ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

CYBERRESPONSABLE AUJOURD'HUI, EN SÉCURITÉ DEMAIN

Neuchâtel, canton vibrant et avant-gardiste, est un véritable pôle d'innovation. Mais cette attractivité rend l'environnement neuchâtelois particulièrement intéressant pour les cybermenaces. Cependant, l'administration cantonale a choisi de ne pas se laisser submerger par la crainte, et d'agir face à ces nouveaux défis.

Tout le monde peut faire un geste, même petit, afin de renforcer sa cybersécurité. Animé par cet élan, le service informatique de l'entité neuchâteloise a élaboré une série de conseils et de directives pratiques. Ces recommandations sont conçues pour assurer une navigation en toute sécurité dans ce monde digital, tout en assurant la protection optimale des données personnelles.

Ensemble, résistons aux cyberattaques et protégeons ce canton.

L'ère digitale offre une myriade d'opportunités incroyables. Pour en profiter, adoptons des mesures de sécurité adéquates et utilisons la technologie de manière responsable et sûre.

Ensemble, bâtissons un Neuchâtel digital, sécurisé et prospère !

N **NAVIGATION WEB**
Naviguez avec sagesse

E **ÉDUCATION**
La cybercitoyenneté s'apprend

U **UTILISATION**
Un clic avisé, un monde sécurisé

C **CONFIDENTIALITÉ**
Restez discret·ète

H **HAMEÇONNAGE**
Ne vous laissez pas manipuler

A **AUTHENTIFICATION**
La clé de votre sérénité

T **TECHNOLOGIE**
Sauvegarde et mise à jour, le duo gagnant

E **ÉTHIQUE**
Le cœur d'une digitalisation responsable

L **LÉGISLATION**
Soyez des cybercitoyennes et cybercitoyens

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

N E U C H A T E L

NAVIGATION WEB
Naviguez avec sagesse

Naomi, en navigant sur Internet depuis son ordinateur, a cliqué sur un lien malveillant. Cela a automatiquement déclenché le téléchargement d'un logiciel inconnu. Un individu malveillant a ainsi pu se connecter et accéder à toutes les informations sur l'ordinateur de Naomi.

Pour éviter une situation similaire à celle de Naomi, voici quelques précautions à prendre :

- **Naviguer prudemment en évitant les sites suspects**
  Soyez vigilant·e sur Internet, évitez les liens et sites web sans le cadenas « HTTPS », en particulier s'ils proviennent de sources inconnues ou suspectes.
- **Prévenir les infections avec un antivirus**
  Afin de détecter et bloquer les menaces potentielles. Les dernières versions de Windows ont un antivirus intégré.
- **Installer les mises à jour pour se protéger des pirates**
  Afin de réduire les failles de sécurité des logiciels et systèmes d'exploitation (Windows, MacOS, iOS, Android, etc.).
- **Rester informé et partager ses connaissances**
  Améliorez votre connaissance des menaces en ligne et des bonnes pratiques, consultez par exemple ibarry.ch, administré par la Swiss Internet Security Alliance (SISA). Partagez ces notions avec vos proches pour les aider à naviguer en toute sécurité sur Internet.

NE SOYEZ PAS UNE PROIE FACILE !
RESTEZ ALERTE, ÉVITEZ LES SITES SUSPECTS ET MAINTENEZ VOS APPAREILS À JOUR !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

ÉDUCATION
La cybercitoyenneté s'apprend

Émilie a reçu l'e-mail d'un inconnu et, poussée par la curiosité, elle a ouvert la pièce jointe, un document Word classique. Ce faisant, elle a déclenché un rançongiciel caché qui a verrouillé tous ses documents. L'expéditeur de l'e-mail lui a exigé une rançon pour débloquer l'accès aux fichiers. Émilie, n'ayant pas de sauvegarde de ses données, les a perdues. Cette expérience lui a montré combien la cybersécurité est cruciale.

Voici quelques mesures pour éviter une situation similaire à celle d'Émilie :

- **Rester informé·e et partager ses connaissances**
  Améliorez votre connaissance des menaces en ligne et des bonnes pratiques, consultez par exemple ibarry.ch, administré par la Swiss Internet Security Alliance (SISA). Partagez ces notions avec vos proches pour les aider à naviguer en toute sécurité sur Internet.
- **Ne pas mordre à l'hameçon**
  Apprenez à repérer les e-mails malveillants en vérifiant l'adresse de l'expéditeur, l'orthographe, la grammaire et les liens avant de cliquer ou d'ouvrir des pièces jointes, surtout si ces e-mails proviennent d'expéditeurs inconnus ou si le contenu semble suspect.
- **Sauvegarder ses données avant qu'il ne soit trop tard**
  Utilisez un périphérique de stockage externe ou un service de stockage en ligne pour récupérer vos données en cas d'incident ou de panne.
- **Prévenir les infections avec un antivirus**
  Afin de détecter et bloquer les menaces potentielles. Les dernières versions de Windows ont un antivirus intégré.

LA CYBERSÉCURITÉ N'EST PAS RÉSERVÉE AUX SPÉCIALISTES ! NE DEVENEZ PAS UNE VICTIME, PRENEZ LES RÊNES DE VOTRE SÉCURITÉ !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

UTILISATION
Un clic avisé, un monde sécurisé

Confronté à un ordinateur qui fonctionnait lentement, Ulysse a téléchargé un logiciel gratuit d'une source inconnue promettant de résoudre son problème, sans considérer les risques potentiels. Malheureusement, le logiciel a corrompu son système Windows qui s'est éteint et ne pouvait plus s'allumer. Cet incident l'a encouragé à être plus prudent et à ne télécharger des logiciels que depuis des sources officielles et fiables.

Voici quelques mesures pour éviter une situation similaire à celle d'Ulysse :

- **Télécharger les logiciels uniquement depuis une source fiable**
  Évitez de télécharger des logiciels gratuits à partir d'une source inconnue, illégale ou non vérifiée, préférez toujours les sites officiels et fiables.
- **Prévenir les infections avec un antivirus**
  Afin de détecter et bloquer les menaces potentielles. Les dernières versions de Windows ont un antivirus intégré.
- **Sauvegarder ses données avant qu'il ne soit trop tard**
  Utilisez un périphérique de stockage externe ou un service de stockage en ligne pour récupérer vos données en cas d'incident ou de panne.
- **Rester informé·e et partager ses connaissances**
  Améliorez votre connaissance des menaces en ligne et des bonnes pratiques, consultez par exemple ibarry.ch, administré par la Swiss Internet Security Alliance (SISA). Partagez ces notions avec vos proches pour les aider à naviguer en toute sécurité sur Internet.

UNE ERREUR PEUT COÛTER CHER !
ÉVITEZ LES TÉLÉCHARGEMENTS DOUTEUX !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

C

CONFIDENTIALITÉ
Restez discret·ète

Camille a publié des photos personnelles sur les réseaux sociaux, sans vérifier ses paramètres de confidentialité. Elle s'est rendu compte que ses publications étaient publiques lorsqu'elle a reçu des commentaires malsains d'inconnus. Suite à cet incident, elle a appris à protéger sa confidentialité en ligne en faisant attention aux informations qu'elle partage publiquement.

Voici quelques mesures pour éviter une situation similaire à celle de Camille:

- **Protéger sa vie privée des regards indiscrets**
  Évitez de télécharger des logiciels gratuits à partir d'une source inconnue, illégale ou non vérifiée, préférez toujours les sites officiels et fiables.
- **Contrôler les paramètres de confidentialité sur ses réseaux sociaux**
  Prenez quelques minutes pour vérifier les paramètres de confidentialité de vos comptes sur les réseaux sociaux afin de déterminer qui a accès à vos publications et informations personnelles.
- **Dompter les accès et les permissions de ses applications**
  Assurez-vous que les applications que vous utilisez respectent votre confidentialité et ne partagent pas d'informations sans votre consentement. Révoquez l'accès aux applications suspectes ou inutiles.
- **Être rigoureux·se avec ses mots de passe**
  Créez des mots de passe uniques et robustes pour chaque compte en ligne. Préférez la longueur avec un minimum de complexité (par exemple, Mon-Jardin-Secret-998). L'utilisation d'un gestionnaire de mots de passe fiable, tels que KeePass (keepass.info) ou Dashlane (dashlane.com), peut s'avérer très utile pour la gestion de vos identifiants.

**ATTENTION AUX PUBLICATIONS EN LIGNE!
UNE FOIS VOS PROPOS PUBLIÉS, IL EST SOUVENT TROP TARD POUR LES RÉTRACTER!**

NEUCHÂTEL

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

HAMEÇONNAGE
Ne vous laissez pas manipuler

Le jour de son anniversaire, Hugo a mordu à l'hameçon, pensant recevoir un cadeau de sa banque, il a cliqué sur un lien d'un faux e-mail. Malheureusement, le lien menait à une fausse page de connexion où il a entré ses identifiants, qui ont ensuite été volés. Cet incident a entraîné la perte de ses économies et l'a incité à apprendre à identifier les tentatives d'hameçonnage afin d'éviter de futurs désagréments.

Voici quelques mesures pour éviter une situation similaire à celle de Hugo:

- **Ne pas mordre à l'hameçon**
  Apprenez à repérer les e-mails malveillants en vérifiant l'adresse de l'expéditeur, l'orthographe, la grammaire et les liens avant de cliquer ou d'ouvrir des pièces jointes, surtout si ces e-mails proviennent d'expéditeurs inconnus ou si le contenu semble suspect.
- **Signaler l'hameçonnage à reports@antiphishing.ch**
  Lorsque vous identifiez un e-mail malveillant, il est important de le reporter. Transmettez le à reports@antiphishing.ch, administré par le centre national pour la Cybersécurité (NCSC).
- **Ignorer les sollicitations d'informations personnelles ou sensibles**
  Ne répondez pas aux messages demandant des informations personnelles ou des mots de passe.
- **Prévenir les infections avec un antivirus**
  Afin de détecter et bloquer les menaces potentielles. Les dernières versions de Windows ont un antivirus intégré.

NE TOMBEZ PAS DANS LE PIÈGE!
LES PIÈCES JOINTES CONTIENNENT PARFOIS DE MAUVAISES SURPRISES!

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

A

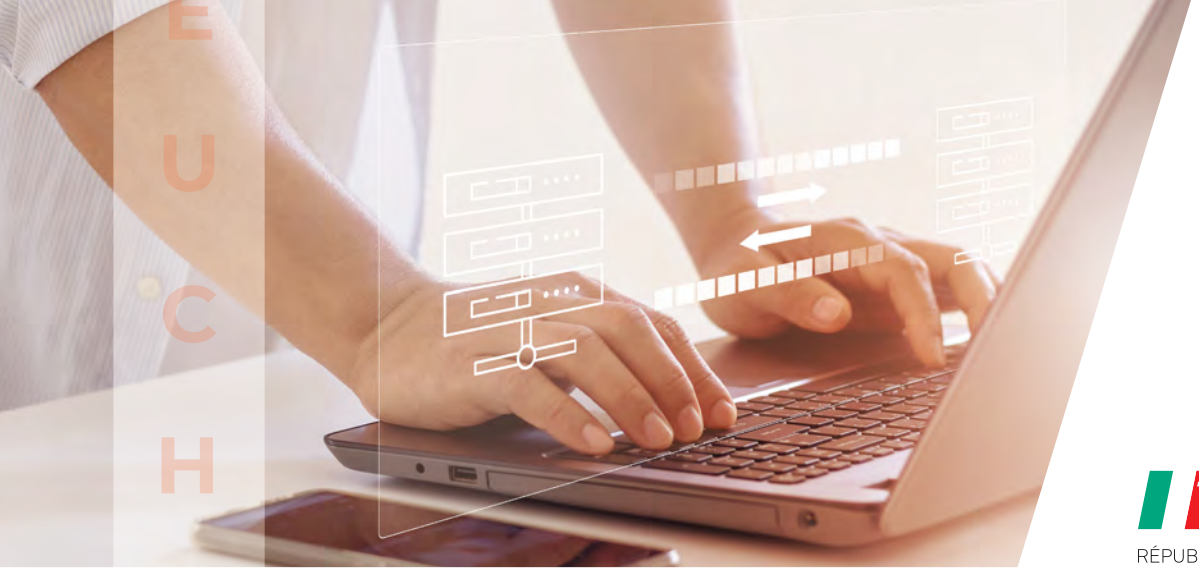
AUTHENTIFICATION
La clé de votre sérénité

Arthur utilisait un mot de passe trop simple, «Arthur123!», pour sa boutique en ligne favorite. Un pirate informatique a réussi à le deviner, mais heureusement, l'authentification multifacteur qu'il avait configurée a empêché l'accès non autorisé à son compte et à ses informations personnelles. Cette expérience a souligné pour Arthur l'importance de renforcer la sécurité avec un facteur supplémentaire, comme l'envoi d'un code sur son téléphone portable, en plus d'un mot de passe fort et unique.

Afin d'éviter le cas d'Arthur et renforcer l'authentification, suivez ces mesures:

- **Booster la sécurité avec l'authentification multifacteur (MFA)**
  Ajoutez une couche de sécurité supplémentaire à vos comptes, c'est facile et faisable en quelques minutes. Même si le mot de passe est connu, le compte est protégé.
- **Différencier les mots de passe privés et professionnels**
  Pour protéger vos informations, créez des mots de passe distincts pour vos comptes privés et professionnels.
- **Restreindre l'accès aux appareils**
  Verrouillez vos appareils, ne partagez pas vos mots de passe et limitez l'accès physique à votre ordinateur ou téléphone aux personnes de confiance.
- **Être rigoureux avec ses mots de passe**
  Créez des mots de passe uniques et robustes pour chaque compte en ligne. Préférez la longueur avec un minimum de complexité (par exemple, Mon-Jardin-Secret-998). L'utilisation d'un gestionnaire de mots de passe fiable, tels que KeePass (keepass.info) ou Dashlane (dashlane.com), peut s'avérer très utile pour la gestion de vos identifiants.

FERMEZ-VOUS LA PORTE EN SORTANT DE CHEZ VOUS? VERROUILLEZ VOS APPAREILS DE LA MÊME MANIÈRE, VOS DONNÉES ONT DE LA VALEUR!



ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

TECHNOLOGIE
Sauvegarde et mise à jour, le duo gagnant

Tom, commerçant, a perdu la totalité de son fichier client suite à une panne d'ordinateur. Il n'avait malheureusement pas effectué de sauvegarde. Cet incident l'a incité à maintenir ses appareils et logiciels à jour et à sauvegarder régulièrement ses données pour une protection optimale.

Voici quelques mesures pour éviter une situation similaire à celle de Tom :

- **Sauvegarder ses données avant qu'il ne soit trop tard**
  Utilisez un périphérique de stockage externe ou un service de stockage en ligne pour récupérer vos données en cas d'incident ou de panne.
- **Installer les mises à jour pour se protéger des pirates**
  Afin de réduire les failles de sécurité des logiciels et systèmes d'exploitation (Windows, MacOS, iOS, Android, etc.).
- **Prévenir les infections avec un antivirus**
  Afin de détecter et bloquer les menaces potentielles. Les dernières versions de Windows ont un antivirus intégré.
- **Restreindre l'accès aux appareils**
  Verrouillez vos appareils, ne partagez pas vos mots de passe et limitez l'accès physique à votre ordinateur ou téléphone aux personnes de confiance.

COMME UN VOYAGE EN VOITURE, ATTACHEZ VOTRE CEINTURE DE SÉCURITÉ ET NE LAISSEZ PAS LES CYBERCRIMINELS VOUS DÉVIER DE VOTRE TRAJET !

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

NEUCHÂTEL

ÉTHIQUE
Le cœur d'une digitalisation responsable

Elsa a relayé une rumeur sur les réseaux sociaux sans vérifier sa véracité, contribuant ainsi à la propagation de fausses informations. Cet acte a été identifié par un groupe de personnes touchées par cette désinformation qui ont porté plainte pour diffamation. Cet incident a amené Elsa à adopter une utilisation éthique et responsable d'Internet, en vérifiant les sources d'information, en respectant la vie privée des autres et en refusant de participer à la diffusion de rumeurs ou à des actes de cyberharcèlement.

Voici quelques mesures pour éviter une situation similaire à celle d'Elsa :

- **Assumer la responsabilité de ses actions en ligne**
  Réfléchissez aux impacts de vos publications, partages ou interactions sur les réseaux sociaux et agissez de manière responsable.
- **Ne pas participer à la désinformation**
  Avant de partager des informations, assurez-vous qu'elles proviennent de sources fiables et crédibles.
- **Respecter la vie privée et le consentement d'autrui**
  Ne partagez pas d'informations personnelles sans leur consentement et respectez leur droit à la confidentialité.
- **Dire non au cyberharcèlement**
  Dénoncez les comportements inappropriés et soyez conscient·e des conséquences de vos actions en ligne.

L'ÉTHIQUE SUR INTERNET EST COMME LA POLITESSE. RESTEZ POLI·E, RESPECTUEUX·SE ET ÉVITEZ LES CONFLITS OU COMPORTEMENTS INAPPROPRIÉS !

C H A I E

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

L

LÉGISLATION
Soyez des cybercitoyennes et cybercitoyens

Louise a découvert que ses photos personnelles publiées sur son réseau social préféré étaient utilisées sans son consentement par une entreprise en ligne pour la promotion d'un produit anti-constipation. Suite à cet incident, elle a cherché à comprendre ses droits et obligations relatifs à la protection des données pour mieux protéger sa vie privée et éviter d'autres problèmes à l'avenir.

Voici quelques mesures pour éviter une situation similaire à celle de Louise:

- **Comprendre les droits à la protection des données (nLPD)**
  Informez-vous sur les lois et régulations en vigueur concernant la protection des données personnelles, telle que la nouvelle loi fédérale sur la protection des données (nLPD) en Suisse.
- **Respecter les droits d'auteur pour éviter des sanctions légales**
  Ne partagez ni ne téléchargez aucun contenu protégé par des droits d'auteur sans autorisation. Le partage de contenu piraté est illégal et peut entraîner des sanctions légales.
- **Signaler les abus en ligne aux autorités**
  Si vous êtes témoin ou victime d'une tentative d'extorsion ou d'une infraction en ligne, signalez-le aux autorités compétentes, comme le réseau social ou la police. Vous contribuez ainsi à la lutte contre la cybercriminalité et aidez à protéger les internautes.
- **Ne pas ignorer les conditions d'utilisation de ses applications**
  Informez-vous sur ce que les propriétaires de ces applications peuvent faire avec vos données. Il est possible que, dans certaines conditions, vos données ne vous appartiennent plus une fois qu'elles sont publiées.

LES LOIS SONT LES GARDIENNES DE NOTRE VIE DIGITALE. ELLES GARANTISSENT QUE VOS DONNÉES PERSONNELLES SOIENT CONSERVÉES EN TOUTE CONFIDENTIALITÉ.