

C'est ensemble qu'on avance

CLUB INFORMATIQUE VRAIS BRANCHÉS DE LONGUEUIL



LA CAPACITÉ DE
L'INTELLIGENCE
ARTIFICIELLE

À DÉCELER

LES COURRIELS
INDÉSIRABLES





Synopsis:

Les fonctions de recherche de l'intelligence artificielle peuvent vous permettre de contourner le danger face aux courriels indésirables, vous évitant bien des difficultés et surtout de tomber dans le piège en cliquant au mauvais endroit.

Venez découvrir comment l'intelligence artificielle repère les courriels frauduleux: analyser des entêtes, détection de liens piégés, apprentissage automatique des tactiques d'hameçonnage.

Ordre du jour

Introduction à l'IA
et la détection des
courriels
indésirables

Origines et
développement
de l'IA

Comment l'IA
détecte les
courriels
indésirables

Avantages de
l'utilisation de l'IA

Défis de l'IA dans
la détection des
courriels
indésirables

Perspectives
d'avenir

Conclusion

Procédure à
suivre pour tester
un courriel
légitime

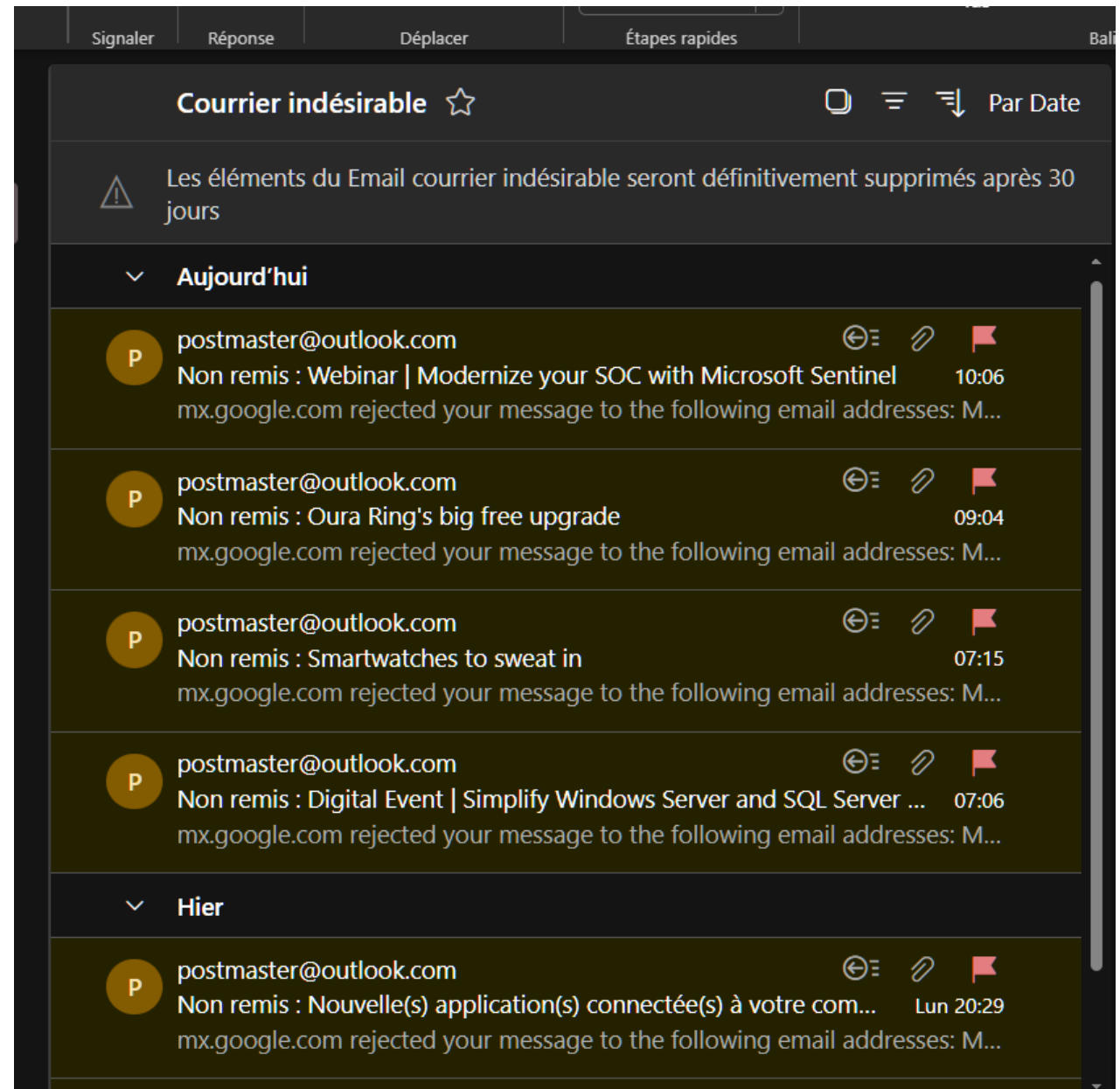
Procédure à
suivre pour tester
un courriel
indésirable

Gabarit pour
vérifier si un
courriel est
légitime

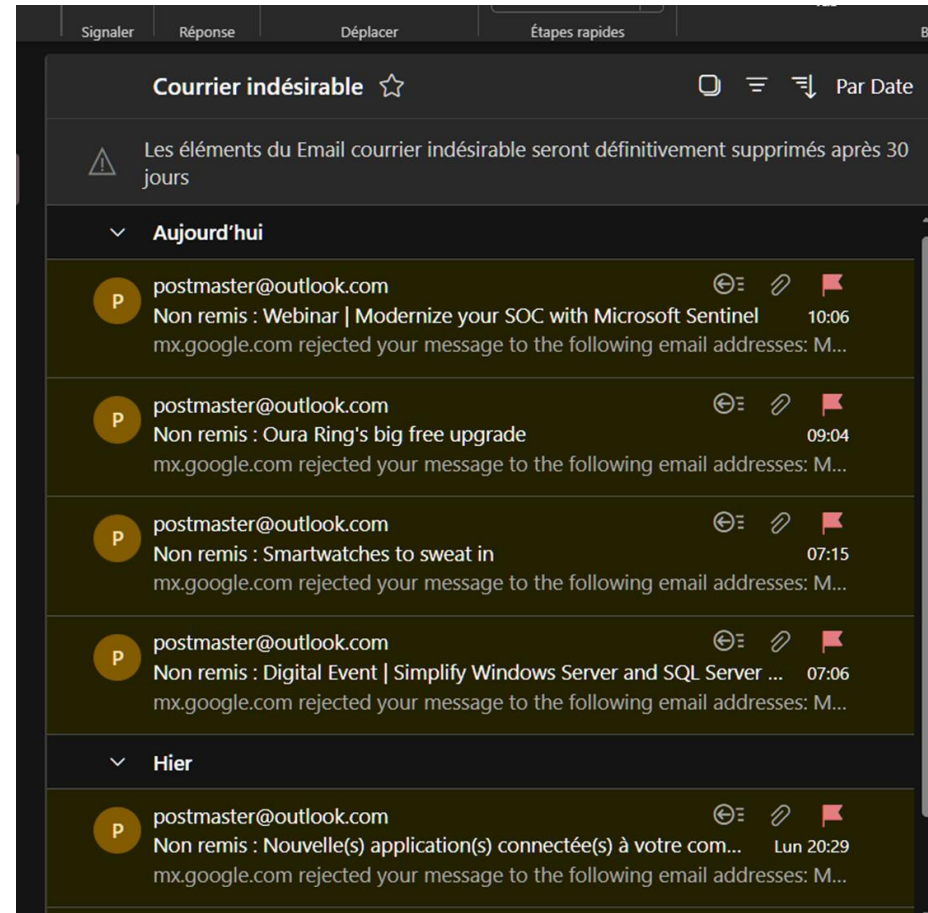
Modèle de
conversation
sécuritaire

Ressources utiles

Boîte des indésirables



Quelques exemples qui sont dans la boîte des “indésirables”



Introduction à l'IA et la détection des courriels indésirables

Introduction à l'intelligence artificielle (IA)

- Transformation des aspects quotidiens
- Capacité à détecter les courriels indésirables

Mécanismes de détection des courriels indésirables

- Analyse des entêtes
- Détection de liens piégés
- Apprentissage automatique des tactiques d'hameçonnage

Avantages de l'utilisation de l'IA

- Rapidité de détection
- Précision accrue

Défis rencontrés

Perspectives d'avenir

Origines et développement de l'IA

Débuts modestes de l'IA

- Initialement un rêve de la science-fiction
- Évolution vers des systèmes sophistiqués

Avancées technologiques

- Réalité tangible de l'IA
- Traitement de volumes massifs de données
- Précision impressionnante

Comment l'IA détecte les courriels indésirables

Techniques utilisées par l'IA

- Apprentissage machine
- Traitement du langage naturel

Analyse des caractéristiques des courriels

- Contenu des courriels
- Adresses de l'expéditeur
- Modèles de comportement

Identification des courriels suspects

- Algorithmes de détection

Amélioration continue des modèles

- Grâce à l'apprentissage automatique
- Efficacité accrue de l'IA

Avantages de l'utilisation de l'IA

Gestion efficace des courriels

- Réduction du temps nécessaire pour trier les courriels indésirables
- Moins d'efforts pour gérer les courriels

Adaptation rapide aux nouvelles menaces

- Amélioration de la sécurité des systèmes de communication

Défis de l'IA dans la détection des courriels indésirables

- Développement constant de nouvelles techniques par les cybercriminels
 - Contournement des systèmes de détection
 - Nécessité de mise à jour continue des algorithmes
- Préoccupations concernant la confidentialité
 - Sécurité des données traitées par l'IA



Perspectives d'avenir

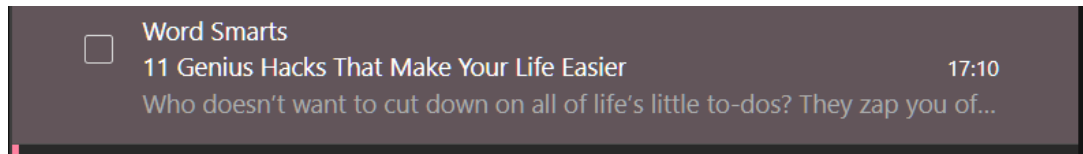
- Évolution des technologies
 - Amélioration continue des performances de l'IA
 - Intégration accrue dans les systèmes de sécurité et de communication
- Collaborations essentielles
 - Entre chercheurs, entreprises et gouvernements
 - Maximisation des avantages de l'IA
 - Minimisation des risques associés

Conclusion



- Présentation du 7 mai pour le CIVBDL
 - Thème: IA et son pouvoir de déceler les courriels indésirables
- Capacités impressionnantes de l'IA
 - Gestion efficace des courriels indésirables
- Objectifs de la présentation
 - Offrir des insights précieux
 - Inspirer l'intégration des technologies IA

Procédure à suivre pour tester un courriel légitime



Accéder à la boîte de messagerie

- Choisir un courriel légitime

Utiliser le menu contextuel

- Clic droit sur le courriel
- Menu contextuel apparaît

Afficher la source du message

- Glisser la souris sans cliquer
- Cliquer sur "Afficher la source du message"

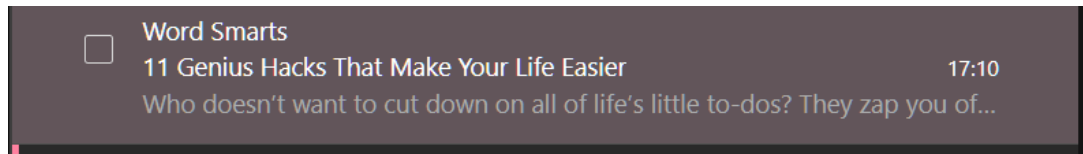
Copier la source du message

- Utiliser "CTRL+A" pour copier
- Assurer que le copié est complet

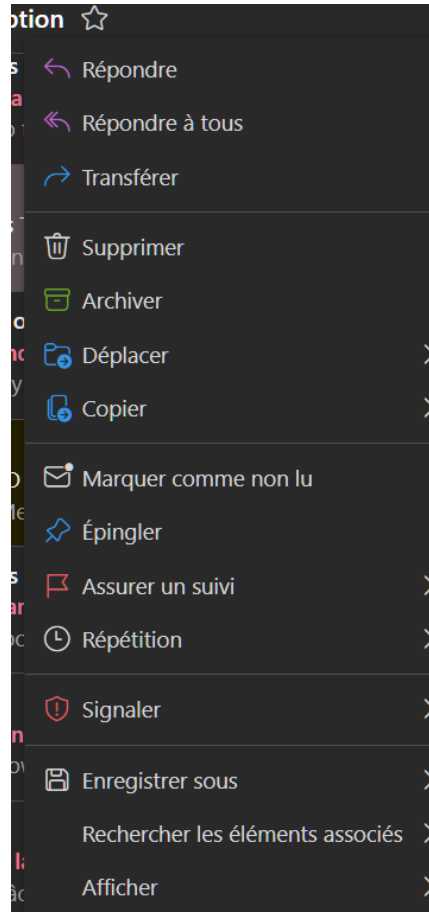
Analyser avec ChatGPT

Test #1 avec un courriel légitime

- Test #1 avec un courriel légitime
 - Accéder à une boîte de messagerie
 - Utiliser l'IA pour identifier les courriels indésirables



Menu contextuel et source du message



- Clic droit sur le courriel
 - Menu contextuel apparaît
- Allez au bas jusqu'à "Afficher"
 - Glisser la souris sans cliquer de gauche vers la droite
- Cliquer du gauche sur "Afficher la source du message"
 - La "Source du message" s'ouvre

Copier le message et utiliser ChatGPT

Source du message

```
Received: by 2002:ac0:fd82:0:b0:351:75fb:d752 with SMTP id g2csp6374552imy;  
Mon, 28 Apr 2025 14:10:52 -0700 (PDT) [redacted]  
Received: from mta-70-5-127.sparkpostmail.com (mta-70-5-127.sparkpostmail.com. [156.70.5.127])  
by mx.google.com with ESMTPS id 3f1490d57ef6-e7303e1a67bsi9493318276.205.2025.04.28.14.10.52  
for <michel.cloutier27@gmail.com> [redacted]
```

- Accéder à votre compte IA
 - Utiliser ChatGPT version o3
- Écrire la requête
 - Demander à l'IA de confirmer la légitimité du courriel
- Copier le message complet
 - Utiliser le raccourci clavier CTRL+A
- Séance sur la détection des courriels frauduleux
 - Analyse des entêtes
 - Détection de liens piégés
 - Apprentissage automatique des tactiques d'hameçonnage
- Séance adaptée aux aînés
 - Offerte par le CIVBDL

Source du message

Received: from SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) by MN2PR01MB5837.prod.exchangelabs.com with HTTPS; Mon, 28 Apr 2025 16:16:24 +0000 [REDACTED]

Received: from SJ0PR05CA0111.namprd05.prod.outlook.com (2603:10b6:a03:334::26) by SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8678.29; Mon, 28 Apr 2025 16:16:23 +0000 [REDACTED]

Source du message

Received: from SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) by MN2PR01MB5837.prod.exchangelabs.com with HTTPS; Mon, 28 Apr 2025 16:16:24 +0000 [REDACTED]

Received: from SJ0PR05CA0111.namprd05.prod.outlook.com (2603:10b6:a03:334::26) by SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8678.29; Mon, 28 Apr 2025 16:16:23 +0000 [REDACTED]

Source du message

Received: from SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) by MN2PR01MB5837.prod.exchangelabs.com with HTTPS; Mon, 28 Apr 2025 16:16:24 +0000 [REDACTED]

Received: from SJ0PR05CA0111.namprd05.prod.outlook.com (2603:10b6:a03:334::26) by SA6PR01MB8830.prod.exchangelabs.com (2603:10b6:806:433::15) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8678.29; Mon, 28 Apr 2025 16:16:23 +0000 [REDACTED]

```
--> </td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> </tr> <!--  
- Footer TEST Ends --> </table> </tr> </table> </center>=20  
<img border=3D"0" width=3D"1" height=3D"1" alt=3D"" src=3D"http://sp.malwar=  
ebytes.com/q/IBKQVjwp-ECLk3DIIm5Rx9g~~~/AARGbBA~/61aC3hsVkP1_BJ_PXgBb1UJTJRhT=  
FqJvcVG8NcD0L9SkjljLGRIKdvjrJ1Holtbh0DZ6As9iCqWA6zb6ST-1Q~~~">  
</body> </html> =  
  
--_-----T36VHiow7LqJC7LAfTrCdQ===_21/D5-31481-6D9AF086--
```

Fermer

```
--> </td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> </tr> <!--  
- Footer TEST Ends --> </table> </tr> </table> </center>=20  
<img border=3D"0" width=3D"1" height=3D"1" alt=3D"" src=3D"http://sp.malwar=  
ebytes.com/q/IBKQVjwp-ECLk3DIIm5Rx9g~~~/AARGbBA~/61aC3hsVkP1_BJ_PXgBb1UJTJRhT=  
FqJvcVG8NcD0L9SkjljLGRIKdvjrJ1Holtbh0DZ6As9iCqWA6zb6ST-1Q~~~">  
</body> </html> =  
  
--_-----T36VHiow7LqJC7LAfTrCdQ===_21/D5-31481-6D9AF086--
```

Fermer

Réponse de ChatGPT



- Réception quotidienne de l'infolettre
 - Courriel légitime
 - Information personnelle
- Réponse de ChatGPT
 - Verdict rapide
 - Infolettre marketing légitime
 - Pas un courriel d'hameçonnage
 - Publicité
 - Option de désabonnement

Conseils pratiques

- Survoler les liens sans cliquer
 - Vérifier que l'URL reste dans le domaine annoncé
- Désabonnement sans risque
 - Utiliser le lien “Unsubscribe” plutôt que de répondre au message
- Filtrer automatiquement
 - Dans Gmail, utiliser Filtre > Supprimer ou Archiver pour ne plus voir ces courriels
- Rester prudent
 - Les liens traquent vos clics pour le marketing
 - Ouvrez-les seulement si le contenu vous intéresse vraiment

Synthèse pour affichage au club



- Infolettre de Word Smarts
 - Sécuritaire mais publicitaire
- SPF et plateforme d'envoi vérifiés
 - Assurez-vous de la sécurité des envois
- Actions recommandées
 - Cliquer ou se désabonner sans danger
 - Ne jamais partager d'informations personnelles en réponse
- Remerciements
 - Merci, j'apprécie. Michel

Évaluation des données du message

Indice vérifié	Ce que j'ai vu	Signification
Domaine expéditeur	wordsmarts.com ; contenu du site = blogue linguistique Word Smarts	Le domaine existe vraiment et correspond au thème de l'infolettre
Plateforme d'envoi	IP 156.70.5.127 = SparkPost (service pro) Fournisseur de Données IP Fiables	Les grandes marques utilisent SparkPost pour leurs envois bulk
SPF	received-spf: pass	Gmail a confirmé que SparkPost était autorisé à envoyer pour wordsmarts.com
Lien de désabonnement	En-tête List-Unsubscribe: présent	Exigé par la loi ; signe de mailing légitime
Contenu	Sujet "11 Genius Hacks...", images hébergées sur le même domaine, aucun formulaire de connexion bancaire	Typique d'un bulletin lifestyle, pas de demande de mot de passe









Procédure à suivre pour tester un courriel indésirable

- Identification des courriels frauduleux
 - Courriel qualifié comme indésirable par Gmail
 - Message frauduleux (hameçonnage / pourriel)
- Actions à entreprendre
 - Supprimer le courriel
 - Ne pas répondre, télécharger ni ouvrir de pièce jointe
 - Ne pas cliquer sur les liens
 - Signaler le message comme indésirable dans Gmail
- Conseils pour la prochaine fois
 - Vérifier le domaine après le @
 - Survoler les liens avec la souris
 - Se méfier des cadeaux ou urgences inattendus

#	Élément	Pourquoi c'est suspect
1	Adresse "De" : nepasrepondreGextoAJl@wPApO.wPApO.com prétendant être Tim Hortons	Le domaine n'a aucun lien avec timhortons.ca ou timhortons.com.
2	Serveur expéditeur : IP 188.245.160.181 (hébergeur allemand, Hetzner)	Une chaîne légitime de Tim Hortons devrait passer par des serveurs canadiens ou une plateforme marketing reconnue (ex. Salesforce, Mailchimp).
3	Objet : « Yeti ramblar : ready for shipping, confirm now! »	Tim Hortons n'offre pas de gourdes Yeti ; l'urgence d'« agir maintenant » est typique du hameçonnage.
4	Aucun enregistrement DKIM/DMARC valable	Les e-mails commerciaux légitimes signent presque toujours leurs messages.
5	Corps du message : codé entièrement en Base64, HTML surchargé de CSS et de texte fourre-tout	Technique classique pour masquer le vrai contenu aux filtres anti-spam et attirer l'attention avec un visuel tape-à-l'œil.
6	Liens masqués : redirigent vers storage.googleapis.com/.../hamsrefly.html puis probablement vers un autre domaine douteux	Les marques utilisent leurs propres noms de domaine ou ceux de partenaires connus, jamais une URL d'hébergement anonyme.

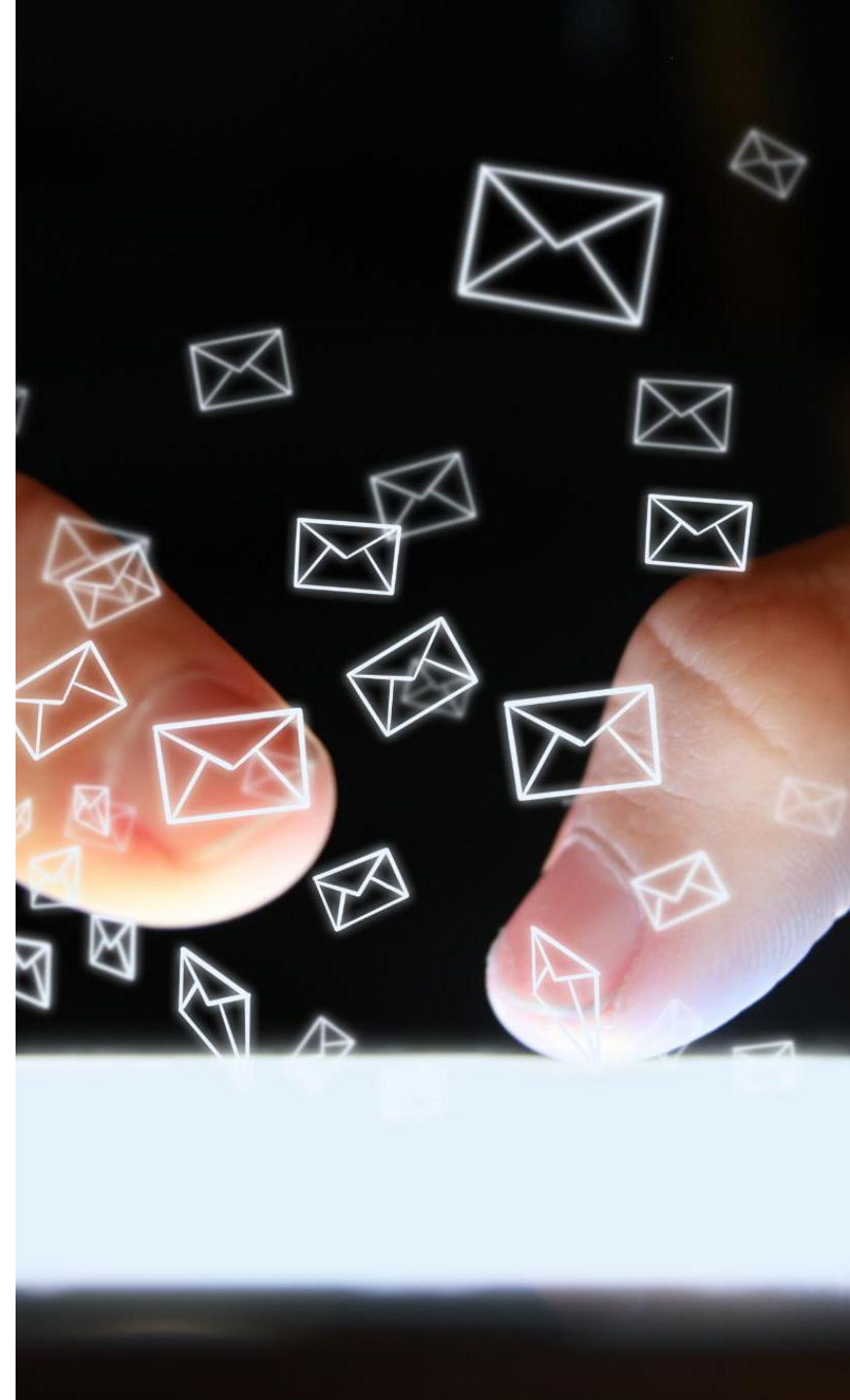
Gabarit pour vérifier si un courriel est légitime

- Usage du guide
 - Imprimez ou projetez pendant les ateliers
 - Police suggérée : Arial 14 pt minimum
 - Contraste élevé : texte noir sur fond blanc ou jaune pâle
- Astuce accessibilité
 - Agrandir les emojis
 - Remplacer par de grandes icônes si nécessaire

Étape	Pictogramme	Question à se poser	Action conseillée
1. Expéditeur		Reconnaissez-vous la personne ou l'entreprise ?	Si NON → méfiance
2. Domaine du courriel		L'adresse se termine-t-elle par le vrai site (ex. @timhortons.com) ?	Si NON → probablement frauduleux
3. Objet / Urgence		Promet-on un cadeau ou demande-t-on d'agir « maintenant » ?	Urgence = drapeau rouge
4. Liens		En survol, l'URL pointe-t-elle vers le même domaine légitime ?	Si NON → ne cliquez pas
5. Pièces jointes		Attachement inattendu ? (PDF, ZIP, DOCX, etc.)	Ne pas ouvrir sans confirmer l'origine
6. Orthographe et mise en page		Fautes, traduction approximative, images floues ?	Qualité basse = suspect
7. Signatures DKIM / DMARC (avancé)		Le courriel est-il marqué « signé » ou « authentifié » ?	Absent = méfiance
8. Verdict		Au moins 2 signaux rouges ?	Supprimer & signaler indésirable

Modèle de conversation sécuritaire

- Introduction
 - Salutation formelle
 - Nom du contact
- Contenu du courriel
 - Réception du courriel
 - Authenticité du courriel
- Demande de confirmation
 - Avant ouverture
 - Merci

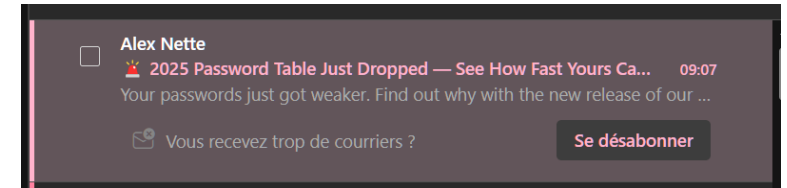


Ressources utiles



Étude de courriel reçu dans ma boîte de messagerie

- Vérification de la légitimité du courriel
 - Provenance de l'email: alex.nette@hivesystems.com
 - Contenu: Table de mots de passe
- Recherche sur Hive Systems
 - Publication annuelle de la table de mots de passe
 - PDG: Alex Nette
- Analyse des en-têtes
 - SPF valide
 - Domaine légitime
- Éléments suspects
 - Objet codé
- Conclusion



Réponse de ChatGPT

Provenance de l'e-mail

- Expéditeur: alex.nette@hivesystems.com
- Sujet: Table de mots de passe

Vérification de la légitimité

- Recherche sur Hive Systems
- Confirmation de la publication de la table

Analyse des éléments suspects

- Liens de suivi
- Objet codé
- Informations de délivrabilité (SPF, DKIM)

Conclusion

- Campagne marketing légitime

Redirections et pistage

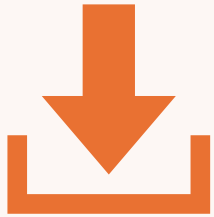
Liens traçants générés par HubSpot

- URLs hs-NNNNNNN.na1.hubspotlinks.com
- Redirigent vers le vrai site de Hive Systems

Objet encodé en UTF-8 avec emoji

- Pratique courante pour le marketing
- Pas un signe de fraude en soi

Contenu et légitimité



Annonce de la parution de la Password Table 2025

Message pointe vers la page de téléchargement publique

Site officiel de Hive Systems



Absence de pièces jointes exécutables

Pas de demande d'information sensible

Risque de malware très faible

Risques résiduels

Pistage

- Ouverture et clics enregistrés par HubSpot
- Référence : HubSpot Knowledge Base

Pression marketing

- Appels à l'action cliquables pouvant être confondus avec une urgence
- Signal classique d'hameçonnage
- Référence : Canadian Centre for Cyber Security, Get Cyber Safe

Habitude

- Courriel légitime reprenant certains codes du phishing
- Utilisation d'emoji et de gros boutons
- Importance de rester vigilant
- Référence : Canadian Centre for Cyber Security, Get Cyber Safe

Conseils pratiques pour le CIVBDL

Ouvrez seulement si le sujet vous intéresse

- Formation cybersécurité

Téléchargez la table via le site principal

- Utilisez <https://www.hivesystems.com/password-table>
- Évitez les liens redirigés

Désinscrivez-vous si nécessaire

- Utilisez l'en-tête List-Unsubscribe

Sensibilisez vos membres

- Les courriels légitimes peuvent ressembler à des tentatives d'hameçonnage
- Vérifiez domaine, orthographe et liens avant de cliquer

Tableau récapitulatif

Élément vérifié	Verdict	Commentaire rapide
Domaine expéditeur	✅ Valide	hivesystems.com autorisé
SPF/DKIM/DMA RC	✅ Pass	Authenticité confirmée
Liens	⚠️ Traçants	Redirection HubSpot
Contenu	✅ Informatif	Pas de pièce jointe malveillante
Action suggérée	🤔 Facultative	Ouvrir si utile ; sinon, désinscrire

- Message légitime mais promotionnel
 - Peut être conservé pour vos ateliers
 - Option de se désabonner pour alléger votre boîte

Recherche sur Internet



- Recherche sur Internet terminée
 - Hive Systems 2025 Password Table
 - Alex Nette Hive Systems CEO
- Analyse technique des entêtes
 - Authentification
- Les défis de l'IA
 - Détection des courriels indésirables

Analyse d'un courriel suspect

Élément	Signe de phishing ?	Détail
Lien Glitch.me	Oui	Plateforme détournée pour le phishing
Message urgent	Oui	« 24 heures pour agir »
Expéditeur usurpé	Oui	SPF softfail, IP inconnues
Signature générique	Oui	« Administrator Services »
Personnalisation absente	Oui	Aucun nom, message générique

- Résumé du courriel reçu
 - Objet : Mailbox Update Request
 - Expéditeur : info@civbdl.org
 - Contenu : Demande urgente de mise à jour de la boîte aux lettres
- Éléments suspects détectés
 - Lien vers la plateforme Glitch
 - Pression et urgence
 - Origine technique douteuse
 - Formulation générique et signature vague
- Risque associé
- Conclusion et recommandation
- Conseils complémentaires



info@civbdl.org

Mailbox Update Request

18:00

Dear info@civbdl.org, You have an important mailbox update, please click ...

Requête de MC

- Expertise en analyse de courriel indésirable
 - Évaluation des courriels potentiellement dangereux
- Courriel joint à analyser
 - Contenu du courriel jugé "questionnable"
- Source du message
 - Origine du courriel à examiner
- Perspectives d'avenir
 - Implications futures de l'analyse

Réponse de Perplexity

- Résumé du courriel reçu
 - Objet : Mailbox Update Request
 - Expéditeur : info@civbdl.org
 - Contenu : Demande urgente de mise à jour de la boîte aux lettres
 - Lien proposé : <https://plume-grape-fish.glitch.me/?email=info@civbdl.org>
- Éléments suspects détectés
 - Lien vers la plateforme Glitch
 - Pression et urgence
 - Origine technique douteuse
- Risque associé
- Conclusion et recommandation
- Conseils complémentaires



Résumé visuel

Élément	Signe de phishing ?	Détail
Lien Glitch.me	Oui	Plateforme détournée pour le phishing
Message urgent	Oui	« 24 heures pour agir »
Expéditeur usurpé	Oui	SPF softfail, IP inconnues
Signature générique	Oui	« Administrator Services »
Personnalisation absente	Oui	Aucun nom, message générique

Fiche pédagogique pour sensibiliser aux dangers du phishing

- Expéditeur usurpé
 - Le courriel semble provenir de votre propre adresse
 - Envoyé depuis des serveurs externes non autorisés
 - Technique courante dans les attaques de phishing
- Lien suspect
 - Redirige vers un site hébergé sur Glitch
 - Glitch est légitime mais exploité par des cybercriminels
- Pression temporelle
 - Indique que vous avez 24 heures pour effectuer une mise à jour
 - Tactique pour inciter à une action précipitée
- Authentification SPF échouée
- Recommandations

Indice suspect

Expéditeur inconnu ou usurpé

Liens vers des domaines non officiels

Messages urgents ou menaçants

Fautes d'orthographe ou de grammaire

Demandes d'informations personnelles

Pourquoi c'est inquiétant


Les cybercriminels peuvent falsifier l'adresse de l'expéditeur pour paraître légitimes.

Les liens peuvent rediriger vers des sites malveillants conçus pour voler vos informations.


Créer un sentiment d'urgence pousse à agir sans réfléchir.


Les courriels frauduleux contiennent souvent des erreurs linguistiques.

Les entreprises légitimes ne demandent jamais de données sensibles par courriel.




Analyse technique du courriel



- Expéditeur usurpé
 - Le courriel semble provenir de `info@civbdl.org`
 - Envoyé depuis des serveurs externes non autorisés (`bellnet-ca.site`)
 - Adresse IP : 188.127.251.196
 - Lien suspect
 - Redirection vers un site hébergé sur Glitch
 - Utilisation de Glitch par des cybercriminels
 - Pression temporelle
 - Message indiquant 24 heures pour une mise à jour
 - Tactique pour inciter à une action précipitée
 - Authentification SPF échouée
 - Champ `received-spf`: softfail
- 





Recommandations

- Ne cliquez pas sur le lien contenu dans le courriel
 - Évitez d'ouvrir des liens non vérifiés
 - Ne répondez pas au message
 - Ignorer les courriels suspects
 - Supprimez immédiatement le courriel de votre boîte de réception
 - Éliminez les courriels potentiellement dangereux
 - Signalez l'incident à votre fournisseur de services de messagerie ou à l'administrateur de votre domaine
 - Permettre des mesures appropriées
- 

Proposition de fiche pédagogique

- Importance de la sensibilisation au phishing
 - Protéger les membres du Club Informatique
 - Réduire les risques de cyberattaques
- Exemples concrets de phishing
 - Emails frauduleux
 - Sites web trompeurs
- Mesures de prévention
 - Vérification des sources
 - Utilisation de logiciels de sécurité
- Rôle du CIVBDL
 - Formation des membres
 - Partage d'informations

Conseils pour reconnaître les tentatives de phishing

 Indice suspect	 Pourquoi c'est inquiétant
Expéditeur inconnu ou usurpé	Les cybercriminels peuvent falsifier l'adresse de l'expéditeur pour paraître légitimes.
Liens vers des domaines non officiels	Les liens peuvent rediriger vers des sites malveillants conçus pour voler vos informations.
Messages urgents ou menaçants	Créer un sentiment d'urgence pousse à agir sans réfléchir.
Fautes d'orthographe ou de grammaire	Les courriels frauduleux contiennent souvent des erreurs linguistiques.
Demandes d'informations personnelles	Les entreprises légitimes ne demandent jamais de données sensibles par courriel.



Atelier pratique pour le CIVBDL

- Briseglase (5 min)
 - Montrez deux courriels projetés : un légitime, un piégé
 - Demandez au public de lever la main quand ils voient un drapeau rouge
- Minicours guidé (15 min)
 - Parcourez la fiche à l'écran
 - Chaque point de la checklist express est illustré d'un exemple réel
 - Insistez sur l'inspection des entêtes (démonstration Outlook & Gmail)
- Exercices pratiques (15 min)
 - Distribuez 6 courriels imprimés ou en PDF : trois sains, trois malveillants
 - Les équipes cochent les 10 questions de la fiche pour chaque message
 - Comparez les scores
- Débrief + ressources locales (10 min)

Formation suivie

Séance	Contenu clé	Devoir
#1 – Anatomie d'un courriel	Domaines, entêtes, SPF/DKIM/DMARC	Analyser un vrai message reçu et noter 3 indices de légitimité
#2 – Scénarios d'attaque & riposte	Phishing, malware via pièces jointes, faux formulaires	Faire le quiz Google + signaler un spam réel dans Outlook/Gmail

Pourquoi ces bonnes pratiques ?

- Fraude canadienne
 - L'hameçonnage est la principale menace signalée
 - Pertes de plus de 165 millions CAD en 2023
- Signes d'urgence et fautes linguistiques
 - Figurent parmi les 7 signaux listés par PensezCybersecurite.ca
 - <https://www.pensezcybersecurite.gc.ca/fr>
 - <https://www.pensezcybersecurite.gc.ca/fr/ressources>
- Survoler les liens avant de cliquer
- Afficher l'original dans Gmail
- Importance de lire l'entête complet
- Tonalité alarmiste
- La récente "**Campagne frauduleuse usurpant l'identité de la NAB (Banque Nationale Australienne)**« , montre que les cybercriminels adaptent leurs logos et couleurs pour tromper les filtres visuels
- Vérification des domaines internationalisés
- 91% des intrusions démarrent par un courriel piégé

Prochaine étape

- Exemples additionnels
 - Intégration dans les exercices
- Version PowerPoint clé en main
 - Facilité d'utilisation
- Quiz en ligne autocorrigé
 - Pour les membres
- Assistance disponible
 - Peaufiner la fiche
 - Préparer le matériel pédagogique

#	Question à se poser	Pourquoi c'est important
1	L'expéditeur correspond-il à une adresse connue & orthographiée correctement ?	Les fraudeurs imitent les domaines (ex. rnicrosoft.com)
2	Le sujet crée-t-il un sentiment d'urgence ou de peur ?	La pression pousse à cliquer sans réfléchir
3	Y a-t-il des fautes inhabituelles ou un français approximatif ?	Souvent signe d'un courriel automatisé malveillant
4	Les liens pointent-ils vraiment vers le domaine annoncé ? (survoler avant de cliquer)	La plupart des attaques redirigent vers un site usurpé
5	Une pièce jointe inattendue ? (ZIP, DOCM, ISO, HTML)	Les malwares se cachent dans les pièces jointes
6	Le message réclame des infos sensibles (Mdp, N° carte, NAS) ?	Une entreprise légitime ne le demande jamais par courriel
7	Votre nom est-il correctement utilisé ?	Les envois massifs utilisent « Cher client »
8	Le courriel passe-t-il l'authentification SPF/DKIM/DMARC ?*	Voir section 3 pour vérifier dans l'entête
9	Le certificat (https://) du site cible est-il valide ?	Pas de cadenas = danger (mais cadenas ≠ sécurité absolue)
10	Avez-vous un doute ? => Ne cliquez pas, signalez et supprimez.	
*Astuce : O365 affiche une coche verte ou un bouclier « via » lorsqu'un domaine est authentifié.		

Fiche-mémo pour reconnaître un courriel légitime vs. malveillant

- Checklist express « Ouvrir en paix »
 - Comment afficher et lire les entêtes
- Comprendre SPF / DKIM / DMARC
 - SPF : liste d'adresses IP autorisées
 - DKIM : signature numérique ajoutée
 - DMARC : règle pour gérer les échecs
- Bons réflexes
 - Survoler sans cliquer les liens
 - Scanner les pièces jointes douteuses
 - Signaler les pourriels
- Outils gratuits à connaître
 - Ressources locales (QC & CA)

Afficher et lire les entêtes



- Outlook (Web ou App)
 - Clic droit sur le message
 - Afficher la source
 - Recherchez Received-SPF, AuthenticationResults
- Gmail
 - : Afficher l'original
 - Google calcule SPF, DKIM & DMARC en haut
 - Repérez spf=pass, dkim=pass, dmarc=pass : bonne nouvelle !
 - Fail ou softfail : méfiance accrue

Comprendre SPF/DKIM/DMARC

- SPF (Sender Policy Framework)
 - Liste d'adresses IP autorisées à envoyer au nom du domaine
- DKIM (DomainKeys Identified Mail)
 - Signature numérique ajoutée au message par le domaine
- DMARC (Domain-based Message Authentication, Reporting & Conformance)
 - Règle qui détermine quoi faire quand SPF ou DKIM échoue
 - Actions possibles: quarantaine, rejet



Bons réflexes

- Survoler les liens sans cliquer
 - Outlook : floutez la souris
 - Mobile : appuyez longuement
- Numériser les pièces jointes douteuses
 - Utiliser VirusTotal
 - Utiliser votre antivirus (AV)
- Signaler les pourriels
 - Outlook : bouton Signaler comme hameçonnage
 - Gmail : : Signaler le phishing
- Supprimer ou déplacer dans Indésirable

Ressources locales

- GetCyberSafe
 - Reconnaître l'hameçonnage
- Gouvernement du Québec
 - Capsule « Courriels d'apparence officielle »
- Centre antifraude du Canada
 - Numéro de contact:
18884958501



Checklist express

#	Question à se poser	Pourquoi c'est important
1	L'expéditeur correspond-il à une adresse connue & orthographiée correctement ?	Les fraudeurs imitent les domaines (ex. rnicrosoft.com)
2	Le sujet crée-t-il un sentiment d'urgence ou de peur ?	La pression pousse à cliquer sans réfléchir
3	Y a-t-il des fautes inhabituelles ou un français approximatif ?	Souvent signe d'un courriel automatisé malveillant
4	Les liens pointent-ils vraiment vers le domaine annoncé ? (survoler avant de cliquer)	La plupart des attaques redirigent vers un site usurpé
5	Une pièce jointe inattendue ? (ZIP, DOCM, ISO, HTML)	Les malwares se cachent dans les pièces jointes
6	Le message réclame des infos sensibles (Mdp, N° carte, NAS) ?	Une entreprise légitime ne le demande jamais par courriel
7	Votre nom est-il correctement utilisé ?	Les envois massifs utilisent « Cher client »
8	Le courriel passe-t-il l'authentification SPF/DKIM/DMARC ?*	Voir section 3 pour vérifier dans l'entête
9	Le certificat (https://) du site cible est-il valide ?	Pas de cadenas = danger (mais cadenas ≠ sécurité absolue)
10	Avez-vous un doute ? => Ne cliquez pas, signalez et supprimez.	
*Astuce : O365 affiche une coche verte ou un bouclier « via » lorsqu'un domaine est authentifié.		

Rappel



- En cas de doute
 - Mieux vaut supprimer que cliquer
 - Partagez cette fiche-mémo
 - Au sein du CIVBDL
 - Remerciements
 - Merci de la part des membres et des collaborateurs du CIVBDL
 - Nous apprécions le partage
 - Michel Cloutier
 - Présentation sur Zoom:
 - 20250507
- C'est ensemble qu'on avance