

Une forme de spam : **l'hameçonnage** (ou « *phishing* », de l'anglais, terme dérivé de « *fishing* », la pêche à la ligne), consiste à tromper le destinataire en faisant passer un courriel pour un message de sa banque ou d'un quelconque service protégé par mot de passe. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe, un numéro de carte bancaire) en les attirant sur un site factice enregistrant toutes leurs actions.

De : Caisse.DEpargne@suit.net  
À : Recipients  
Cc :  
Objet : Mauvaise essai d'accès à votre compte

Bonjour cher Client Caisse d'Épargne,

---



**Cher client !**

Dans le cadre de nos mesures de sécurité, nous vérifions régulièrement l'activité de l'écran Caisse épargne. Nous avons demandé des informations à vous pour la raison suivante:

Notre système a détecté des charges inhabituelles à une carte de crédit liée à votre compte Caisse épargne.

**Numero de Reference: 259-187-991**

C'est le dernier rappel pour vous connecter à Caisse épargne, le plus tôt possible. Une fois que vous serez connecté, Caisse épargne vous fournira des mesures pour rétablir l'accès à votre compte.

La procédure est très simple:

1. Cliquez sur le lien ci-dessous pour ouvrir une fenêtre de navigateur sécurisée.
2. Confirmez que vous êtes le propriétaire du compte et suivez les instructions.

---

[Accédez à votre compte](#)

### Menez l'enquête :

- 1) le destinataire est-il clairement identifié ?
- 2) L'objet du courrier attire-t-il votre attention ? Faites un commentaire sur cet objet.
- 3) Le logo est-il authentique ?
- 4) Soulignez toutes les lettres du texte auxquelles il manque un accent. Faites le total des erreurs d'accent
- 5) Relevez deux tournures ou expressions incorrectes dans le texte. Proposez une version corrigée de ces expressions.
- 6) Quels conseils (au moins quatre) donneriez-vous pour éviter à vos proches de se faire piéger ? (aidez-vous des questions précédentes)