Les spams et l'hameçonnage

...Ou comment repérer en trois regards un message qui cherche à vous faire payer ou à vous voler vos informations.

Guide d'après les supports de cours « Les spams » et « Les arnaques » de l'atelier Part'âges numériques.

- Un spam, c'est quoi ?
- Quand le spam devient dangereux
- Comment reconnaître un faux ?
- Que faire ?
- Pour s'entraîner

Un spam, c'est quoi ?

Un **spam** est un message électronique, souvent publicitaire, envoyé **de façon répétée** à un grand nombre de personnes **sans leur accord**.

Le tout premier spam date du **3 mai 1978** : un commercial de l'entreprise DEC invite environ 600 utilisateurs d'ARPANET (l'ancêtre d'Internet) à une démonstration, sans penser à mal. Les réactions furent vives.

> La grande majorité des spams est **inoffensive** : de la publicité. Ils vantent parfois des produits dont la vente est interdite en France (faux médicaments, produits de dopage, montres contrefaites, crédits...).

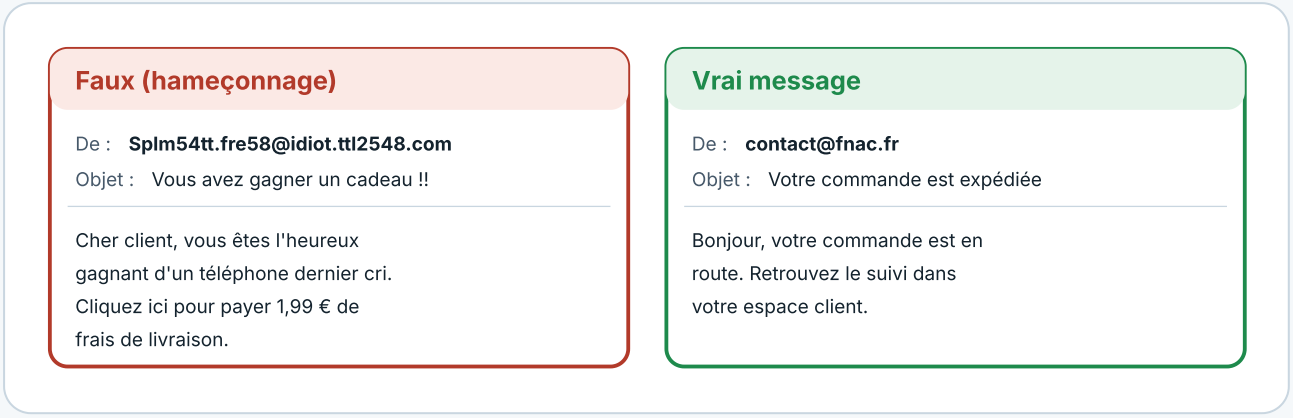
Quand le spam devient dangereux

Les spammeurs ne peuvent pas entrer directement dans votre ordinateur. Mais ils peuvent vous amener à **ouvrir une pièce jointe** contenant un logiciel malveillant, ou à vous connecter à un **faux site** qui ressemble à celui de votre banque ou de votre magasin préféré.

Cette technique s'appelle le **phishing**, ou **hameçonnage**.

> **L'arnaque n'a lieu que si vous sortez votre carte bancaire** ou que vous donnez vos codes. Tant que vous ne cliquez pas et ne payez pas, il ne se passe rien.

Comment reconnaître un faux ?



Posez-vous la question : *« La FNAC enverrait-elle un message avec des fautes aussi grossières ? »*



- **L'adresse de l'expéditeur** : un vrai message de la Fnac vient d'une adresse en `@fnac.fr`, jamais d'une suite de lettres et de chiffres incompréhensible.

- **Le nom de domaine** : un nom qui n'a rien à voir avec l'enseigne (par exemple un message « Carglass » qui renvoie vers un autre nom) est le signe d'une tentative de fraude.
- **Le réflexe** : on achète sur un site dont on connaît l'adresse exacte, qu'on tape soi-même ou qu'on a en favori.

Que faire ?

1. Ne cliquez sur **aucun lien** et n'ouvrez **aucune pièce jointe**.
2. Ne répondez pas.
3. Placez le message dans les **courriers indésirables** (Spam) ou supprimez-le.
4. En cas de doute, allez directement sur le site officiel en tapant son adresse.

> Voir aussi Les arnaques : SMS, téléphone, WhatsApp et Les noms de domaine.

Pour s'entraîner, à son rythme

1. Ouvrez le dossier « Courriers indésirables » de votre messagerie. Repérez l'adresse de deux expéditeurs.
2. Comparez : une adresse officielle d'un magasin et celle d'un faux message.
3. Expliquez à voix haute les trois paliers d'auto-détection.

À retenir

- Un spam est un message de masse envoyé sans accord.
- L'hameçonnage cherche à vous faire payer ou donner vos codes.
- On vérifie l'adresse de l'expéditeur, les fautes et le nom de domaine.
- Aucun clic, aucune pièce jointe : on supprime.

Petit lexique

Spam	Message de masse non sollicité.
Phishing	Hameçonnage : faux message imitant une enseigne.
Pièce jointe	Fichier joint à un courriel.
Expéditeur	Celui qui envoie le message.

Sources : support de cours de l'atelier Part'âges numériques (Niveau 1, « L'internet »).