FORMATION EN CYBERSECURITÉ

K2E Security

LES OBJECTIFS

DE LA SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

- Protéger votre information importante
  - *compte bancaire, compte de travail, information personnelle*
- Éviter de compromettre votre lieu de travail
- Protéger vos amis et vos collègues de travail

LES ATTAQUES

L'INGÉNIERIE SOCIALE

- **Objectif:** Vous dupez afin de recevoir des renseignements ou afin de vous faire commettre une action criminelle
- Il y a plusieurs types d'attaque:
  - Appel téléphonique (ex: un technicien en informatique imposteur appelle)
  - Courriel (hameçonnage - "Phishing")
- Soyez prudent! Les ingénieurs sociaux peuvent déjà avoir plus de renseignements que vous ne le pensez.

LES ATTAQUES

L'HAMEÇONNAGE

- Un courriel qui cache son intention de nuire
- COMMENT identifier un hameçonnage ?
  - Le courriel veut que vous interagissez en:
    - *Téléchargeant un fichier*
    - *Cliquant sur un lien*
    - *Répondant pour donner de l'information*
  - Il crée un sentiment **d' URGENCE**
    - *Évoque: la peur, l'avidité, la curiosité ou la compassion*

UN EXEMPLE

D'HAMEÇONNAGE

À: <destinataires-non-divulgués>
De: fraude@servicepublic.com
Sujet: Réclamez votre Grand Prix! MAINTENANT

Bonjour,

Nous avons un virement bancair de $1000000!

c'est ton prix

Cliquez ici pour réclamer

expir dans deux jours

Merci,
Mike
BMO

Mais ce n'est pas toujours aussi évident...

SOYEZ VIGILANT! 👀

- Un courriel d'hameçonnage peut sembler provenir d'individus ou d'organisations dans lesquels vous avez confiance.
- Il faut se concentrer sur trois parties importantes d'un courriel

L'expéditeur

QUI envoie ce couriel?

Le contexte

POURQUOI envoyer ceci?

Le contenu

Est-ce que ça tient debout?

LES ATTAQUES

LA MYSTIFICATION

- Le faux expéditeur
  - L'expéditeur associe un faux nom d'affichage à son adresse électronique pour dissimuler ses intentions malveillantes (ce pourrait être le nom d'un ami, d'un collègue ou même votre propre nom)
- Soyez prudent en voyant que le courriel a été envoyé à plusieurs personnes.
- Méfiez-vous d'organisations ayant des services de messagerie gratuits
  - ex: support@servicepublic.com

QUOI VÉRIFIER?

À: <destinataires-non-divulgués>
De: finance@gmail.com
Sujet: Salaire

Bonjour Kim,

Nous avons un virement bancaire de $1512.30!

Ceci est pour vos deux dernières semaines de travail.

Cliquez ici pour déposer votre argent

Ce virement expirera dans dix jours.

Merci,
Mike
Banque Royale

Demandez-vous:

□ *Est-ce que l'expéditeur m'enverrait vraiment ce courriel ?*

□ *Devrait-il déjà avoir cette information ?*

□ *Est-ce que je m'attendais à cette requête ?*

□ *Est-ce logique ?*

Méfiez-vous:

□ *Des offres qui requièrent peu d'effort et demandent de l'information personnelle*

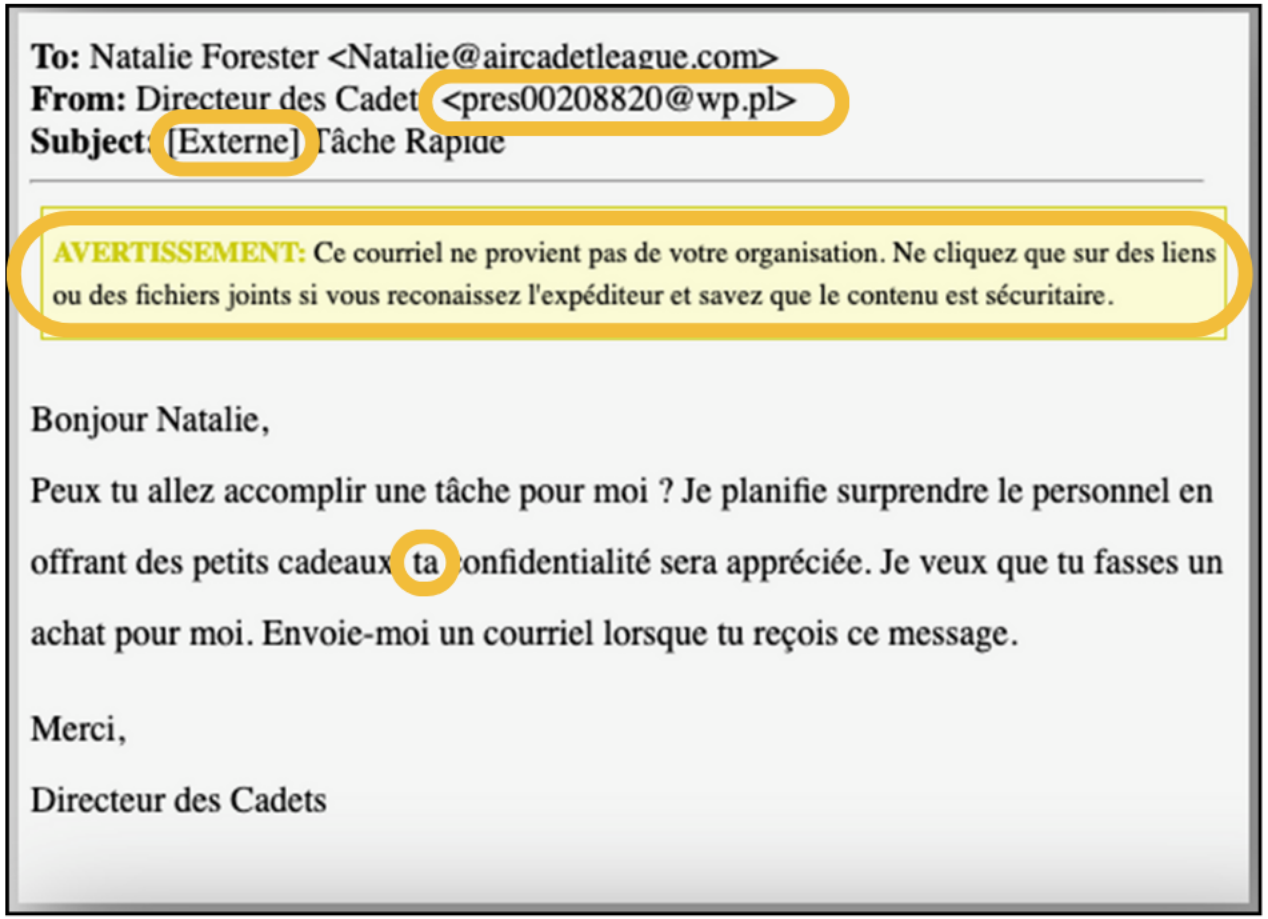
□ *Des salutations et des messages généraux*

Des erreurs de grammaire

De LIENS et de FICHIERS JOINTS

NE DONNEZ JAMAIS VOS MOTS DE PASSE

EXEMPLE



To: Natalie Forester <Natalie@aircadetleague.com>
From: Directeur des Cadet <pres00208820@wp.pl>
Subject: [Externe] Tâche Rapide

AVERTISSEMENT: Ce courriel ne provient pas de votre organisation. Ne cliquez que sur des liens ou des fichiers joints si vous reconaissez l'expéditeur et savez que le contenu est sécuritaire.

Bonjour Natalie,

Peux tu allez accomplir une tâche pour moi ? Je planifie surprendre le personnel en offrant des petits cadeaux ta onfidentialité sera appréciée. Je veux que tu fasses un achat pour moi. Envoie-moi un courriel lorsque tu reçois ce message.

Merci,

Directeur des Cadets

Demandez-vous:

□ *Est-ce que ce courriel vient de mon organisation ?*

□ *Est-ce qu'il y a un avertissement?*

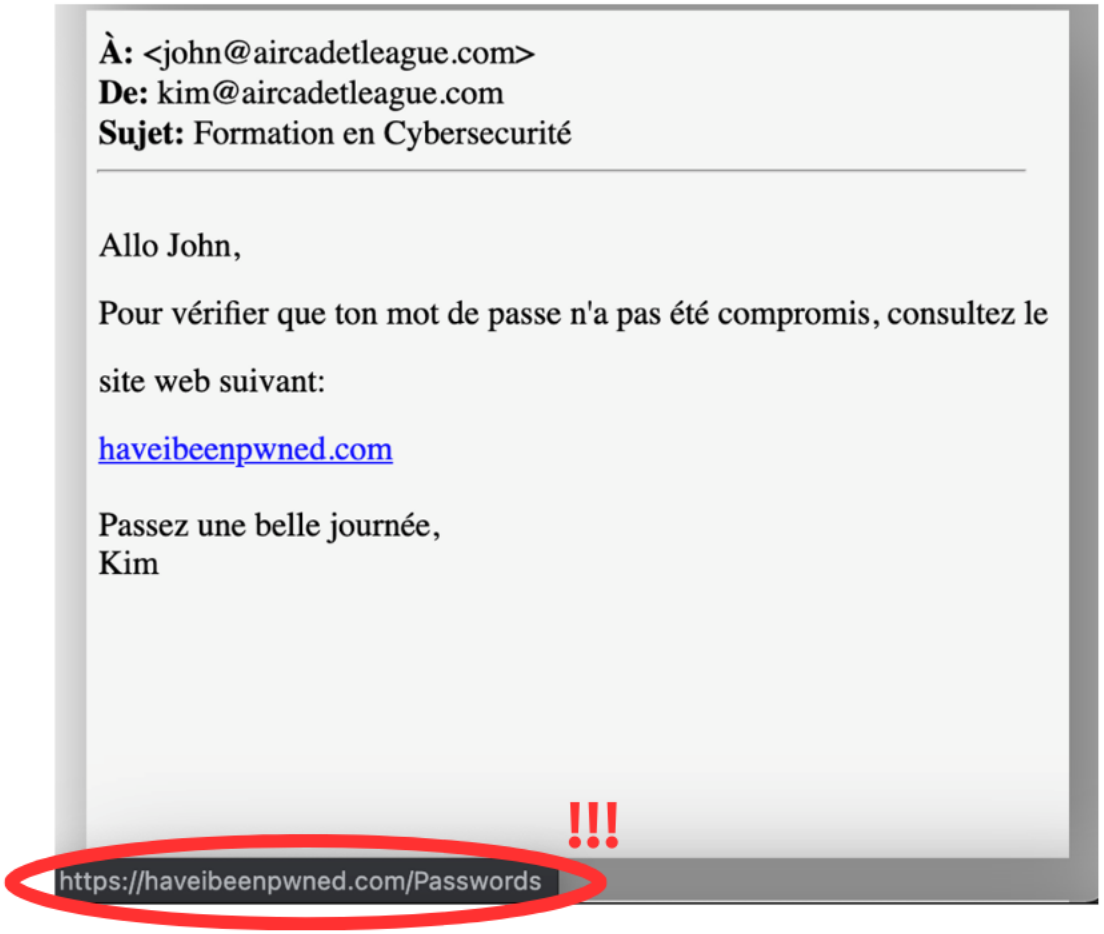
□ *Y a-t-il une raison pour laquelle le directeur des cadets utilise son compte personnel?*

□ *Y a-t-il des erreurs de grammaire ?*

Devrais-je répondre ? NON

APPELEZ LA PERSONNE OU ENVOYEZ UN COURRIEL À L'ADRESSE DE SON ORGANISATION

QUAND CLIQUER?



✓ *Placez votre souris sur le lien sans cliquez !*

✓ *Ne cliquez pas si vous n'êtes pas certain !*

INSPECTEZ LES LIENS

www.paypal.com/ca/webapps/mpp/home

Bon lien ! Ce qui vient après le premier ‘ /’ n’a pas d’importance

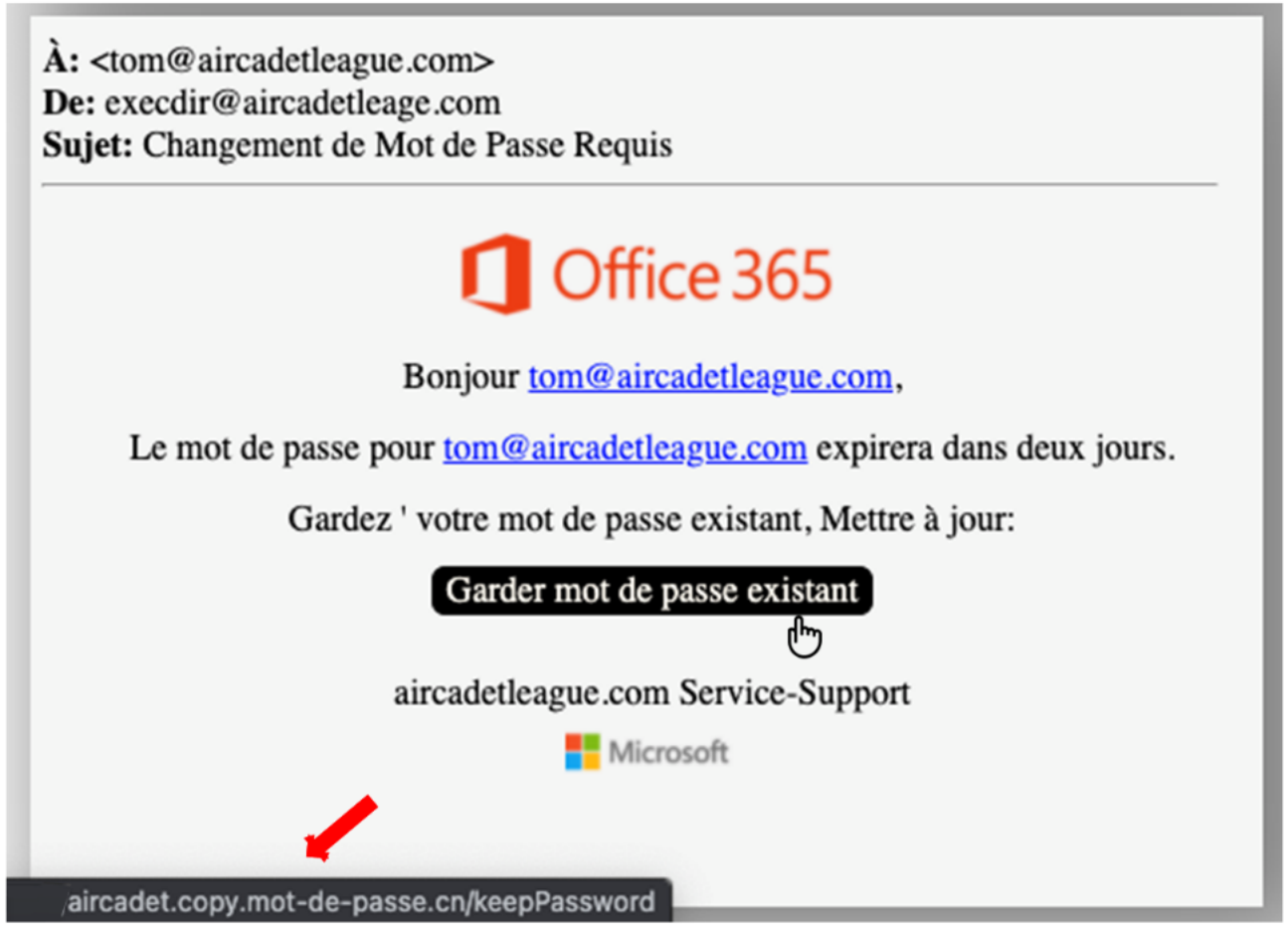
paypal.com.vendre-acheter.cn/services

Mauvais lien ! Ce qui vient avant le premier ‘ /’ est important.
.cn = Chine et non Canada
.vendre-acheter n’est pas le domaine de PayPal

www.BANQUER0YALE.com

Mauvais lien ! Un zéro (0) remplace le O. Il faut faire attention à la substitution de caractères.

LE PIÈGE DU MOT DE PASSE



- Est-ce que je m'attendais à cette requête ?
- Survolez le lien
- **Si vous n'êtes pas certain:**
  - Ne cliquez pas le lien
  - Appelez
  - Si possible, allez sur le vrai site web

L'Objectif du Piège

- Il demande de "vérifier" ou de "garder" votre mot de passe existant

LES MOTS DE PASSE

Les mots de passe se font souvent pirater parce que les humains ont des façons de penser similaires

Bonnes Pratiques en Matière de Mots de Passe:

- Au moins 12 caractères
- Au moins une lettre majuscule et une lettre minuscule
- Un nombre
- Un symbole (- / _ *)
- Authentification à deux facteurs
- Une phrase de passe est généralement sécuritaire et facile à retenir

BONS MOTS DE PASSE

Sol3eil-plAsma-aplomb

paiN-munition5-canard

MAUVAIS MOTS DE PASSE

pa$$word1

cadets2023!

À ÉVITER

❌ Un mot du dictionnaire
❌ Noter son mot de passe
❌ Partager son mot de passe
❌ Inverser les mots
❌ Le même mot de passe pour tout
❌ Nom d'utilisateur, noms, endroits, fêtes, mots techniques

À FAIRE

✓ Combinaisons de mots au hasard
✓ Gestionnaire de mots de passe pour auto-créer et enregistrer ses mots de passe

Ex: *Bitwarden*
1Password

LES LOGICIELS MALVEILLANTS

Soyez conscient de la diversité des virus

- *Trojan (chevaux de Troie)* – prennent l'apparence d'un logiciel utile
- *Virus de cryptage web* – se cachent dans des sites web infectés
- *Pirates de navigateur* – prennent contrôle de votre navigateur pour vous redirigez vers leur site web
- *Infecteurs de fichier* – attaquent lorsque vous utilisez un fichier exécutable *(ex: extension .exe)*
- *Macrovirus* – attaquent lorsque vous ouvrez un document infecté (ex: Microsoft Word, Excel)

COMMENT AVOIR UN VIRUS ?

- *Ouvrir des fichiers joints ou cliquer des liens venant de sources douteuses*
- *Cliquer des annonces publicitaires*
- *Oublier de mettre à jour des appareils électroniques*
- *Être imprudent sur les réseaux sociaux*
  - *ex: ton ami t'envoie une vidéo drôle, CLIQUER pour regarder! 'Je t'ai vu dans cette vidéo !'*
- *Télécharger des applications qui ne proviennent pas d'un site web officiel*
  - *ex: Télécharger de la musique piratée*

CE QU'UN VIRUS PEUT FAIRE...

- *Effacer des données importantes*
- *Voler de l'information ou des mots de passe*
- *Corrompre des fichiers*
- *Envoyer des pourriels à vos contacts*
- *Prendre contrôle de votre ordinateur*
- *Rançongiciel – bloquer l'accès à vos données*
- *Demande un service ou de l'argent*

AVEZ-VOUS DÉJÀ UN VIRUS INFORMATIQUE ?

- *Plusieurs fenêtres contextuelles*
- *Votre page d'accueil est différente*
- *Beaucoup de courriels sont envoyés de votre compte*
- *Votre appareil tombe en panne*
- *Votre ordinateur est lent*
- *Des programmes inconnus sont exécutés lorsque vous allumez votre appareil*
- *Votre mot de passe change involontairement*

PROTÉGEZ VOS APPAREILS

- Sauvegardez vos documents dans différents endroits sécuritaires pour prévenir les conséquences d'un Rançongiciel
- Mettez à jour vos appareils et leurs applications, les mises à jour enlèvent souvent des vulnérabilités.
- Logiciel Antivirus
  - Attention! Les virus peuvent se déguiser en logiciels antivirus (Trojan)
  - Activez votre antivirus gratuit: Windows Defender
  - Achetez un logiciel antivirus tel que CrowdStrike si vous voulez encore plus de protection
  - Ne téléchargez pas de fichiers et logiciels qui ne sont pas de sources officielles

WIFI PUBLIC ET POINT D'ACCÈS SANS FIL

- Connectez seulement aux WIFIs en lesquels vous avez confiance
- Connectez seulement aux WIFIs et points d'accès sans fil sécuritaires qui ont des mots de passe
- Soyez méfiant des WIFIs de lieux publics (ex: hotel) si vous n'utilisez pas un VPN
- Désactivez la connection automatique aux WIFI
- Utilisez seulement les sites web HTTPS

LES PARE-FEUX ET LES VPNS

- **Firewalls**
  - Le Pare-feu peut:
  - Définir vos préférences de sécurité et décider ce qui peut atteindre votre ordinateur
  - Bloquer certains sites web
  - Protéger votre réseau des réseaux externes (internet)
- **Le VPN peut:**
  - Permettre à l'utilisateur d'être anonyme en ligne
  - Protéger votre information et crypter vos données

LE PARTAGE DE FICHIERS

- N’utilisez pas votre adresse courriel personnelle dans votre organisation
- Utilisez des services de partage de fichiers sécuritaires: OneDrive/SharePoint, Google Drive
- Activez un logiciel antivirus et installez/activez un pare-feu
- Partagez des fichiers à des personnes en qui vous avez confiance et des personnes de votre organisation
- Ne téléchargez pas de l’information confidentielle sur des clés USB non cryptées en cas de perte ou de vol

Risques

- L’installation de virus
- La perte de données importantes
- Donner plus de permissions que l’on veut

RÉSUMÉ

- Inspectez vos courriels
- Adhérez aux bonnes pratiques en matière de mots de passe – considérez utiliser un gestionnaire de mots de passe
- Inspectez un lien avant de le cliquez
- Soyez prudent en ouvrant ou téléchargeant des fichiers joints
- Téléchargez des logiciels fiables de sources officielles
- Soyez prudent en connectant aux réseaux publics
- Allez seulement sur des sites HTTPS
- Considérez utiliser un VPN et un logiciel antivirus
- Mettez à jour vos appareils électroniques et leurs applications
- Assurez-vous que les paramètres de vos appareils soient sécuritaires - vérifiez que vos appareils ne se joignent pas automatiquement aux réseaux étrangers

QUESTIONS?

K@K2ESEC.COM

INFO SUPPLÉMENTAIRE

Propriétaire de Windows – Windows Defender

- Protection contre les logiciels d'espionnage, les virus et autres logiciels malveillants

1. Cliquer le menu Démarrer (bouton Windows)
2. Icône Réglages > Mise à jour et sécurité > Sécurité de Windows
3. Protection contre les virus > Paramètres de protection
4. Activer la protection en temps réel

https://www.premiers-clics.fr/cours-informatique/activer-ou-desactiver-antivirus-windows-defender/

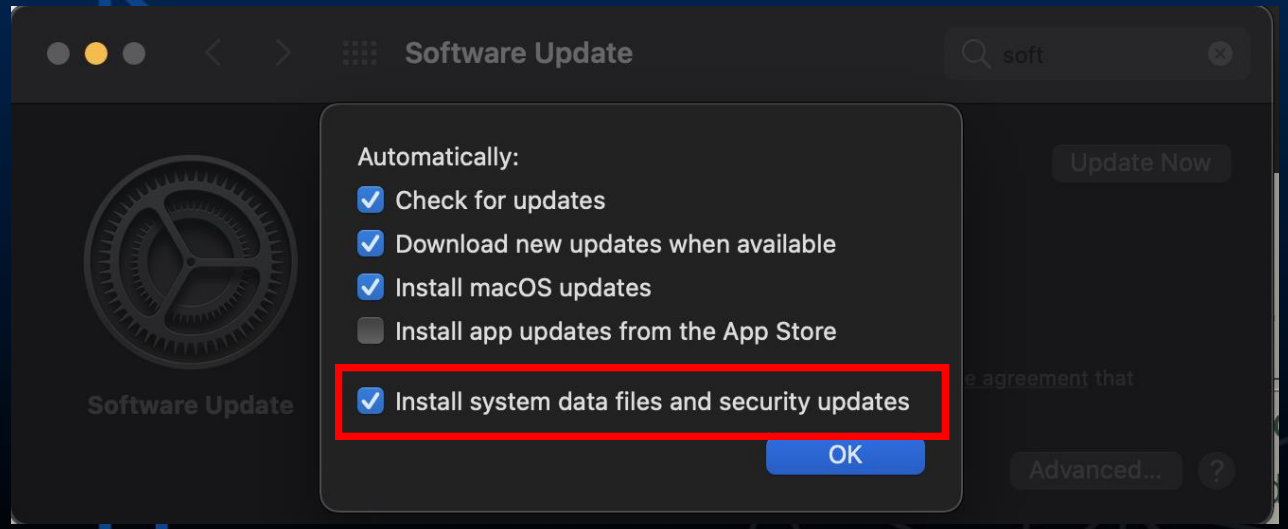
Propriétaires de Mac - XProtect

- Les Macs ont un antivirus de base nommé XProtect
- Il vérifie les applications exécutées et les compare à une liste de programmes malveillants
- System Preferences > Software Update > Install system data files and security updates (OS X 10.10 or later)

  En français:

  Préférences Système > Mise à jour de logiciels > Installer les fichiers de données système et les mises à jour de sécurité (OS X 10.10 ou plus)

- Ceci confirme que XProtect est automatiquement mis à jour



https://support.apple.com/en-ca/guide/security/sec469d47bd8/web

Gmail – Authentification à deux facteurs

1. Ouvrez https://myaccount.google.com/
2. Panneau de Navigation > Sécurité
3. Sous "Connexion à Google” > Validation en deux étapes > Commencer.
4. Suivez les étapes à l’écran

https://support.google.com/accounts/answer/185839?hl=fr&co=GENIE.Platform%3DDesktop

Microsoft – Authentification à deux facteurs

1. Allez aux paramètres de sécurité: https://account.microsoft.com/security
2. Connectez-vous
3. Sélectionnez "Plus d'options de sécurité"
4. Vérification en deux étapes > Configurer la vérification en deux étapes
5. Suivez les instructions

https://support.microsoft.com/fr-fr/account-billing/proc%C3%A9dure-d-utilisation-de-la-v%C3%A9rification-en-deux-%C3%A9tapes-avec-votre-compte-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4

Comment activer l'authentification à deux facteurs pour Google Suites

https://support.google.com/a/answer/9176657?hl=fr&ref_topic=2759193&sjid=8659623856037069961-NA

1. Connectez-vous à la Console d'administration Google > Sécurité > Authentification > Validation en deux étapes
   a) *Autoriser les utilisateurs à activer la validation en deux étapes*
   b) *Application > Désactivée (si cette option est activée les utilisateurs sans l'authentification à deux facteurs seront incapables de se connecter à leur compte)*
2. Dites aux utilisateurs qu'ils peuvent activer l'authentification à deux facteurs en suivant les instructions suivantes:
   https://support.google.com/accounts/answer/185839
3. (Optionel) Sélectionnez Application > Activée - après vous être assuré que tous les membres se soient enrôlés.

Comment activer l’authentification à deux facteurs pour Microsoft Office Suite

L’administrateur doit activer l’authentification à deux facteurs > Activer Authentification moderne pour votre organisation

Lire les étapes contenues dans le lien ci-dessous:

https://learn.microsoft.com/fr-ca/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?redirectSourcePath=%252fen-us%252foffice%252f8f0454b2-f51a-4d9c-bcde-2c48e41621c6&view=o365-worldwide

Les étapes pour les utilisateurs:

1. Connectez-vous comme vous le feriez d’habitude
2. Vous allez être notifié que plus d’information est nécessaire > Cliquez sur Suivant
3. Téléchargez l’application gratuite Microsoft Authenticator sur votre téléphone

https://support.microsoft.com/fr-fr/office/configurer-votre-connexion-microsoft-365-pour-l-authentification-multifacteur-ace1d096-61e5-449b-a875-58eb3d74de14?ui=en-US&rs=en-US&ad=US

Sources

[1] A. Grace, “What Is A Computer Virus?” https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

[2] Crystal Bedell, P. Loshin, and K. Hanna, “What is a computer worm and how does it work?,” *SearchSecurity*. https://searchsecurity.techtarget.com/definition/worm.

[3] ENOUGH IS ENOUGH, “A Guide to Public Wifi Security Risks & How to Use it Safely,” *Internet Safety 101*. https://internetsafety101.org/publicwifisafety.

[4] United States Government, “Risks of File-Sharing Technology | CISA,” Cybersecurity and Infrastructure, 2010. https://us-cert.cisa.gov/ncas/tips/ST05-007 (accessed Jul. 26, 2021).