CYBERSÉCURITÉ 360°

PARCE QU'UN CLIC PERSONNEL PEUT COÛTER CHER PROFESSIONNELLEMENT

16 septembre 2026

Présentateurs …

Frédéric Bouthillier

Directeur général, chargé de projet et conseiller senior TI, Frédéric Bouthillier cumule plus de 30 ans d'expérience en technologies et en gestion d'équipes. Formé en informatique au Cégep de Valleyfield, il développe très tôt une passion pour le service à la clientèle et le déploiement de solutions technologiques. Il poursuit ensuite son perfectionnement à travers diverses formations en gestion, en technologies et en cadres de bonnes pratiques (dont ITIL).

Après des passages marquants chez Coba, Groupe Inca et MédiSolution, il rejoint l'équipe de DBG Groupe Conseil dès sa création en 1999 (devenue Trilogie). Depuis, il contribue à bâtir Trilogie ; où il en devient copropriétaire en 2021.

Reconnu pour son pragmatisme, son accessibilité et sa loyauté, Frédéric se distingue par sa connaissance approfondie des technologies, son leadership humain et sa volonté naturelle d'aider.

Présentateurs …

Guy Lépine

Directeur général adjoint chargé de projet et conseiller senior TI, Guy Lépine est diplômé en électronique du Cégep du Vieux Montréal et titulaire d'un AEC en réseautique de l'Institut Teccart. Il a également complété un certificat sur mesure en gestion de projets à l'Université Laval, consolidant une expertise multidisciplinaire à l'intersection des technologies, de la gouvernance et de la gestion organisationnelle.

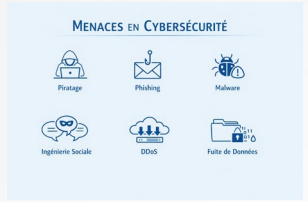
Fort de plus de 25 ans d'expérience en informatique, dont 20 ans dans le milieu municipal, il possède une compréhension fine des environnements institutionnels, des impératifs de conformité et des exigences de reddition de comptes propres au secteur public. Son parcours l'a amené à piloter des projets stratégiques, à moderniser des infrastructures critiques et à structurer des pratiques de sécurité alignées sur les normes reconnues.

En tant que co-propriétaire et dirigeant de Trilogie Groupe Conseil, Guy se spécialise dans la gouvernance de la sécurité de l'information, la gestion des risques, la conformité réglementaire (dont la Loi 25) et la mise en place de cadres opérationnels auditables. Il est reconnu pour sa capacité à transformer des enjeux techniques en orientations claires, structurantes et adaptées aux réalités organisationnelles.

Son approche repose sur la rigueur, la transparence et la pédagogie — trois piliers qui lui permettent d'accompagner efficacement les organisations dans l'amélioration de leur posture cyber, la maturité de leurs processus et la résilience de leurs opérations.

Objectifs spécifiques

Comprendre les principales menaces qui ciblent les municipalités québécoises.

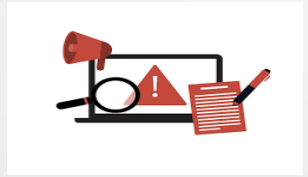


Identifier les risques liés aux comportements numériques personnels

Appliquer les bonnes pratiques d'hygiène numérique au travail et à la maison

Reconnaître les tentatives de fraude et d'ingénierie sociale

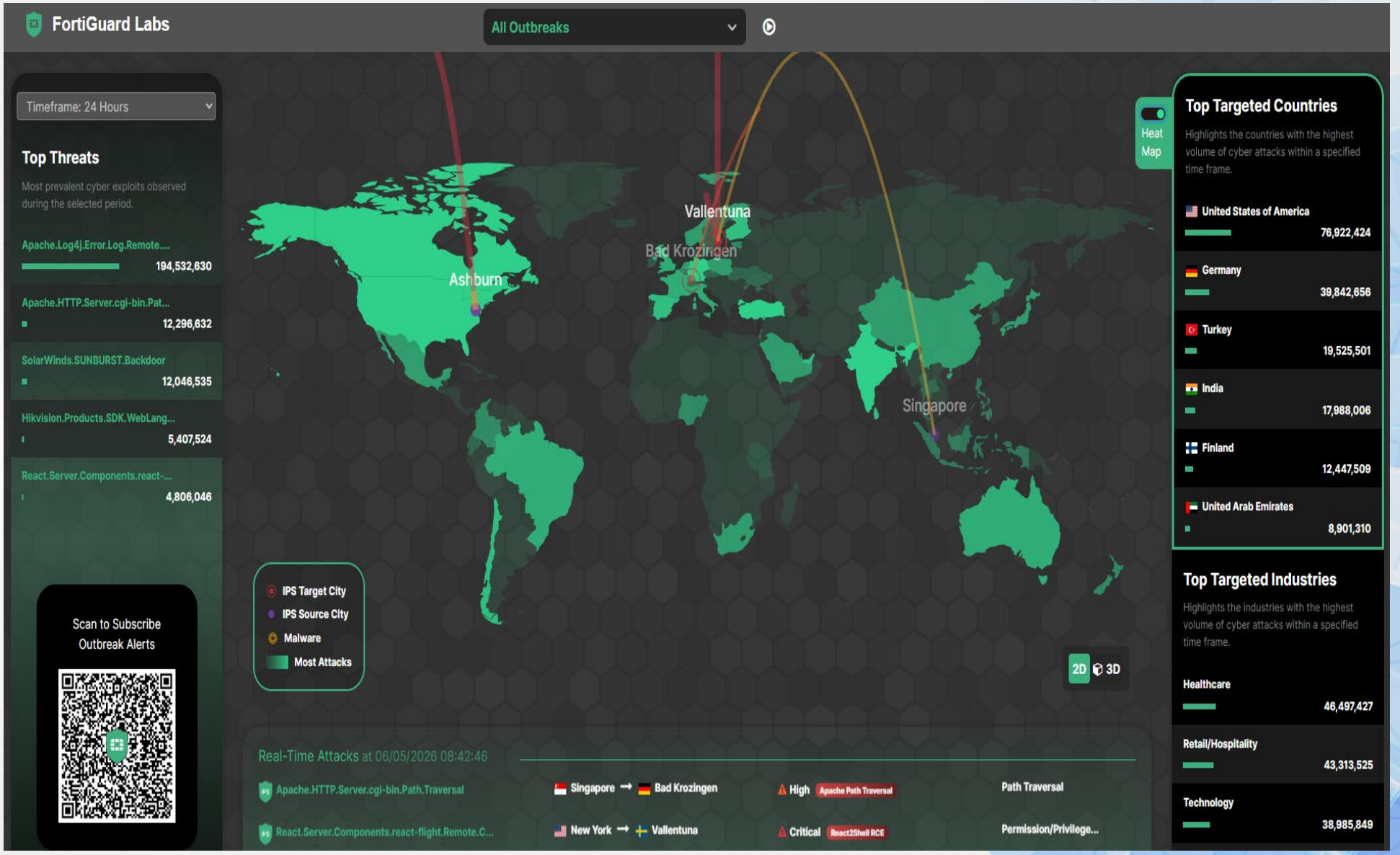
Enjeux relatifs à la Loi 25 …



Réagir efficacement à un incident

Contexte global et municipal

Qu'est-ce qui se passe en temps réel …

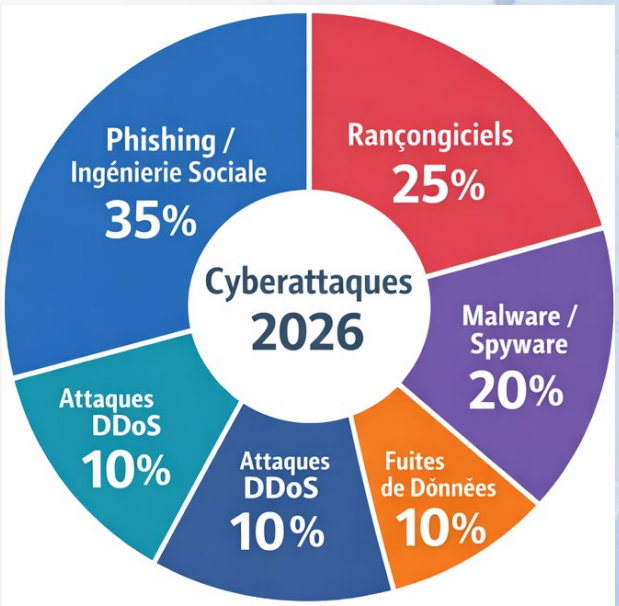


https://www.fortiguard.com/threat-map

Quelques statistiques…

🌎 Cyberattaques mondiales (2026)

Type d'attaque	Part estimée	Source
Phishing / Ingénierie sociale	35 %	DataGlobeHub 2026
Rançongiciels (Ransomware)	25 %	Marketing, Ventes & Entrepreneuriat 2026
Malware / Spyware	20 %	IBM DBIR 2026
Attaques DDoS	10 %	Statista 2026
Fuites de données / Exfiltration	10 %	Forbes Advisor 2026



💡 **En 2026, on estime 600 millions de cyberattaques par jour dans le monde, soit une hausse de 50 % par rapport à 2025. Le coût global de la cybercriminalité atteint 10 500 milliards $ US.**

Quelques statistiques…

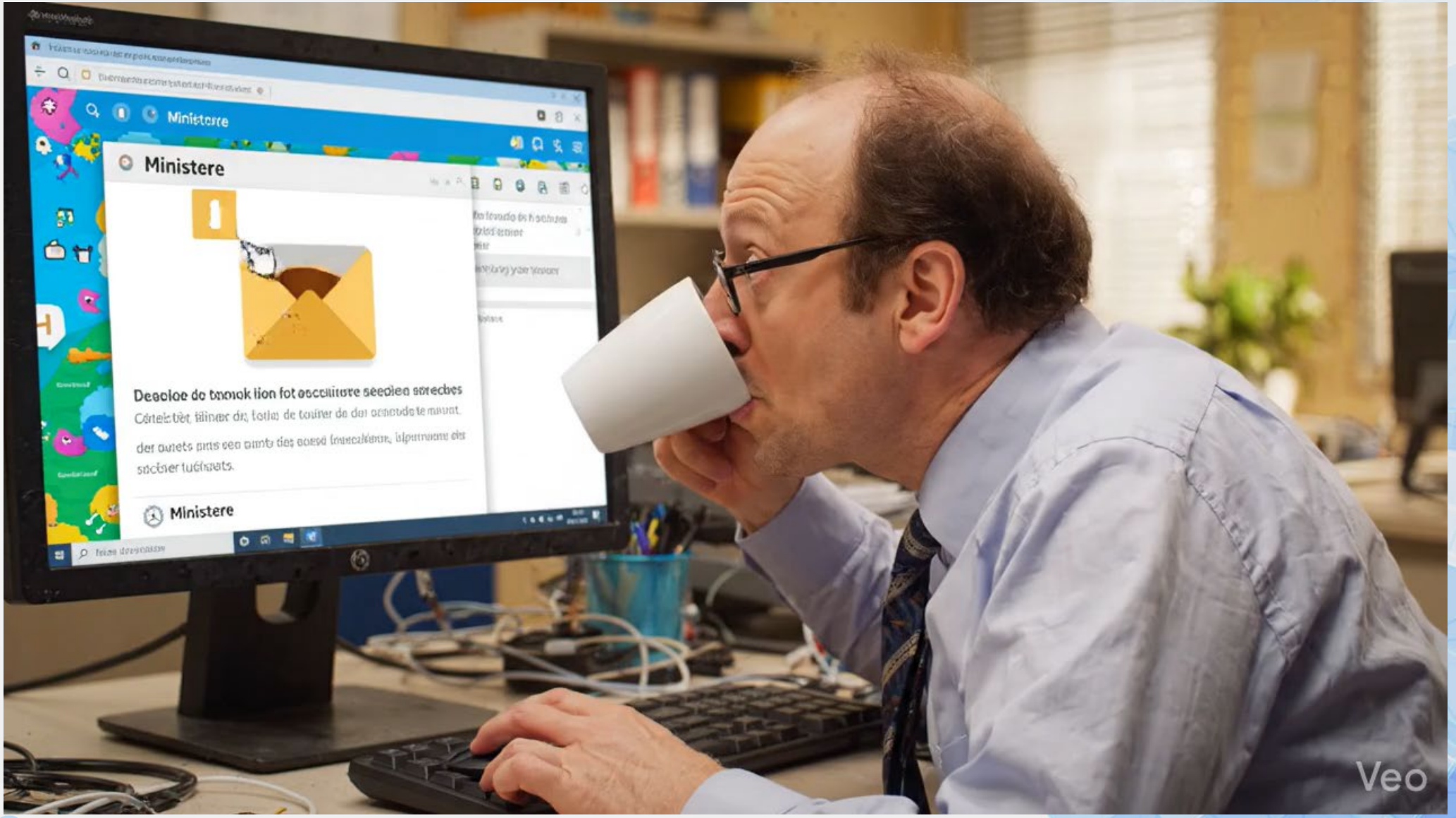
CA Cyberattaques au Canada (2025-2026)

Type d'attaque	Part estimée	Source
Rançongiciels (Ransomware)	**40 %**	Centre canadien pour la cybersécurité 2025-2026
Phishing ciblé (emails frauduleux)	**25 %**	Canada.ca – Évaluation 2025-2026
Intrusions réseau / espionnage étatique	**15 %**	CST Canada 2026
Fuites de données / erreurs humaines	**10 %**	Centre canadien pour la cybersécurité
Attaques DDoS / sabotage	**10 %**	Canada.ca – Évaluation 2025-2026

💡 **Le Centre canadien pour la cybersécurité confirme que les rançongiciels demeurent la menace principale pour les infrastructures essentielles. Les PME représentent plus de 60 % des victimes d'attaques au Canada.**

Pourquoi les municipalités …

Ce qu'on ne voudrait pas …



Pourquoi les municipalités ou MRC …

Les **municipalités** sont des cibles privilégiées pour les cyberattaques parce qu'elles gèrent une quantité importante de données sensibles. Elles disposent souvent de ressources informatiques limitées, ce qui réduit leur capacité à se protéger efficacement contre les menaces.

Ces organisations stockent des renseignements personnels (citoyens, employés, finances locales) et assurent des **services publics essentiels** — tout arrêt de leurs systèmes peut paralyser la délivrance de permis, la facturation, ou la gestion des infrastructures.

Les cybercriminels exploitent cette vulnérabilité pour :

- **exiger des rançons** via des rançongiciels, sachant que les municipalités doivent rétablir leurs services rapidement ;
- **voler ou revendre des données** à forte valeur (identités, coordonnées bancaires, dossiers fiscaux) ;
- **perturber la confiance publique** et la continuité des opérations.

Selon la FQM (Fédération québécoise des municipalités), près de **44 % des attaques par rançongiciels** dans le monde visent des administrations publiques locales, avec des interruptions de service pouvant durer jusqu'à **22 jours**

Le Centre canadien pour la cybersécurité a recensé **plus de 100 cas** de cybermenaces contre des municipalités canadiennes depuis 2020!

En résumé :

Les municipalités sont des cibles de choix parce qu'elles combinent **forte dépendance numérique**, **données critiques**, et **moyens de défense souvent insuffisants** ; ce qui en fait un terrain idéal pour les cybercriminels cherchant impact rapide et gains financiers.

Impacts …

Une cyberattaque contre une municipalité peut avoir des conséquences profondes sur trois axes :

💰 Impact financier

Les coûts directs incluent la récupération des systèmes, la restauration des données, et parfois le paiement d'une rançon. À cela s'ajoutent les frais de consultants, de sécurité renforcée et de communication de crise. Selon le Centre canadien pour la cybersécurité, une attaque municipale moyenne peut coûter entre 500 000 $ et 3 millions $, sans compter les pertes économiques liées à l'interruption des services.

⚙️ Impact sur les services

Les attaques paralysent souvent :

- la facturation et la perception des taxes
- la gestion des permis et des demandes citoyennes
- les systèmes de communication interne et d'urgence

Certaines municipalités ont dû suspendre leurs opérations pendant plusieurs semaines, affectant directement les citoyens et la confiance envers l'administration.

🧭 Impact sur la réputation

Une cyberattaque ébranle la crédibilité et la confiance du public ; qui peut durer des années, même après la restauration complète des systèmes.

Les citoyens peuvent percevoir la municipalité comme négligente en matière de sécurité, ce qui nuit à son image et à ses relations avec les partenaires institutionnels.

AGFMQ
Association des gestionnaires financiers municipaux du Québec

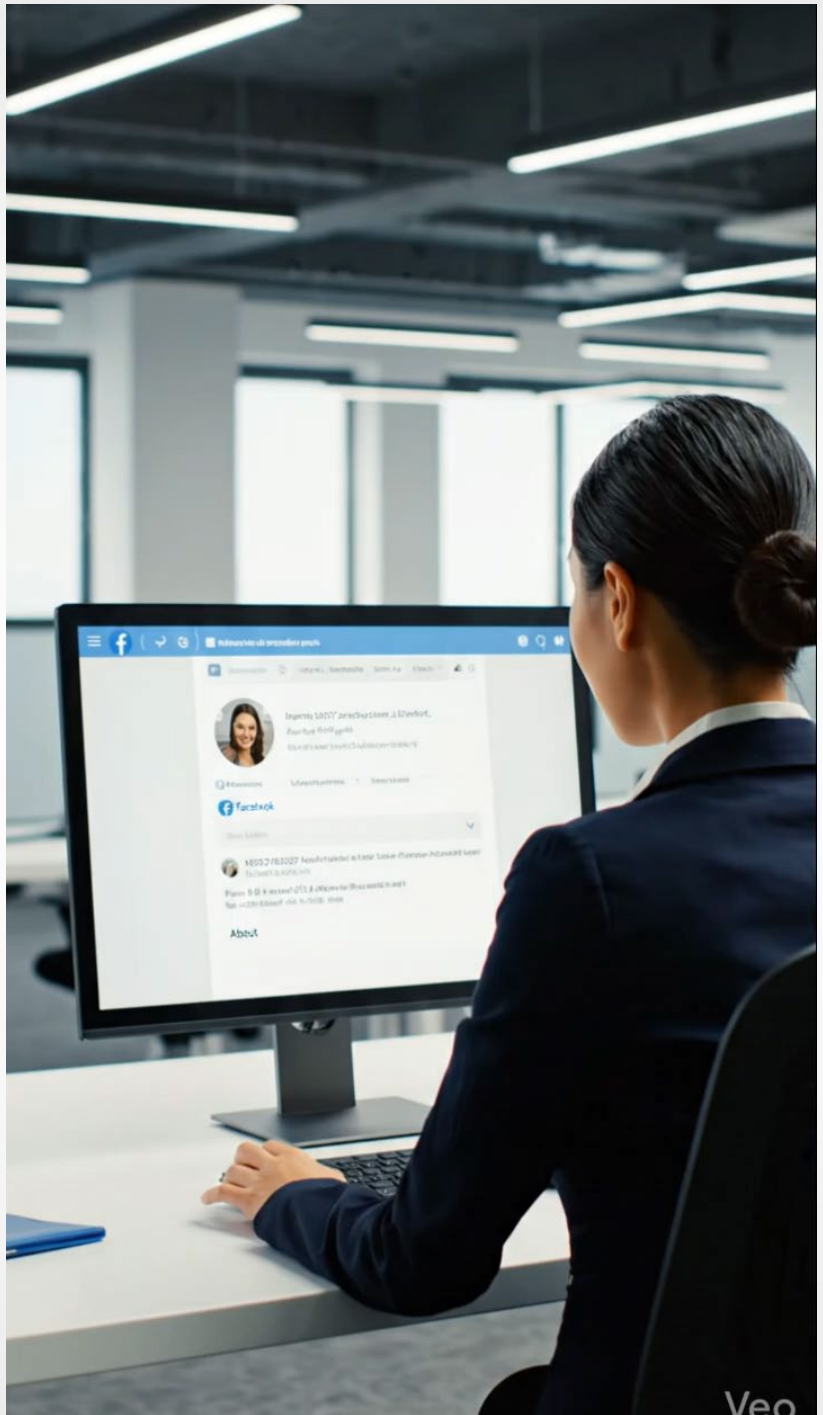
Menaces

Personnelles & Professionnelles

trilogie

AGFMQ

Association des gestionnaires financiers municipaux du Québec



trilogie

AGFMQ
Association des gestionnaires financiers municipaux du Québec

trilogie

Rançongiciel, fraude au changement de coordonnées bancaires

⚠️ Menaces personnelles et professionnelles

Les cybermenaces touchent autant les individus que les organisations.
Sur le plan personnel, les attaques visent à voler des identités, piéger par hameçonnage ou compromettre des comptes pour accéder à des données sensibles ou financières.
Sur le plan professionnel, les cybercriminels utilisent des rançongiciels pour bloquer les systèmes informatiques ou pour effectuer des fraudes avec des changements de coordonnées bancaires afin de détourner des paiements.

Rançongiciel

Un logiciel malveillant chiffre les données et bloque les systèmes municipaux (perception, paie, permis). Les pirates exigent une rançon pour les débloquer.

- ➡️ ***Conséquences :*** **interruption des services, perte de données, coûts élevés.**
- ➡️ ***Prévention :*** **sauvegardes hors ligne, mises à jour régulières, formation et sensibilisation.**

Fraude au changement de coordonnées bancaires

Des fraudeurs se font passer pour un fournisseur et demandent de modifier le compte de paiement. Les fonds sont ensuite détournés.

- ➡️ ***Conséquences :*** **pertes financières, atteinte à la réputation.**
- ➡️ ***Prévention :*** **vérification téléphonique directe, double validation des paiements, vigilance face aux courriels suspects.**

Une seule faille peut exposer à la fois la vie privée et les opérations municipales — d'où l'importance d'une vigilance numérique constante.

Ville de Montmagny… 2021

- **Cyberattaque à Montmagny (référence site Web de Montmagny)**

La Ville de Montmagny a été victime d'une cyberattaque de type rançongiciel dans la nuit du 16 au 17 janvier 2021, entraînant une paralysie complète des systèmes informatiques et téléphoniques. Six jours après l'attaque, le téléphone municipal était seulement en voie de rétablissement, tandis que la majorité des services numériques demeuraient hors service. Les autorités ont indiqué que la restauration complète pourrait prendre plusieurs semaines, voire quelques mois, selon les experts mobilisés.

Au moment de la publication, quelques jours plus tard, la Ville n'avait pas confirmé si une rançon avait été exigée ou payée. Le directeur général mentionnait que tous les scénarios étaient envisagés, incluant le paiement de la rançon advenant que la reconstruction des données s'avérait plus coûteuse.

Montmagny s'ajoutait alors à une liste croissante de municipalités québécoises touchées par des rançongiciels depuis 2019, dont Longueuil, Otterburn Park, Montréal-Ouest, Marieville et Châteauguay.

Montmagny a gagné au loto-crypto !!!

AGFMQ
Association des gestionnaires financiers municipaux du Québec

trilogie

Hygiène numérique professionnelle

AGFMQ
Association des gestionnaires financiers municipaux du Québec

trilogie

Hygiène numérique professionnelle…

🔐 Hygiène numérique professionnelle

L’hygiène numérique professionnelle consiste à appliquer des pratiques essentielles pour protéger les systèmes municipaux et assurer la continuité des services. Elle repose d’abord sur une **gestion rigoureuse des accès** aux systèmes financiers, de taxation et de paie, afin que seules les personnes autorisées puissent consulter ou modifier les informations sensibles.
Gestionnaire de mot de passe de base :
Local sur le poste : Keepass (https://keepass.info/download.html)
Version corporative : Keeper (https://www.keepersecurity.com/fr_FR/)

Elle inclut aussi la **transmission sécurisée des documents**, particulièrement ceux contenant des données citoyennes ou financières, afin d’éviter toute interception ou altération.
LiquidFile (https://www.liquidfiles.com/)
SecureExchange (https://www.secure-exchanges.com/transmission-securisee)
Mailfence (https://mailfence.com/)

Enfin, une bonne hygiène numérique exige des sauvegardes fiables, une continuité des opérations en cas d’incident, ainsi qu’une journalisation complète permettant de retracer les actions et détecter rapidement toute activité suspecte. Ensemble, ces pratiques renforcent la sécurité, la résilience et la confiance envers les services municipaux.

AGFMQ
Association des gestionnaires financiers municipaux du Québec

Hygiène Numérique Personnelle

Séparer Vie Privée & Vie Professionnelle

trilogie

C'est quoi ça l'hygiène numérique ?

Mots de passe, MFA, Wi-Fi maison, appareils personnels

🔐 Hygiène numérique personnelle

L'hygiène numérique consiste à adopter des bonnes pratiques quotidiennes pour protéger ses données et préserver la frontière entre vie privée et vie professionnelle. Elle repose sur quelques réflexes essentiels :

- Mots de passe robustes et authentification multifactorielle (MFA) pour sécuriser les accès.
- Gestionnaire de mot de passe
- Wi-Fi maison protégée par un mot de passe fort et un chiffrement à jour
- Appareils personnels régulièrement mis à jour et protégés contre les logiciels malveillants
- VPN pour sécuriser les connexions à distance et éviter les interceptions de données
- Séparation claire entre les usages personnels et professionnels : ne pas mélanger comptes, appareils ou documents
- Effectuer des sauvegardes de données personnelles

Une bonne hygiène numérique, c'est comme une routine de brossage des dents - simple, mais essentielle pour éviter les fuites de données et préserver la confiance.

Mots de passe, MFA, Wi-Fi maison, appareils personnels

Hygiène numérique personnelle

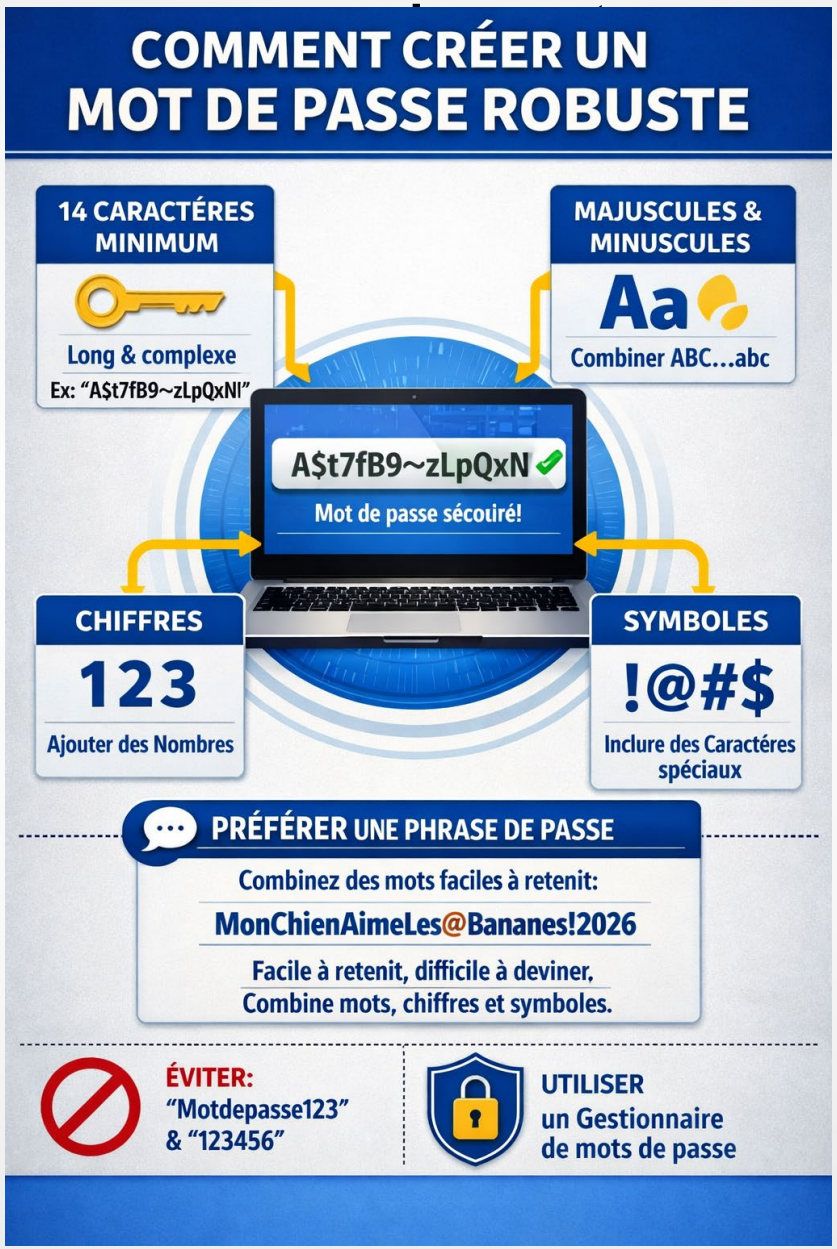
Mot de passe robuste …

Combien de temps pour craquer votre mot de passe?

Nombre de caractères	Uniquement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Lettres minuscules et majuscules + chiffres	Lettres minuscules et majuscules + chiffres + caractères spéciaux
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	1 sec	5 sec
8	Immédiat	5 sec	22 min	1 heure	8 heures
10	Immédiat	58 min	1 mois	7 mois	5 ans
12	25 sec	3 semaines	300 ans	2 000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 000 000 ans	200 000 000 ans

Source : IronTech Security

Trucs et astuces … Mot de passe



Participation – Quiz … après la pause

Oups …

AVEZ-VOUS RÉFLÉCHI AVANT D'OUVRIR LE LIEN ??

Avez-vous pensé qu'il pourrait s'agir d'hameçonnage !?

Qu’est-ce que le « Quishing » ?

https://francoischarron.com/securite/fraude-et-arnaques-web/cest-quoi-le-quishing-et-quels-sont-les-risques/VwwHZoJbXu/

Petit rappel de la définition de Quishing ?

Le terme: Quishing est la combinaison de deux termes. Il combine: **Code QR** et: **Phishing**.

C'est quoi du "phishing" ?

En bon français, une attaque de "phishing" est une tentative d'hameçonnage.

Les pirates vont « à la pêche aux poissons » en lançant plusieurs hameçons sur le web. Ces hameçons prennent la forme de messages textes ou bien de courrier électronique.

Le but de ces messages est de nous faire peur et nous inciter à cliquer sur un hyperlien (URL).

Cet hyperlien (URL) a pour but d'infecter notre appareil d'un virus ou d'un logiciel malveillant sur notre ordinateur, notre tablette ou notre téléphone intelligent.

Trucs utiles et bonnes pratiques …

🔐 Bonnes pratiques de sécurité pour les utilisateurs face aux codes QR

1. Ne jamais scanner un code QR provenant d'une source inconnue
Un QR collé sur un poteau, un comptoir, un dépliant douteux ou un courriel non sollicité = **danger potentiel**.

➡️ **Même principe que pour les liens : *si tu ne connais pas la source, ne « scanne » pas*.**

2. Vérifier l'URL AVANT d'ouvrir le site

La plupart des téléphones affichent l'URL avant l'ouverture.
L'utilisateur doit vérifier :

- que le domaine est légitime (ex. trilogie.qc.ca, pas trilogie-support-help.com)
- qu'il n'y a pas de faute ou variation suspecte
- que le protocole est **https**

3. Ne jamais entrer d'identifiants après avoir scanné un QR

Un QR peut rediriger vers :

- une fausse page Microsoft 365
- un faux portail bancaire
- un faux site municipal

➡️ **Règle d'or : *si un QR mène à une page de connexion, c'est suspect*.**

Trucs utiles et bonnes pratiques …

🔐 Bonnes pratiques de sécurité pour les utilisateurs face aux codes QR

4. Se méfier des QR collés par-dessus d'autres QR

Technique courante : un attaquant colle un autocollant QR malveillant sur un vrai QR légitime (affiche, borne, restaurant).

➡️ **Toujours vérifier visuellement si le QR semble modifié ou superposé.**

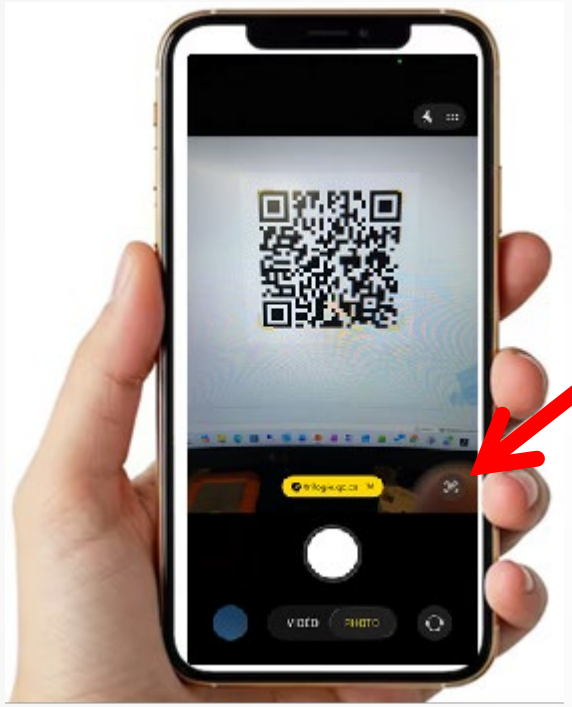
5. Ne jamais payer ou fournir des infos sensibles via un QR

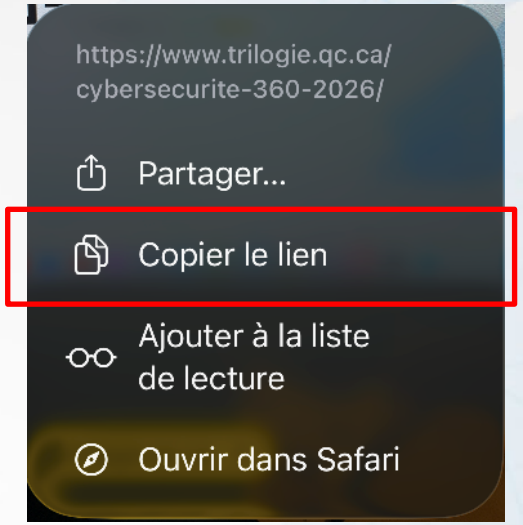
Les fraudeurs utilisent des QR pour :

- paiements frauduleux
- fausses factures
- fausses amendes de stationnement
- fausses demandes de mise à jour de mot de passe

➡️ **Toujours valider la demande par un autre canal (le site officiel).**

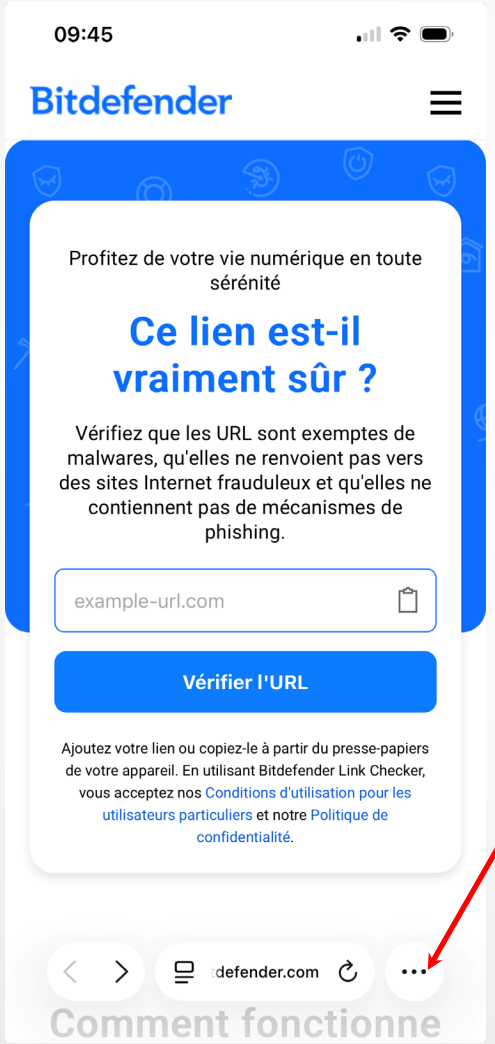
Bonne pratique … petits trucs simples

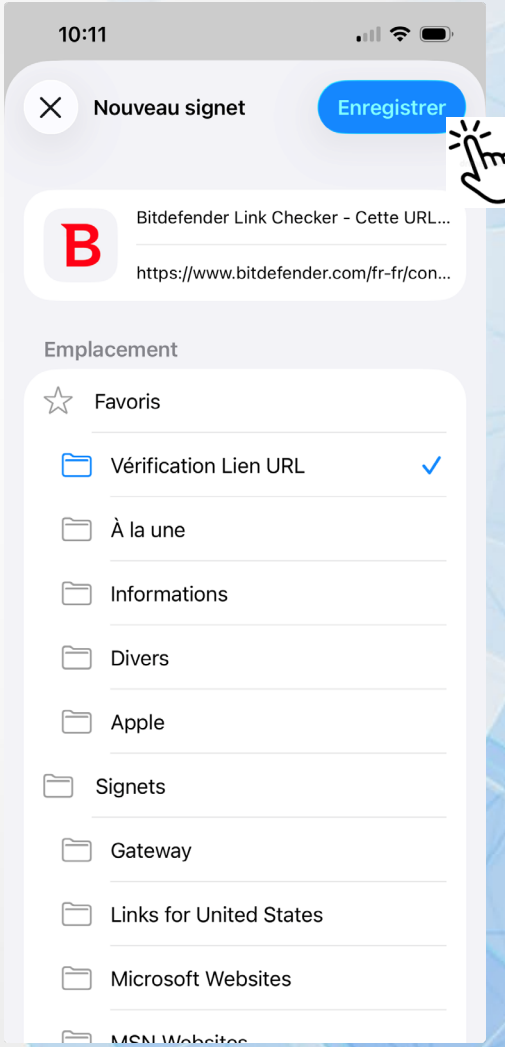




Bonne pratique … petits trucs

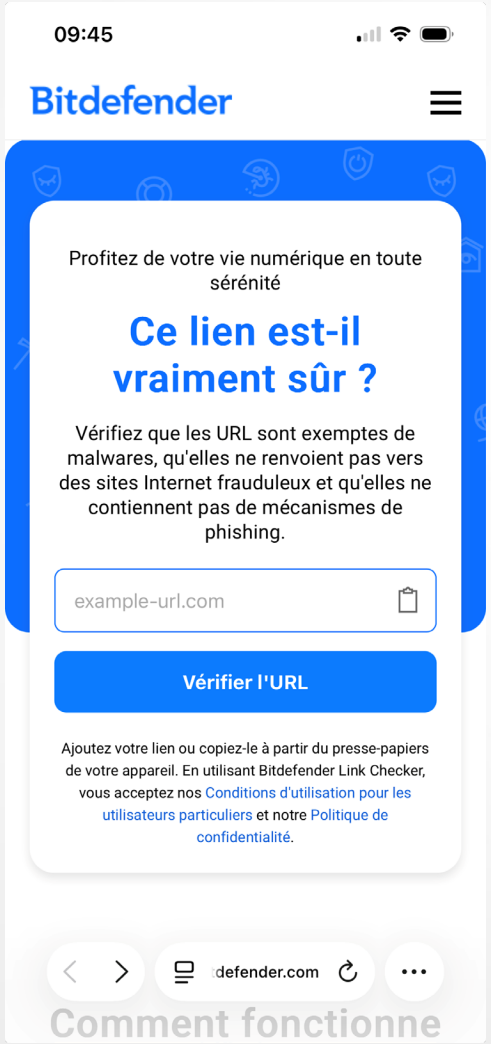
https://www.bitdefender.com/fr-fr/consumer/link-checker

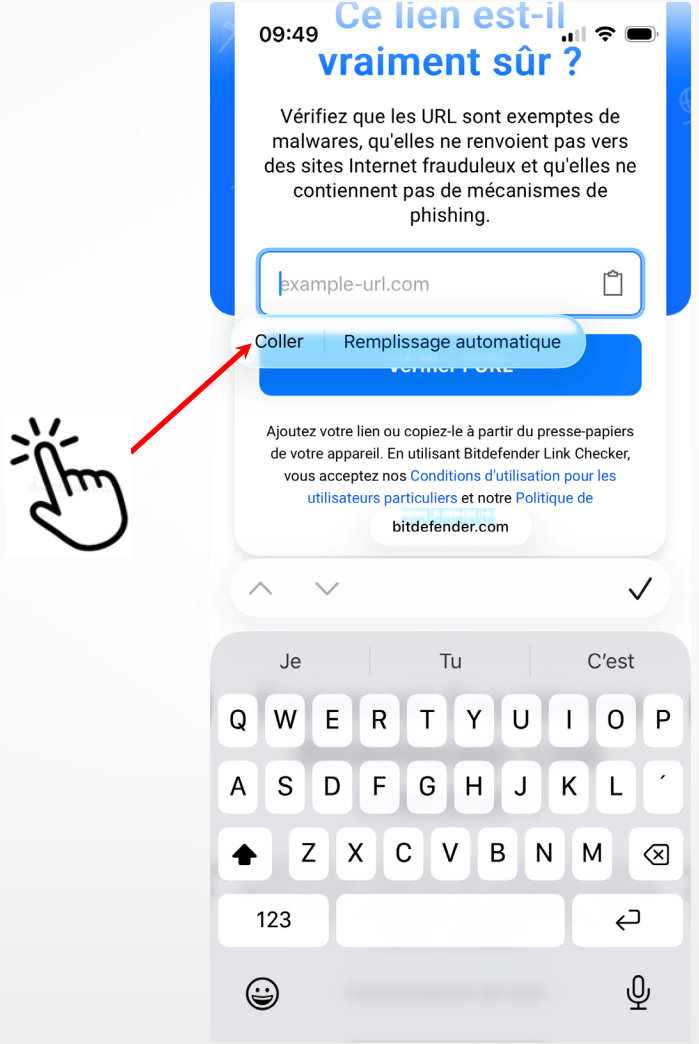


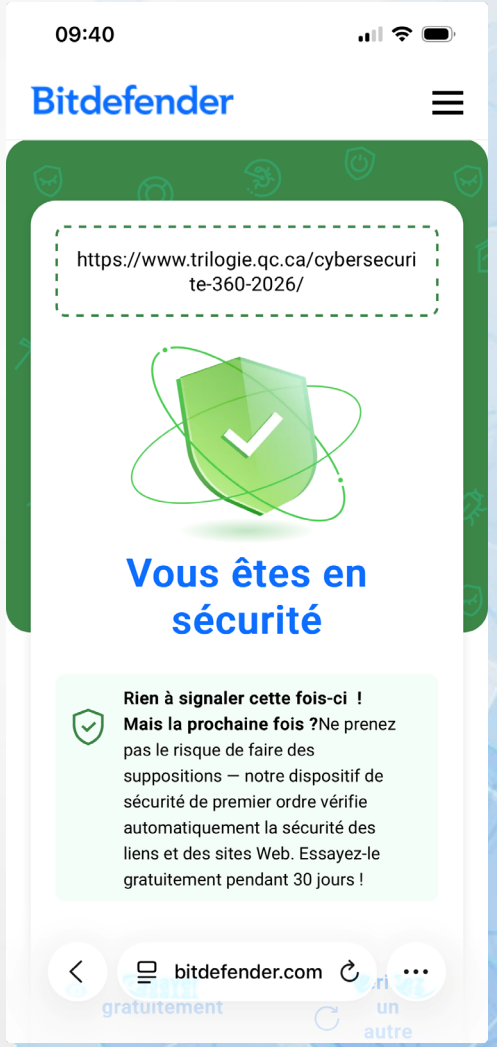


Bonne pratique … petits trucs

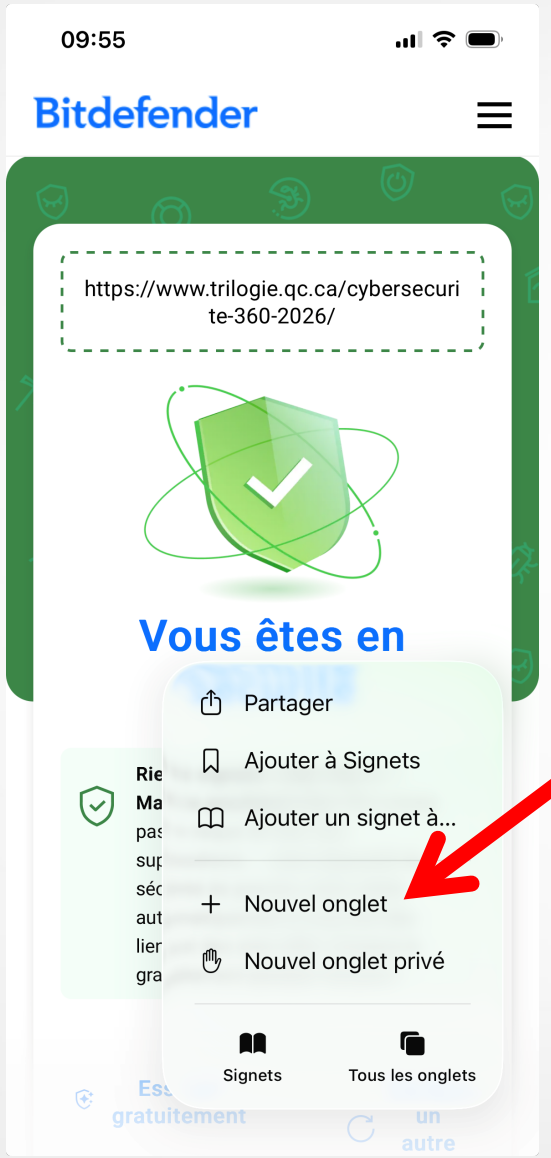
https://www.bitdefender.com/fr-fr/consumer/link-checker

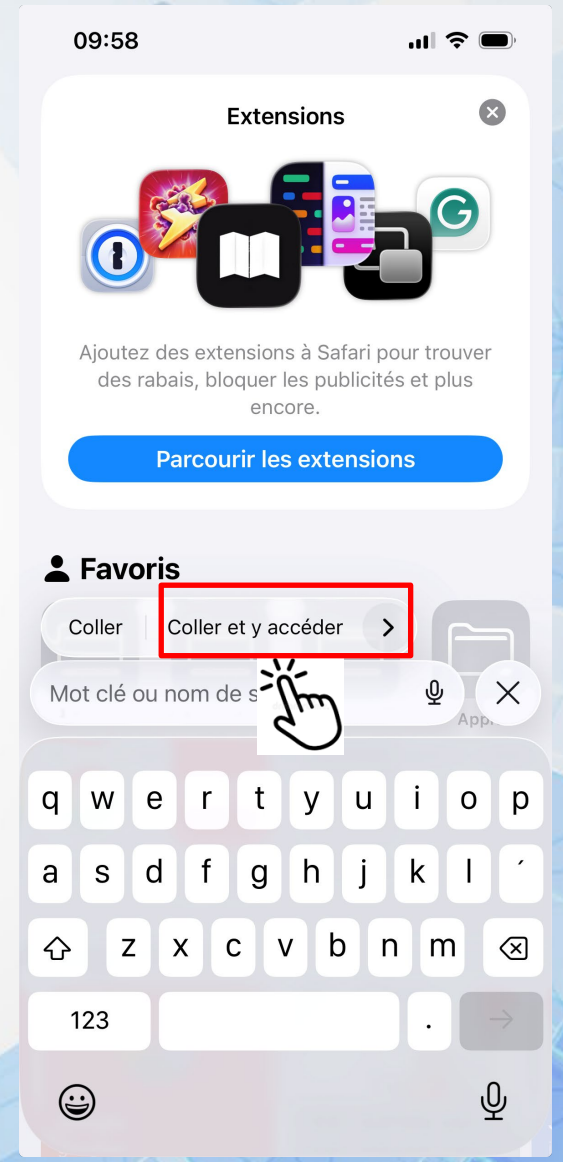






Bonne pratique … petits trucs





VRAI - Quiz …

Démarrage

Allez sur

www.menti.com

Entrez le code

7172 0341

Ou scannez le code QR

NE PAS OUBLIER …

Penser à ne pas oublier…

Utiliser un antivirus

Prudence lors des achats en ligne

Ne pas négliger les mises à jour de sécurité sur tous les appareils

Vigilance face aux messages suspects

Faire des sauvegardes de données régulières

Eviter les Wi-Fi publics ou inconnus, surtout pour des opérations sensibles

Utiliser des mots de passe robustes

Maîtriser ses réseaux sociaux, notamment face au cyberharcèlement

Bon ou pas bon …

Outlook | Répondre | Répondre à tous | Transférer | ...

Sendre : **Service des Finances** <finance@ville-quebec.qc.ca> 9:34

De : **Avis de Mise à Jour Bancaire**

Bonjour,

Suite à nos récents contróles de sécurité, nous avons constaté des divergences dans vos informations bancaires enregistrees.

Pour garantir la continuité de vos paiements sans interruption, nous vous invitons à mettre à jour vos coordonnées bancaires dés que possible.

Attention : Votre compte sera SUSPENDU si les informations ne sont pas mises à jour avant le 25 avril

Le formulaire de mise à jour est disponible en piéce jointe pour faciliter la saisie des informations requises.

Mettre à Jour Mes Informations Bancaires

Merci de procéder rapidement à cette mise à jour.

Bien cordialement,

Service des Finances
Ville de Québec.
QUÉBEC

Mise_a_jour_info.docx (79 Ko)

☑ *Demande Confidentielle*
☑ *Répondez Rapidement !*

URGENT ! ACTION IMMÉDIATE REQUISE !

Bon ou pas bon …

Outlook | Répondre | Répondre à tous | Transférer | ...

Sendre : **Service des Finances** <finance@ville-quebec.qc.ca> 9:34

De : **Avis de Mise à Jour Bancaire**

Bonjour,

Suite à nos récents contróles de sécurité, nous avons constaté des divergences dans vos informations bancaires enregistrees. 1

Pour garantir la continuité de vos paiements sans interruption, nous vous invitons à mettre à jour vos coordonnées bancaires dés que possible.

Attention : Votre compte sera SUSPENDU si les informations ne sont pas mises à jour avant le 25 avril

Le formulaire de mise à jour est disponible en piéce jointe pour faciliter la saisie des informations requises.

Mettre à Jour Mes Informations Bancaires 2

Merci de procéder rapidement à cette mise à jour.

Bien cordialement,

Service des Finances
Ville de Québec.
QUÉBEC

Mise_a jour_info.docx (79 Ko)

☑ *Demande Confidentielle*
☑ *Répondex Rapidement !*

URGENT ! ACTION IMMÉDIATE REQUISE ! 3

Loi 25 …

Loi 25 :

Protection des reseignements personnels au Québec

Loi 25 …

Elle met en avant les 5 principaux enjeux :

🔐 **Renseignements / Données personnelles — protection et accès limité.**
La Loi 25 renforce la protection des renseignements personnels. Les organisations doivent limiter l'accès aux données sensibles et s'assurer qu'elles sont stockées et utilisées de façon sécuritaire. Chaque employé devient un acteur clé de la confidentialité.

🛡️ **Sécurité de l'information — mesures de cybersécurité et gestion des incidents.**
Les municipalités et entreprises doivent mettre en place des mesures de cybersécurité robustes : pare-feu, mises à jour, gestion des incidents et formation du personnel. L'objectif : prévenir les fuites et assurer la continuité des services.

🤖 **Transparence & IA — évaluation des impacts des systèmes automatisés.**
Toute utilisation de systèmes automatisés ou d'intelligence artificielle doit être transparente. Les organisations doivent informer les citoyens et évaluer les impacts de ces technologies sur la vie privée et la prise de décision.

👥 **Droits des citoyens — accès, rectification et portabilité des données.**
Les citoyens disposent désormais de droits accrus : accès à leurs données, rectification d'erreurs et portabilité des informations. Les municipalités doivent offrir des mécanismes simples pour exercer ces droits.

⚖️ **Sanctions & conformité — obligations légales et amendes en cas de manquement.**
La Loi 25 prévoit des amendes importantes en cas de non-respect : jusqu'à plusieurs millions de dollars pour les organisations fautives. La conformité devient une responsabilité stratégique et un gage de confiance publique.

Loi 25 …

Obligations clés

- 👤 Nommer et publier un RPRP
- 🔒 Adopter une politique de confidentialité conforme
- 📋 Tenir les registres réglementaires
- ✏️ Mettre à jour les contrats fournisseurs
- 📁 Documenter les procédures internes
- 🤝 Gérer les demandes citoyennes
- 🎓 Former le personnel
- 🔍 Réaliser des EFVP pour les projets technologiques

AGFMQ
Association des gestionnaires financiers municipaux du Québec

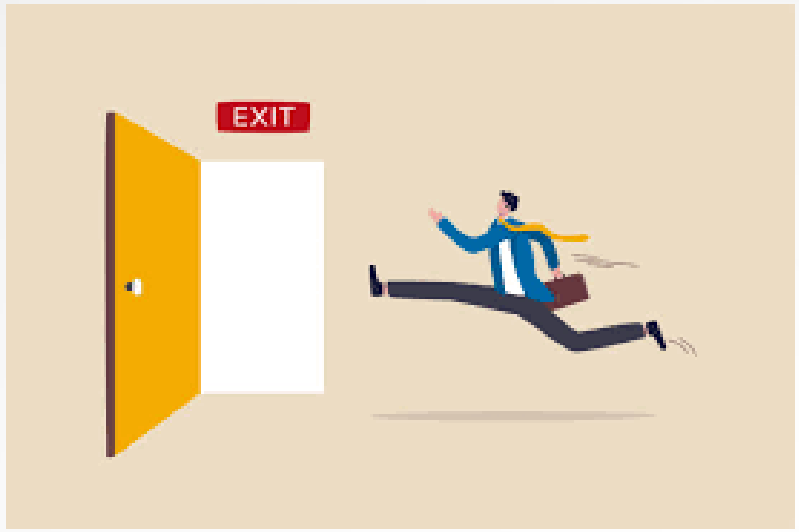
trilogie

Réaction à un incident

Incident au bureau …

Je viens de cliquer sur un courriel douteux …

Quoi faire…



LES BONS RÉFLEXES

PAS DE PANIQUE!

Quoi faire…

Lorsqu'un employé ouvre un courriel douteux ou clique sur un lien suspect, il est essentiel d'agir rapidement et méthodiquement pour limiter les impacts potentiels sur la sécurité de l'entreprise.

1 - Ne pas paniquer et ne rien fermer

Garder le courriel ou la fenêtre ouverte sans cliquer davantage. Éviter de supprimer le message ou de redémarrer l'ordinateur avant analyse.

2 - Déconnecter le poste du réseau

Si un lien ou une pièce jointe a été ouvert, ou si une fenêtre de connexion à été ouverte et rempli, débrancher le câble réseau et/ou désactiver le Wi-Fi pour éviter la propagation d'un éventuel logiciel malveillant.

3 - Avertir immédiatement le service TI ou le responsable de la sécurité

Mentionner l'heure, le type de lien ou de pièce jointe, et toute action effectuée.

4 - Ne pas tenter de corriger soi-même

Éviter d'utiliser des outils de nettoyage ou de suppression non validés. L'équipe TI doit effectuer les vérifications et la restauration si nécessaire.

Quoi faire…

5 - Changer votre mot de passe dès que possible
Si des identifiants ont été saisis après le clic, modifier immédiatement les mots de passe concernés et activer la double authentification.

6 - Sensibiliser et documenter l'incident
L'incident doit être consigné pour améliorer les pratiques internes et renforcer la formation du personnel.

💡 **Message clé**

Un seul clic peut compromettre tout un réseau.

La rapidité de réaction et la communication avec le service TI sont les meilleurs remparts contre une cyberattaque.

Incident à la maison …

Je suis sur Facebook et ce ne sont pas mes commentaires …

Quoi faire…

LES BONS RÉFLEXES

PAS DE PANIQUE!

Quoi faire…

Réagir rapidement

- Changer immédiatement le mot de passe.
- Vérifier les publications et messages envoyés automatiquement.
- Informer ses contacts qu'il s'agit d'une fraude.
- Signaler le compte compromis à Facebook via : facebook.com/hacked.

Renforcer l'accès au compte

- Utiliser un mot de passe unique et complexe : au moins 12 caractères, mélangeant majuscules, minuscules, chiffres et symboles.
- Activer la double authentification (MFA) : via application (Google Authenticator, Microsoft Authenticator) ou SMS.
- Ne jamais partager ses identifiants, même avec des collègues ou amis.

Vérifier les connexions et appareils

- Dans les paramètres Facebook → Sécurité et connexion, vérifier les appareils connectés et déconnecter ceux inconnus.
- Activer les alertes de connexion : Facebook envoie un avis si quelqu'un tente d'accéder au compte depuis un nouvel appareil.

FICHE RÉFLEXE…

FICHE RÉFLEXE…

Fiches Réflexes

Les Bonnes Pratiques

Sauvegarde

- Faire des copies régulières
- Stocker sur des supports **sécurisés**
- Tester la restauration des données

Protection des données

Utiliser un VPN

- Activer le VPN lors des déplacements
- Sécuriser la connexion Internet
- Protéger la navigation

Connexion sécurisée

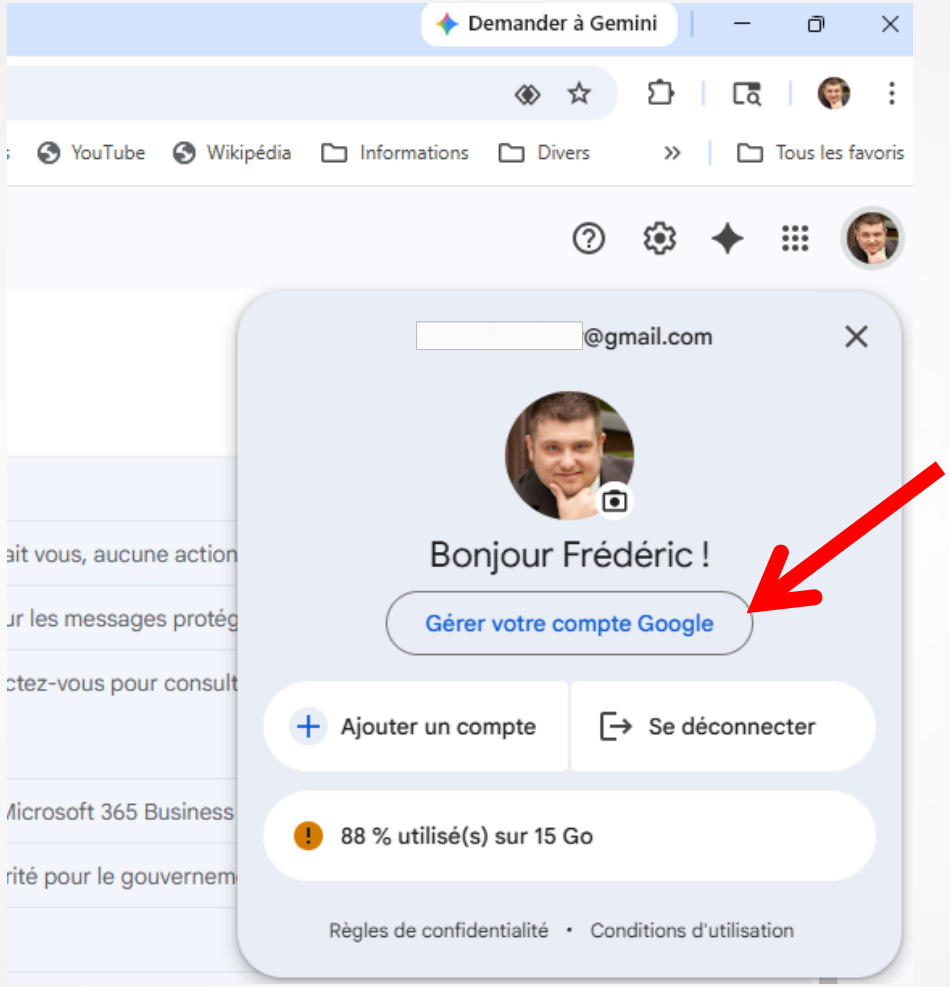
Antivirus

- Installer une solution efficace
- Mettre à jour fréquemment
- Analyser le système régulièrement
- Renforcer la sécurité des systèmes

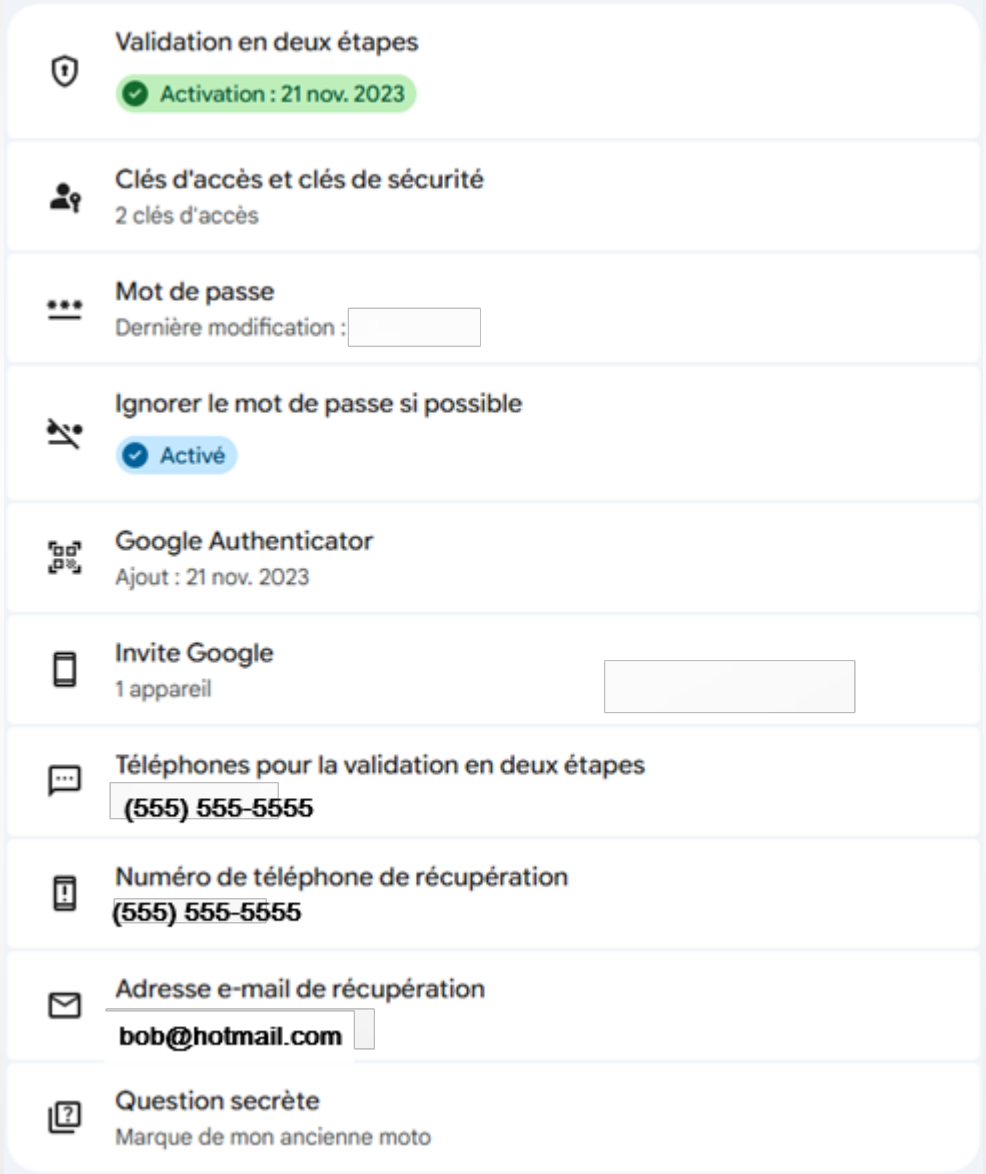
Sécurité des systèmes

Ces réflexes simples renforcent la sécurité de vos données, de vos connexions et des appareils, tant à la maison qu'au travail

Truc et astuces … gmail



Truc et astuces … gmail



Liens Utiles …

Centre Canadien de la Cybersécurité **:** **https://www.cyber.gc.ca/fr**

CIRA (Autorité canadienne pour les enregistrements Internet) Bouclier Canadien Gratuit : **https://www.cira.ca/fr/canadian-shield/**

Centre Antifraude du Canada : **https://antifraudcentre-centreantifraude.ca/index-fra.htm**

Campagne nationale de sensibilisation : **https://www.pensezcybersecurite.gc.ca/fr**

Gouvernement du Québec :

https://www.quebec.ca/securite-situations-urgence/cybersecurite/conseils-cybersecurite

Cours gratuits en ligne : **https://academie.francoischarron.com/**

De bons produits, testés par une équipe … par contre attention à la publicité !!

Vérificateurs de lien URL :

https://www.bitdefender.com/fr-fr/consumer/link-checker

https://nordvpn.com/fr/link-checker/?srsltid=AfmBOorlbxcdziAU1cFjiLxlwapQtp4IBFQ4DDtEN_Jf1eiRL3m5aLss

https://www.fortiguard.com/webfilter

Liens Utiles …

Sauvegardes de vos données personnelles :

https://francoischarron.com/gadgets-techno/web-applications/comment-faire-un-backup-de-son-ordinateur-1/ocKtML9etC/

Antivirus personnel :

https://www.journaldemontreal.com/nos-recos/techno/meilleur-antivirus/

RPV (ou VPN) :

https://www.journaldemontreal.com/nos-recos/techno/meilleur-vpn/

Gestionnaire de mot de passe :

https://fr.cybernews.com/lp/meilleurs-gestionnaires-mots-passe/?campaignId=20589777809&adgroupId=155396172393&adId=675211611541&targetId=kwd-491759452508&device=c&gunique=CjwKCAjw46HPBhAMEiwASZpLRPhz_SDMQsKiwPc6p81C0WBFbJwWsOAG2X4tNkYd9bocYO6kpRJ9YxoCCnkQAvD_BwE&gad_source=1&gad_campaignid=20589777809&gbraid=0AAAACyNk23VPOXw_EY8IDbUTj3uNlYT1&gclid=CjwKCAjw46HPBhAMEiwASZpLRPhz_SDMQsKiwPc6p81C0WBFbJwWsOAG2X4tNkYd9bocYO6kpRJ9YxoCCnkQAvD_BwE

Lexique….

DDoS (Distributed Denial-of-Service)

Une attaque DDoS désigne une "attaque DDoS par déni de service" et il s'agit d'un cybercrime dans lequel l'attaquant inonde un serveur de trafic Internet pour empêcher les utilisateurs d'accéder aux services et sites en ligne connectés.

Malware (Malicious Software)

Qu'est-ce qu'un malware (ou logiciel malveillant) ? Les logiciels malveillants sont tout programme ou logiciel informatique conçu à des fins malveillantes. Les logiciels malveillants sont utilisés pour voler des données ou infliger des dommages aux systèmes informatiques ou logiciels. Les logiciels malveillants comprennent différents types de cybermenaces telles que les virus, les logiciels publicitaires, les logiciels espions et les ransomwares. Le plus souvent, l'objectif des cyberattaques est d'utiliser le malware pour un gain financier.

Phishing (Hammeçonnage)

Le phishing est un type de menace de cybersécurité qui cible les utilisateurs directement par e-mail, SMS ou messages directs. Lors de l'une de ces escroqueries, l'assaillant se fera passer pour un contact de confiance pour voler des données telles que des identifiants, des numéros de compte et des informations de carte de crédit. Le phishing est un type d'attaque d'ingénierie sociale dans laquelle un cybercriminel utilise des e-mails ou d'autres messages textuels pour voler des informations sensibles. En utilisant une adresse e-mail crédible, un attaquant vise à inciter la cible à lui faire suffisamment confiance pour divulguer des données personnelles, telles que des identifiants deconnexion, des numéros de carte de crédit ou des informations de compte financier.

Lexique….

Ransomware
Un rançongiciel (ou ransomware en anglais) est un logiciel malveillant qui prend en otage vos données informatiques. Il chiffre (verrouille) vos fichiers ou bloque l'accès à votre appareil, puis exige le paiement d'une rançon (généralement en cryptomonnaie) en échange de la clé de déverrouillage.

RPRP
Un **RPRP** est l'acronyme de **R**esponsable de la **P**rotection des **R**enseignements **P**ersonnels. Il s'agit de la personne désignée par une entreprise ou une organisation pour veiller à la conformité des lois sur la protection des données personnelles (comme la Loi 25 au Québec).

EFVP
L'**EFVP** (**É**valuation des **F**acteurs relatifs à la **V**ie **P**rivée) est un processus d'analyse des risques qui sert à déterminer et à minimiser l'incidence potentielle d'un projet, d'un système ou d'un service sur la vie privée des personnes.

CAI
Commission d'**A**ccès à l'**I**nformation du Québec.

Petit sondage satisfaction ....

https://forms.office.com/r/r2B9jwt50p

Questions ....

Trilogie

- **450-671-1515**
- **www.trilogie.qc.ca**