d'expédition fantaisiste
- Un objet de message succinct ou alarmiste
- Un message aguicheur ou inquiétant
- Des fautes de français surprenantes
- Une incitation à ouvrir un lien ou une pièce-jointe

ATTENTION AUX LOGOS ! UN LOGO OFFICIEL NE GARANTIT PAS QUE LE MAIL L'EST !

AGATE
AGENCE ALPINE DES TERRITOIRES

L'ESSENTIEL DU MOIS DE LA CYBERSÉCURITÉ

CHOISIR CORRECTEMENT SES MOTS DE PASSE

UN MOT DE PASSE

★ **PROTÈGE L'ACCÈS AUX DONNÉES** de votre boite mail mais aussi du serveur de fichiers de vos collègues, de nos collectivités adhérentes, des services en lignes utilités (paye, marché public...)

LES BONNES PRATIQUES

★ CRÉER UN BON MOT DE PASSE

Suffisamment long et complexe

LA LONGUEUR : 12 caractères minimum

LES SYMBOLES rendent votre mot de passe solide ! N'hésitez pas à remplacer les lettres par des symboles.

LA CONCATÉNATION :
Souvent utilisée par **la phrase de passe**
ex : J'aimefaire2lalugeenS@voie73!

★ SÉPARER LES USAGES

Différents mots de passe sur chaque site et usage, ne pas utiliser vos mots de passe personnels pour le professionnel.

★ UTILISER UN GESTIONNAIRE DE MOTS DE PASSE (à venir)

Fiable et sécurisé, il stocke vos mots de passe, peut les générer et peut vous connecter

ET SI ON TESTAIT VOS MOTS DE PASSE ?

HTTPS://WWW.SECURITY.ORG/HOW-SECURE-IS-MY-PASSWORD/

★ UN MOT DE PASSE C'EST COMME UNE BROSSE À DENTS

On ne la laisse pas n'importe où.... Comme par exemple :

- ★ Les écrire sur un post it
- ★ Les stocker dans un fichier excel
- ★ Les enregistrer sur votre smartphone
- ★ Les garder dans un carnet
- ★ Les partager
- ★ Les laisser dans des fichiers textes sur le réseau partage

★ NE COMMUNIQUEZ JAMAIS VOTRE MOT DE PASSE À UN TIERS

Quand il n'y a pas le choix :

- ★ **On ne partage PAS** par email
- ★ On utilise un **moyen chiffré de partage** (une messagerie type Signal ou une plateforme type PrivateBin par exemple)
- ★ On **SUPPRIME** après le partage

AGATE
AGENCE ALPINE DES TERRITOIRES