A purple and white rounded shapes

Description automatically generatedA purple lock with a keyhole

Description automatically generated**SENSIBILISATION SÉCURITÉ INFORMATIQUE**

Cette brochure a pour but de vous familiariser avec les principaux dangers liés à l’informatique et de vous donner des moyens de protection envers ceux-ci.

Les conseils que vous trouverez dans cette brochure sont conçus pour vous accompagner au quotidien dans la sécurisation de votre univers digital.

**Thèmes abordés :**

* Protection physique de votre matériel
* Utilisation de supports amovibles
* Utilisation de la Webcam, des assistants vocaux et des objets connectés
* Mise à jour des logiciels
* Stratégie de sauvegarde régulières
* Création de mots de passe et sauvegarde
* Les bonnes pratiques

A person typing on a computer

Description automatically generated

A purple and white rounded shapes

Description automatically generatedPROTECTION PHYSIQUE DE VOTRE MAT ÉRIEL

Protéger votre équipement informatique représente de réelles économies mais aussi et surtout la protection de vos données.

Un accident, un vol ou un oubli est vite arrivé et les conséquences peuvent résulter en :

* Une perte des données stockées sur l’appareil.
* Un risque de vol de votre identité et dans certains cas, la divulgation de données sensibles.
* Possible atteinte à votre réputaion et/ou à celle de votre entreprise

Pour éviter au mieux ces situations vous pouvez :

* Installer des filtres de confidentialité sur vos écrans pour limiter l'angle de vue et empêcher les regards indiscrets.
* Verrouiller votre écran lorsqu'il n'est pas utilisé.
* Utilisez les housses de protection pour vos appareils l’ors de transports afin de les protéger des poussières et des chocs.

A purple and white rounded shapes

Description automatically generated

A purple and white rounded shapes

Description automatically generatedUTILISATION DE SUPPORT AMOVIBLES

Les clés USB, Disque dur externe, cartes mémoires et autres supports amovibles contiennet des données qui peuvent s’avérée être sensibles ou confiidentielles.

Risques liés à l’utilisation de supports amovibles:

* Les supports amovibles peuvent devenir des vecteurs de malwares ou de virus.
* Un support perdu ou volé peut exposer des informations sensibles.
* Les supports amovibles peuvent être facilement perdus ou endommagés, entraînant la perte de données importantes.

Pour éviter au mieux ces situations :

* Dans les paramètres de votre ordinateur désactiver l'exécution automatique des programmes depuis les supports amovibles.
* Avant d'utiliser un support amovible, effectuez toujours une analyse antivirus complète.
* A purple and white rounded shapes

  Description automatically generatedLisez attentivement la politique de sécurité de l’entreprise et suivez-la à la lettre.

A purple and white rounded shapes

Description automatically generatedUTILISATION DE LA WEBCAM, DES ASSISTANTS VOCAUX ET DES OBJETS CONNECTÉS

Les webcams, assistants vocaux et autres objets connectés sont utiles mais sont à utiliser avec précaution.

Ce qu’il pourrait arriver :

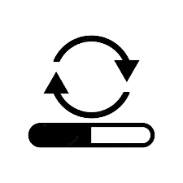
* Les webcams et microphones peuvent être activés à distance par des logiciels malveillants
* Les assistants vocaux et objets connectés peuvent enregistrer des conversations sensibles

Pour éviter au mieux ces situations nous vous devez :

* Si vous n’avez pas du tout l’utilité de votre webcam, demandez au secteur informatique sa désactivation depuis les paramètres de base du système (dans le BIOS)
* N'utilisez pas d'appareils connectés durant les réunions ou discussions confidentielles.
* A purple and white rounded shapes

  Description automatically generatedSi vous suspectez la présence d'un logiciel espion, réinstallez le système d'exploitation pour assurer la sécurité de votre appareil.



A purple and white rounded shapes

Description automatically generatedMISE À JOUR DES LOGICIELS

Les mises à jour des logiciels corrigent les failles de sécurité, améliorent les performances et ajoutent de nouvelles fonctionnalités. Ignorer les mises à jour peut exposer vos appareils à des risques tels que :

* Perte des données stockées sur l’appareil.
* Risque considérable de vol d’identité et dans certains cas, divulgation des données sensibles
* Possible atteinte à votre réputaion ou à celle de votre entreprise selon l’utilisation faite de l’appareil.

Pour éviter au mieux ces situations nous attirons votre attention sur les points suivants :

* Ne pas sur-réagir aux alertes suspectes de mise à jour, cela peut conduire à des escroqueries. Prenez le temps de vérifier avant d'agir.
* Activez les mises à jour automatiques pour les logiciels anti-virus ou demander au secteur informatique de s’en charger.
* A purple and white rounded shapes

  Description automatically generatedEffectuez toutes les mises à jour de votre système d’exploitation sans délais.

STRATÉGIES DE SAUVEGARDES

A purple and white rounded shapes

Description automatically generatedPerdre des données peut signifier perdre des mois de travail, des informations client essentielles ou même exposer l'entreprise à des risques légaux.

C'est pourquoi sauvegarder régulièrement est d’une extreme importance.

Voici quelques un des danger auquels vos données sont exposées :

* Les virus informatiques peuvent corrompre ou détruire nos données.
* Les erreurs humaines comme l’effacement involontaire de données importantes.

Pour éviter au mieux ces situations nous vous conseillons :

* Utilisez un emplacement physique sécurisé (comme un coffre anti-feu) **et** un emplacement sur le cloud de l’entreprise pour effectuer vos sauvegardes.
* Activer le système de sauvegardes automatiques fourni et prévu par l’entreprise.
* A purple and white rounded shapes

  Description automatically generatedVérifiez régulièrement si les données que vous avez sauvegardées peuvent être restaurée

**N'oubliez pas, une bonne sauvegarde aujourd'hui peut sauver votre travail demain !**

A purple and white rounded shapes

Description automatically generatedCRÉATION DE MOTS DE PASSES ET SAUVEGARDES

La création de mots de passe sécurisés et la gestion efficace des sauvegardes sont essentielles pour protéger nos informations contre les accès non autorisés et les pertes de données.

Des mots de passe faibles ou des sauvegardes mal gérées peuvent ouvrir la porte à des risques majeurs tel que :

* Si votre mot de passe est facile à deviner, quelqu'un pourrait se faire passer pour vous et accéder à des informations confidentielles.
* Des mots de passe faibles sont vulnérables aux attaques où des hackers essaient de nombreuses combinaisons pour accéder à vos comptes.

Pour éviter au mieux ces situations nous vous conseillons :

* Ne choisissez pas des mots de passe liés à vous-même ou des mots de passe par défaut.
* A purple and white rounded shapes

  Description automatically generatedUtilisez des outils comme « Sticky Password » ou « SecureSafe » pour gérer vos mots de passes de façon sécurisée.
* Éviter de stocker vos mots de passes à des endroit physiques non-sécurisé.



A purple and white rounded shapes

Description automatically generatedLES BONNES PRATIQUES

Vous trouverez, ci-dessous, une série de bonnes pratiques concernant l’utilisation de vos sessions, votre navigation sur internet, vos messageries, des réseaux sociaux. Vous trouverez aussi des habitudes que nous vous conseillons vivement d’adopter en cas de suspicions d’accès frauduleux, de télétravail, de déplacements et de voyages.

**SESSION**

* Utilisez + L pour verrouiller votre PC avant de vous éloigner.
* Identifiez-vous à chaque ouverture de votre session à l’aide d’un mot de passe robuste et mis à jour régulièrement.
* Configurez votre PC pour se verrouiller après 5 minutes d'inactivité.

**NAVIGUATION INTERNET**

A purple and white rounded shapes

Description automatically generated

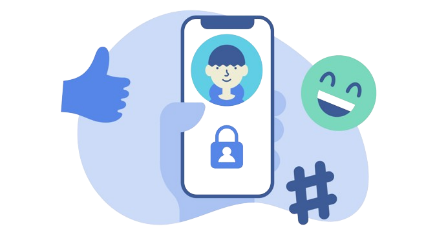
**MESSAGERIE**

* Repérez les e-mails frauduleux (adresses étranges, fautes, liens douteux).
* Informez-vous sur les arnaques communes sur https://www.votrepolice.ch.
* Ne répondez pas aux e-mails suspects.
* Signalez les arnaques à ncsc.admin.ch.

A purple and white rounded shapes

Description automatically generatedLES BONNES PRATIQUES

**RÉSAUX SOCIAUX**

* Évitez de partager ou de réagir à des contenus haineux ou à la désinformation.
* Protégez votre e-réputation ; ne tolérez pas le cyberharcèlement.

**SUSPICION D’ACCÈS FRAUDULEUX**

En cas de suspicion d'accès frauduleux :

* Signalez immédiatement : Utilisez les canaux officiels (email ou téléphone).
* Délai d'annonce court : Rapportez rapidement tout incident suspect
* Contactez la personne référente : Pour évaluer les risques et orienter les actions.
* Fournissez des informations claires : Incluez détails sur la perte, les preuves, etc.
* Informez les autorités compétentes : Comme la police ou les partenaires si

nécessaire.

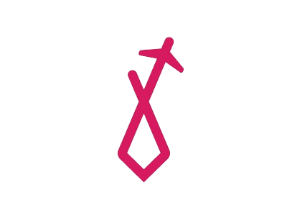
A purple and white rounded shapes

Description automatically generatedLES BONNES PRATIQUES

**TÉLÉTRAVAIL**

* Assurez un environnement physique et numérique sécurisé.
* Maintenez la confidentialité : Faites attention à ne pas divulguer d'informations sensibles en parlant trop fort l’ors d’une réunion par exemple.
* Créez un environnement de travail concentré et sans distractions.

**VOYAGES**

* Verrouillez toujours vos appareils (portables, tablettes) lorsqu'ils ne sont pas utilisés. Utilisez des mots de passe forts ou une authentification biométrique.
* Connexions Sécurisées : Évitez les réseaux Wi-Fi publics non sécurisés. Utilisez un VPN (réseau privé virtuel) pour une connexion sécurisée.
* Gardez toujours vos appareils avec vous ou dans un lieu sûr. Ne laissez pas vos appareils sans surveillance dans des lieux publics.

A purple and white rounded shapes

Description automatically generated

* Personnalisé votre appareil afin de réduire les chances de vol par substitution.
* Pour stockés vos données utiliser le cloud de l’entreprise et jamais de clé USB ou autres support amovibles.
* Soyez vigilant lors de la saisie de mots de passe pour éviter que quelqu'un regarde par-dessus votre épaule.
* Assurez-vous que tous vos appareils sont sauvegardés avant de partir en cas de perte ou de vol et faite contrôler votre matériel par un professionnel au retour à l’entreprise pour ne pas contaminer le système en cas d’infection de votre matériel.

A purple and white rounded shapes

Description automatically generated

A purple and white rounded shapes

Description automatically generated

**A blue and white eye with lines in the center

Description automatically generated**SOYEZ VIGILANT

Chaque clic responsable, chaque mot de passe sécurisé, et chaque mesure de précaution que vous prenez aujourd'hui contribuent à notre sécurité à long terme dans le monde numérique, préservant ainsi la stabilité et la confiance au sein de l’entreprise et pour chacun.

A cartoon of a person looking at a computer screen

Description automatically generated

A purple and white rounded shapes

Description automatically generated

**[ EPSIC**

**Ecole professionnelle**

**Avenue de Genève 63**

**1002 Lausanne**

**🕿 + 41 21 316 58 58**