NE PAS CLIQUER ICI.

Livre électronique
Common Sense Cybersecurity

ESET ENJOY SAFER TECHNOLOGY™

BIEN. MAUVAIS MOT DE PASSE.

Lors de la configuration d'un mot de passe, n'oubliez pas : *mentez, mélangez et gérez.*

CONSEIL 1 : MENTEZ

Lorsqu'on vous demande des réponses de sécurité basées sur vos renseignements personnels, par exemple le nom de jeune fille de votre mère, le nom de votre animal de compagnie, votre première voiture, etc., utilisez de fausses réponses. Si vous utilisez de vraies réponses aux questions de sécurité, les pirates informatiques peuvent facilement les trouver sur les médias sociaux.

CONSEIL 2 : MÉLANGEZ

Si vous utilisez le même mot de passe pour tous vos comptes, vous facilitez grandement le travail d'un pirate informatique. Protégez-vous en utilisant des mots de passe uniques pour chaque site Web et application nécessitant la création d'un compte personnel avec mot de passe.

CONSEIL 3 : GÉREZ

Personne ne peut se rappeler exactement ses mots de passe uniques pour des dizaines de comptes différents. Voilà pourquoi c'est une bonne idée d'utiliser un gestionnaire de mots de passe pour enregistrer les mots de passe de vos comptes de façon sécurisée.

eset

Il n'est pas toujours facile de distinguer le vrai du faux.

PRÉVENEZ LES CYBERMENACES DÉGUISÉES EN SUIVANT CES TROIS CONSEILS.

CONSEIL 1 : FILTREZ VOTRE CONTENU.

La plupart des organisations filtrent leur contenu à un certain niveau sur le lieu de travail et contrôlent les paramètres de filtrage. Cependant, même à la maison, il est conseillé d'utiliser des filtres de contenu pour vous protéger. En filtrant les pages, vous réduisez vos risques de vous exposer aux logiciels malveillants présents sur certains sites.

CONSEIL 2 : LISEZ VOS RÉSULTATS DE RECHERCHE.

Lorsque vous effectuez une recherche en ligne, prenez conscience des sites Web et des publicités fournis en réponse à votre recherche. Faites preuve de vigilance : ils ne concernent pas toujours le site, les services ou les produits que vous recherchez.

CONSEIL 3 : N'ALLEZ PAS TROP LOIN.

Concentrez-vous sur les deux premières pages de vos résultats de recherche. C'est là que se trouvent les organisations et sociétés bien établies et réputées. Plus vous allez loin, plus vous risquez de trouver des sites dangereux.

eset

LES SIGNES DE LA PRÉSENCE DE LOGICIELS MALVEILLANTS SONT FACILES À VOIR.

Identifier les logiciels malveillants est la première étape pour les éviter.

ÉTAPE 1 : SOYEZ TOUJOURS À L'AFFÛT.

Prenez l'habitude de chercher les signes de la présence de logiciels malveillants. Faites attention aux indicateurs de présence d'un logiciel malveillant, par exemple une mauvaise orthographe, une mauvaise grammaire, des URL qui semblent suspectes, ainsi que des invites faisant état d'une urgence pour vous inciter à cliquer sur un lien.

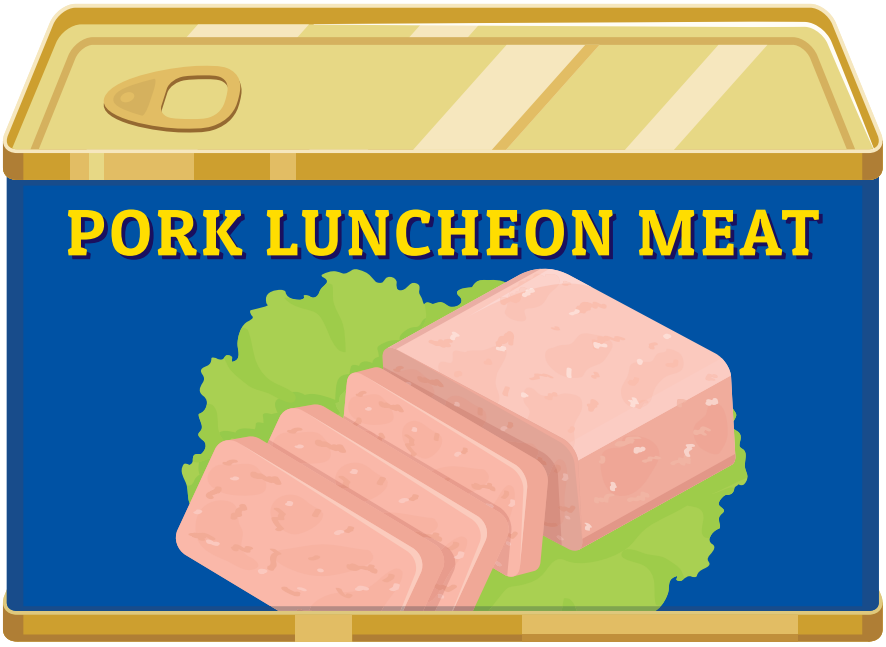
ÉTAPE 2 : VÉRIFIEZ VOS FILTRES DE CONTENU.

Au travail, votre organisation a probablement mis en place des filtres de contenu actifs. C'est aussi une bonne idée d'utiliser ces filtres à la maison, car si un courriel dangereux arrive dans votre boîte de réception, vous ne cliquerez jamais accidentellement sur un lien malveillant.

ÉTAPE 3 : N'IGNOREZ PAS LES MISES À JOUR LOGICIELLES.

Au travail, le service informatique s'assure que vos logiciels sont à jour. C'est une bonne idée de faire la même chose sur vos appareils à la maison. La mise à jour régulière de vos logiciels et de votre système d'exploitation peut régler des bogues et corriger les vulnérabilités qui pourraient être utilisées par les cybercriminels à la recherche de cibles faciles.

ESET



Ne vous laissez pas tromper par un faux.

N'OUVREZ JAMAIS DE COURRIEL INDÉSIRABLE.

CONSEIL 1 : PENSEZ-Y À DEUX FOIS AVANT DE CLIQUER.

Si un courriel, un message ou une autre communication électronique n'est pas attendu et qu'il est trompeur, cela risque d'être un pourriel. Faites preuve d'une grande prudence si un message indésirable contient un lien ou une pièce jointe. Ne téléchargez rien venant d'une source inconnue.

CONSEIL 2 : CONSERVEZ LA CONFIDENTIALITÉ DE VOS RENSEIGNEMENTS PERSONNELS.

Ne publiez jamais votre adresse électronique et vos autres renseignements personnels sur des sites Web publics, des applications ou des services. Si elle vous est demandée, prenez le temps de vous assurer que la personne ou entité demandant ce type d'information est légitime, et partagez vos renseignements de façon judicieuse.

CONSEIL 3 : UTILISEZ UN « TIROIR À POURRIELS » NUMÉRIQUE.

Créez une adresse électronique jetable, que vous pouvez utiliser pour les bulletins d'information, les abonnements, les sondages et les reçus d'achats en ligne ou en magasin. Ceci diminue grandement les risques de devenir la cible de pourriels dangereux.

eset

90 % des logiciels malveillants sont distribués par courriel et ils sont souvent très attirants.

NE VOUS LAISSEZ PAS BERNER PAR LES LOGICIELS MALVEILLANTS DÉGUISÉS EN INVITATION.

ESET

Internal America Revenue

SEE SOMETHING PAY SOMETHING

***Urgent*! Response required.**

Dear Taxplayer,

It has come to our attention that you are delinquent in your full tax payment for 2019. To avoid additional penalty fees, you must provide your SSN# immediately.

Click the link below to take care of it today, or else you'll be hearing from us again. Your wages could be garnished. And we're not talking about salt, pepper and a squeeze of lemon. We mean it. We're coming for you. Just click below to enter your SSN# and we can forget the whole matter.

Tax Filer reference: 123456789
Date received: 15 March 2019

Enter your SSN here: https://www.iard.gov.phished.hard

Internal America Revenue Department

Walla Walla, Washington
90210

L'hameçonnage fonctionne uniquement si vous faites preuve d'inattention.

Faites attention aux trois plus grands indicateurs d'hameçonnage :

INDICATEUR 1 : FAUTES D'ORTHOGRAPHE ET DE GRAMMAIRE

Les fautes d'orthographe et de grammaire, ainsi que les logos inexacts, sont un des premiers indicateurs d'une attaque par hameçonnage. Si vous constatez des erreurs flagrantes, faites particulièrement attention.

INDICATEUR 2 : DOMAINE DE L'ADRESSE ÉLECTRONIQUE

Regardez le domaine de l'adresse électronique de l'expéditeur : concorde-t-il avec un domaine connu? Un domaine d'adresse électronique est la partie de l'adresse électronique située après le symbole @. Les sociétés de confiance ont presque toutes leur propre domaine d'adresse électronique. Si vous ne reconnaissez pas l'expéditeur, lisez attentivement la ligne d'objet.

INDICATEUR 3 : URL INCONNUES

L'URL est-elle exacte? Vous pouvez le vérifier en plaçant le curseur au-dessus du lien contenu dans le courriel afin de voir s'il s'agit d'un site que vous connaissez et auquel vous faites confiance. Si l'URL ne concorde pas avec la source du courriel, ne cliquez pas.

ESET

S'il n'y a pas de « s » après http, votre sécurité n'est pas assurée.

CONSEIL 1 : PARTAGEZ VOS RENSEIGNEMENTS UNIQUEMENT SUR LES SITES FIABLES.

Ne saisissez jamais de renseignements personnels (mots de passe, identifiants de connexion bancaire, etc.) sur un site, sauf si son authenticité est avérée. Les sites utilisant le protocole https: sont généralement plus sécuritaires, mais pour vous en assurer, vérifiez attentivement le nom de domaine.

CONSEIL 2 : MÉFIEZ-VOUS DES RÉSEAUX WI-FI PUBLICS.

Traitez toujours les réseaux Wi-Fi publics comme s'ils étaient risqués. Supposez que des pirates informatiques pourraient chercher une cible facile sur un réseau public. De plus, ne visitez jamais de sites Web délicats (banques, médias sociaux) en utilisant un réseau Wi-Fi public. Utilisez plutôt les données de votre téléphone.

CONSEIL 3 : CHERCHEZ LE CADENAS.

L'icône de cadenas de votre navigateur indique que les données transférées entre le site et vous sont chiffrées et refusent l'accès aux tiers externes. Cependant, cela ne garantit pas que le site Web n'est pas malveillant. Il vaut toujours mieux vérifier deux fois le nom du domaine.

www.eset.com