

ASSURER SA CYBERSÉCURITÉ PENDANT LA SAISON DES IMPÔTS



Que vous le vouliez ou non, la saison des impôts est là. Mais attention: cette saison est aussi pour les cybercriminels une sorte de Saint Graal. La raison est simple : pour les cybercriminels, la saison des impôts constitue une occasion en or de voler des tonnes de renseignements personnels et de données critiques.

Si vous produisez votre déclaration de revenus en ligne, voici quelques façons de vous protéger contre le vol de votre identité et de votre argent.



76 %

**DES CANADIENS S'INQUIÈTENT
DU VOL DE LEUR IDENTITÉ.**



PROTÉGEZ VOTRE IDENTITÉ

**VOTRE DOSSIER FISCAL EST UNE VÉRITABLE MINE D'OR
POUR LES CYBERCRIMINELS. IL CONTIENT TOUS LES
RENSEIGNEMENTS SENSIBLES QUI LES INTÉRESSENT,
COMME VOTRE NUMÉRO D'ASSURANCE SOCIALE (NAS),
VOTRE RELEVÉ D'EMPLOI, VOTRE STATUT FAMILIAL ET MÊME
DES RENSEIGNEMENTS SUR VOS COMPTES BANCAIRES.**



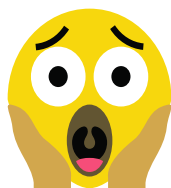
VOUS POUVEZ VOUS PROTÉGER EN :



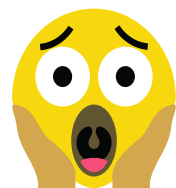
CRÉANT UN **MOT OU UNE PHRASE DE PASSE** POUR CHACUN DE VOS COMPTES FISCAUX



ACTIVANT **L'AUTHENTIFICATION MULTIFACTORIELLE** CHAQUE FOIS QUE CELA EST POSSIBLE



29 %



DES CANADIENS UTILISENT TOUJOURS LE MOT DE PASSE PAR DÉFAUT DE LEURS RÉSEAUX WI-FI À DOMICILE.!



SOUMETTEZ VOTRE DÉCLARATION DE REVENUS EN UTILISANT UN RÉSEAU SÉCURISÉ

Les réseaux Wi-Fi publics qui n'exigent pas de mot de passe, comme les réseaux de votre bibliothèque locale ou de votre café préféré, posent des risques à votre cybersécurité.

Il ne faut jamais accéder à vos comptes sensibles ou envoyer des renseignements sensibles en utilisant un réseau non sécurisé. N'effectuez ces tâches que lorsque vous avez accès à un réseau sécurisé. Si vous devez utiliser un réseau public, ayez recours à un RPV afin de protéger vos renseignements privés.



**VOUS POUVEZ SOUMETTRE
VOS DOSSIERS FISCAUX
EN TOUTE SÉCURITÉ EN :**



UTILISANT TOUJOURS UN
RÉSEAU SÉCURISÉ COMME
**VOTRE RÉSEAU WI-FI
À DOMICILE**



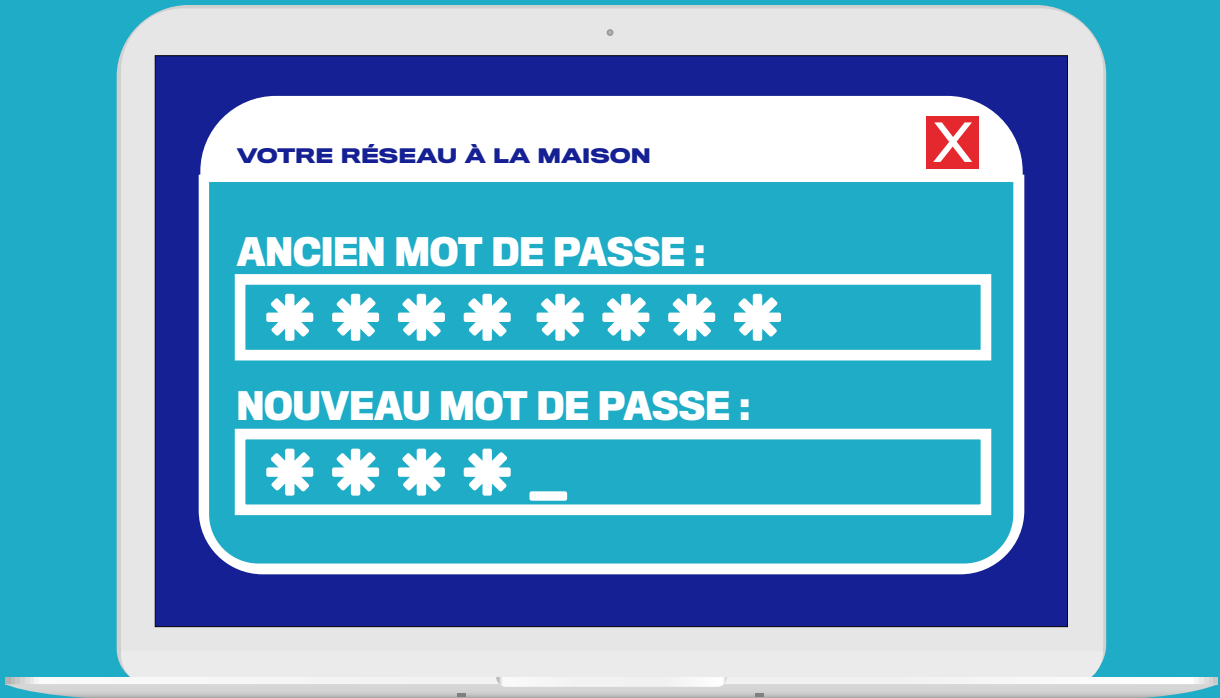
UTILISANT UN **RPV**
POUR PROTÉGER VOS
RENSEIGNEMENTS
PERSONNELS



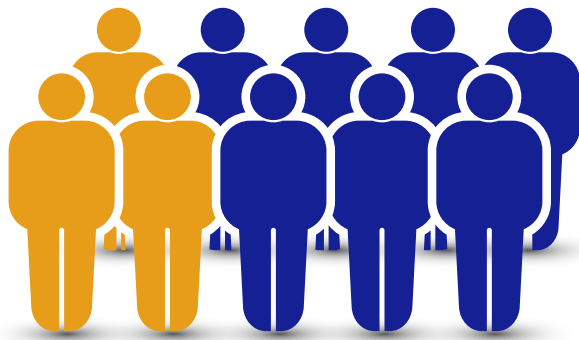
ACTIVANT VOTRE
COUPE-FEU



N'ACCÉDANT JAMAIS À VOS
RENSEIGNEMENTS PERSONNELS SUR
UN **RÉSEAU PUBLIC** À MOINS
D'UTILISER UN RPV

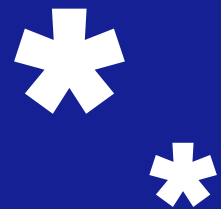
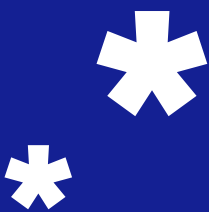
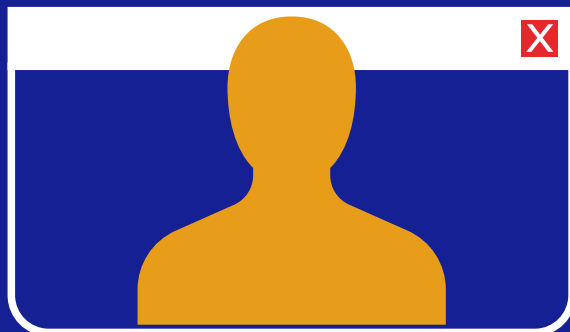


MODIFIANT **LE NOM ET LE MOT
DE PASSE** PAR DÉFAUT DE
VOTRE RÉSEAU À LA MAISON



3 sur 10

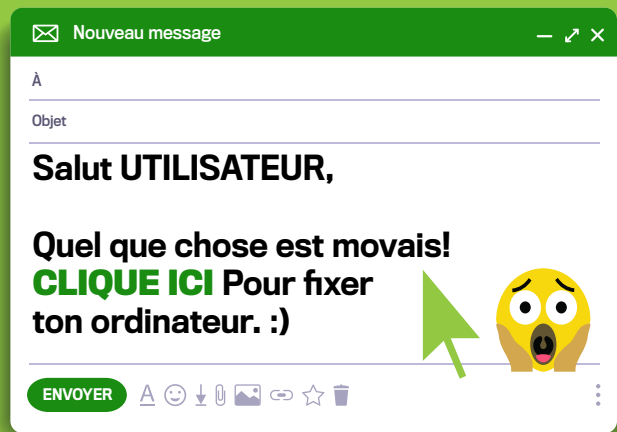
PROPORTION DE CANADIENS QUI S'INQUIÈTENT
DES ATTAQUES D'HAMEÇONNAGE.!



SOYEZ À L'AFFÛT DES TENTATIVES D'HAMEÇONNAGE

Les cybercriminels imitent souvent les sites ou messages d'organisations légitimes pour tenter de voler vos renseignements personnels. Ces tentatives d'hameçonnage sont plus difficiles à reconnaître, car vous serez peut-être tenté de croire que c'est bel et bien l'ARC qui tente de vous rejoindre.

VOUS POUVEZ RECONNAÎTRE UNE TENTATIVE D'HAMEÇONNAGE SI VOUS CONNAISSEZ LES **SIGNAUX D'ALARME :**



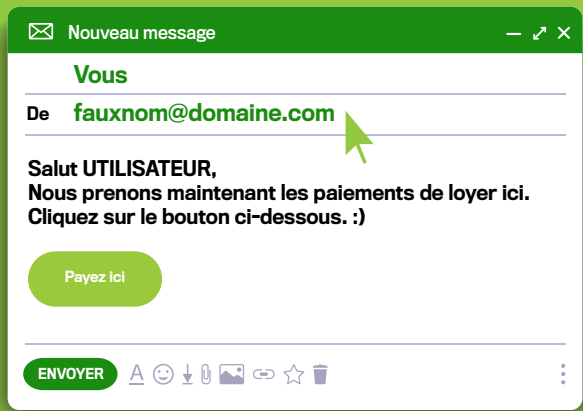
UN COURRIEL OU UN MESSAGE
TEXTE COMPORTANT DES FAUTES
D'ORTHOGRAPHE OU GRAMMATICALES



UN FORMATAGE DÉFICIENT, DES
LOGOS OU DES IMAGES FLOUES



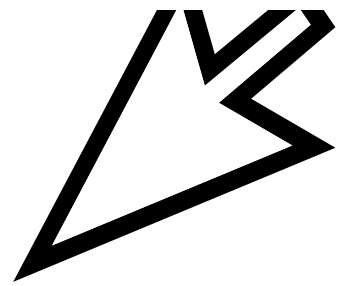
DES LIENS OU FICHIERS
JOINTS SUSPECTS



UNE ADRESSE COURRIEL SUSPECTE
OU QUI NE CORRESPOND PAS À
CELLE DE L'ORGANISATION LÉGITIME
DONT L'EXPÉDITEUR SE RÉCLAME

Vous n'êtes pas sur qu'il s'agit vraiment de
l'Agence du revenu du Canada (ARC)?
Visitez le **site Web** pour savoir à quoi
s'attendre si l'ARC vous contacte.

45 %



DES CANADIENS ACTIVENT LEURS MISES À JOUR AUTOMATIQUES.ⁱ



UNE BONNE DÉFENSE: METTRE À JOUR VOS APPAREILS

**Les mises à jour logicielles ne font pas que
contenir de nouvelles fonctionnalités.**

Elles contiennent aussi des correctifs et des mises à jour de sécurité. S'assurer que vos appareils sont constamment à jour peut vous aider à éviter une cyberattaque.

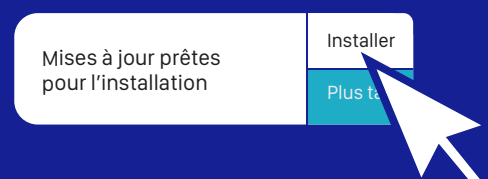
VOUS POUVEZ PROTÉGER VOS LOGICIELS EN :



ACTIVANT LA **MISE À JOUR
AUTOMATIQUE** SUR TOUS
VOS APPAREILS



METTEZ RÉGULIÈREMENT
À JOUR **VOS LOGICIELS
ANTIVIRUS**



FAISANT LA **MISE À JOUR
LOGICIELLE** DÈS QU'ELLE
EST OFFERTE

OBTENEZ PLUS DE CONSEILS POUR VOUS PROTÉGER ET PROTÉGER VOS APPAREILS À

PENSEZ **CYBERSECURITE.CA**



Centre de la sécurité
des télécommunications

Communications
Security Establishment

Canada

ⁱ Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS, 2020

Numéro de catalogue : D96-35/2021F-PDF | ISBN : 978-0-660-38000-1