# L'HISTOIRE DE L'HAMEÇONNAGE

L'hameçonnage est une stratégie utilisée fréquemment par les cybercriminels pour voler vos renseignements personnels et financiers. Ils utilisent l'hameçonnage depuis l'arrivée d'**internet** dans les années 1990 et leurs méthodes se sont beaucoup raffinées au fil des années.

**Voici un bref survol de l'évolution des** campagnes d'hameçonnage **dans le temps :**

## ANNÉES 1990

Si l'hameçonnage existait déjà à cette époque, la toute première attaque répertoriée a eu lieu sur **America Online Inc. (AOL).** Les pirates tentaient de voler les renseignements de connexion et les données personnelles d'utilisateurs d'AOL dans le but de les revendre.

**Chaque jour,**

**6,4 milliards de courriels d'hameçonnage sont envoyés dans le monde**[i]

**1996**

Un groupe nommé AOHell crée le terme « hameçonnage »

# ANNÉES 2000

## 2001

Le développement du commerce en ligne incite les cybercriminels à créer de **faux sites Web** qui imitent des sites Web de compagnies populaires comme eBay et PayPal.

## 2004

Les pirates commencent à utiliser des fenêtres contextuelles pour tenter de s'emparer des renseignements sensibles des internautes insouciants. Des techniques comme **le harponnage** et l'enregistreur de frappes apparaissent.

## 2008

Création du Bitcoin et des cryptomonnaies. Cela favorise la création de maliciels, car les cybercriminels peuvent alors plus facilement convertir en toute impunité (et anonymement) les paiements que leur font parvenir leurs victimes.

[redacted]

[redacted]

[redacted]

[redacted]

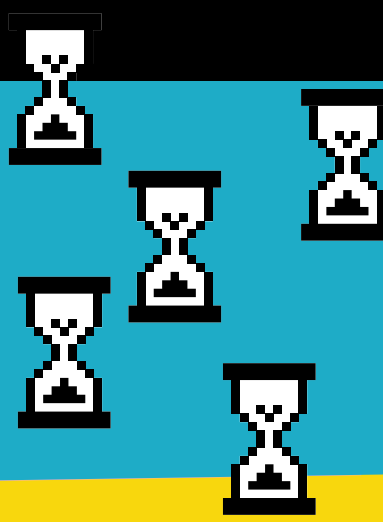
FAIT

**Environ 929 millions de dollars sont volés en raison de l'hameçonnage en 2004-2005.**[ii]

# ANNÉES 2010

## 2013

L'hameçonnage devient la technique préférée pour propager des rançongiciels.

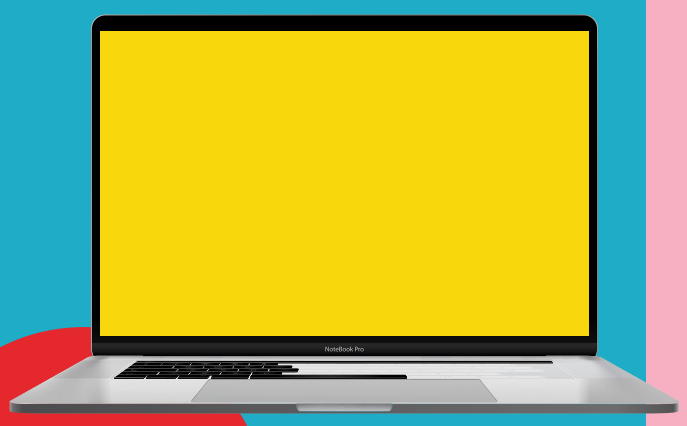


## 2017

Les pirates adoptent le protocole HTTPS pour leurs faux sites Web.

## 2018

Les cybercriminels commencent à cacher des codes malicieux dans des fichiers d'images pour contourner les logiciels antivirus des internautes.



## 2019

Avec les fausses cartes cadeaux, les campagnes d'hameçonnage deviennent plus sophistiquées en offrant des cadeaux aux victimes potentielles. Dans leurs tentatives d'hameçonnage, les cybercriminels commencent aussi à menacer leurs victimes de poursuites judiciaires ou d'emprisonnement si elles ne leur envoient pas des cartes cadeaux ou des Bitcoins.

## FAIT

**En 2018,**
85 % des Canadiens
**disaient avoir reçu un courriel d'hameçonnage.**[iii]

# ANNÉES 2020

Les courriels et appels d'hameçonnage se multiplient avec des campagnes hyperciblées qui visent le grand public et tentent d'exploiter des situations comme la COVID-19 ou des programmes comme la Prestation canadienne d'urgence (PCU). Les cybercriminels ciblent également les utilisateurs de divers services comme les services de diffusion en continu et les réseaux sociaux.

**3 SUR 10**

proportion d'organisations canadiennes qui ont vu une augmentation du nombre de cyberattaques les ciblant durant la pandémie.[iv]

Les campagnes d'hameçonnage peuvent être difficiles à reconnaître, car les cybercriminels sont devenus des experts pour tromper leurs victimes et les amener à dévoiler leurs renseignements personnels.

## VOUS POUVEZ ÉVITER DE DEVENIR VICTIME D'HAMEÇONNAGE EN SUIVANT LES CONSEILS SUIVANTS :

- Réfléchissez quelques minutes avant de répondre
- Ne cliquez jamais sur des liens ou des fichiers joints suspects
- Surveillez les fautes d'orthographe ou les caractères étonnants dans les adresses de courriel
- Surveillez les erreurs grammaticales
- Veillez contre le formatage déficient
- Tentez de communiquer avec l'expéditeur en utilisant un autre moyen que le message reçu pour vous assurer qu'il est bien légitime

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

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada


i. Valimail, 2018 Email Fraud Landscape, 2018
ii. History of Phishing, KnowBe4, 2021
iii. Sécurité Internet au Canada, Printemps, L'Autorité canadienne pour les enregistrements Internet (CIRA), 2018
iv. Rapport sur la cybersécurité de 2020 de l'ACEI, L'Autorité canadienne pour les enregistrements Internet (CIRA), 2020



Numero de catalogue : D96-69/2021F-PDF | ISBN : 978-0-660-39742-9