Apprenez **à reconnaître un email de phishing**

1 Émetteur suspect

Les cybercriminels ne manquent pas de techniques pour faire croire aux utilisateurs qu'un email est authentique. Vérifiez bien que le nom de domaine ne ressemble pas trop à un autre. Prenez garde lorsque vous lisez un email sur votre téléphone portable : le nom d'affichage est peut-être le seul visible, même si l'adresse email est bidon.

2 Objet et ton

Un langage attrayant, menaçant ou marqué par l'urgence est généralement utilisé pour encourager le destinataire à réagir immédiatement. Dans les attaques par phishing, éveiller la curiosité, la cupidité ou la peur est une tactique fréquente.

3 Salutations

Les hameçonneurs envoient souvent les emails à un grand nombre de destinataires pour collecter des informations. La salutation utilisée est donc générique. Les hameçonneurs avisés, eux, personnaliseront l'email en ajoutant un nom, une adresse email ou même un mot de passe piraté par exemple.

4 Erreurs

Lisez l'email avec attention. Si les erreurs de grammaire doivent évidemment vous alerter, les hackers chevronnés n'en commettent pas de flagrantes. Elles seront plus subtiles, comme l'absence d'espaces à certains endroits ou l'utilisation de symboles au lieu de mots. Dans certains cas, il n'y aura aucune erreur.

5 Liens

Avant de cliquer, passez la souris dessus pour faire apparaître l'URL et méfiez-vous des raccourcis de lien, comme Bitly ou TinyURL. Gardez bien en tête que les emails de phishing peuvent contenir des URL qui ne sont pas infectées en plus de l'URL de phishing pour piéger les utilisateurs et contourner les filtres d'emails.

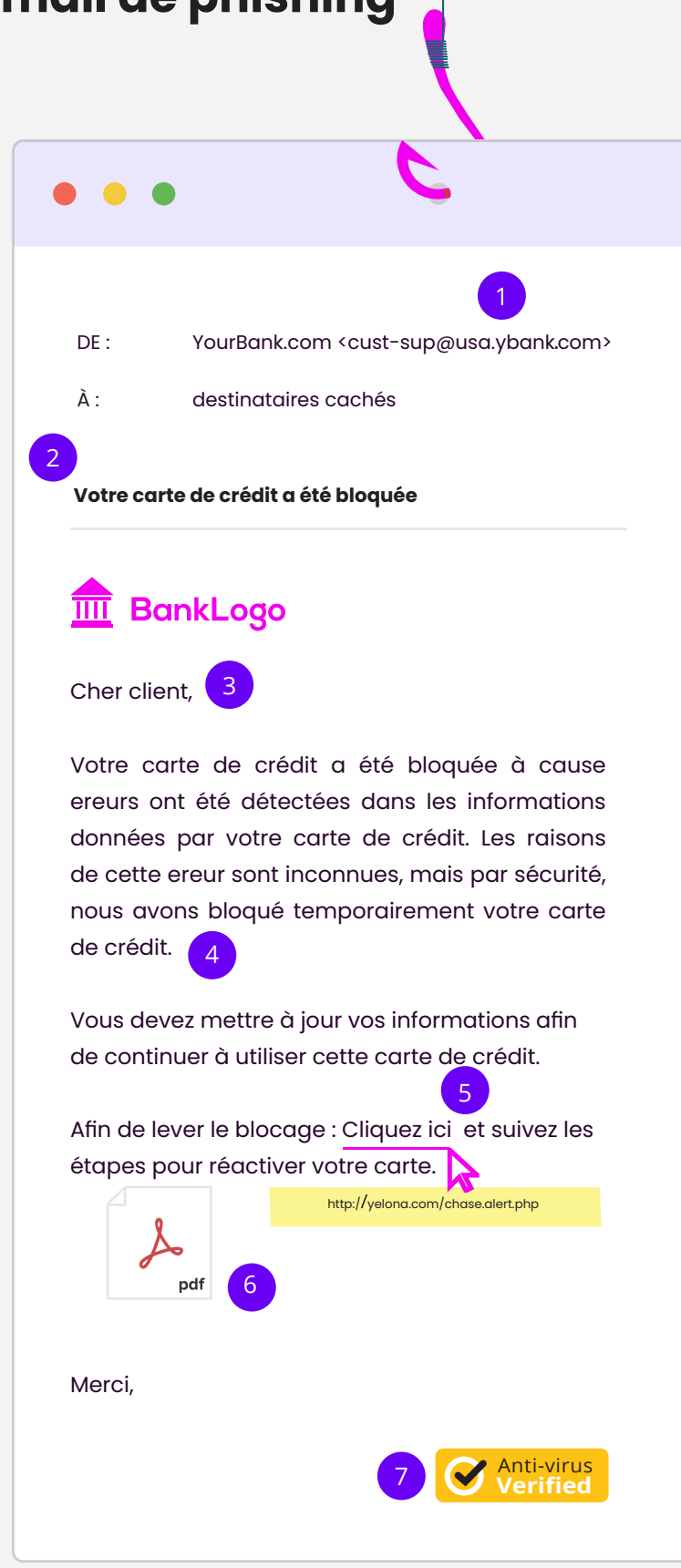
http://ignorethis.IMPORTANT_URL.com/doesn'tmatter

6 Pièces jointes

Faites attention aux emails contenant des pièces jointes. Le lien peut se trouver dans ces pièces jointes plutôt que dans le corps du mail afin de contourner les filtres d'email.

7 Images

Les cybercriminels peuvent facilement reproduire les logos, images et badges des marques dans leurs emails. Ils peuvent aussi créer des pages Internet qui ressemblent en tout point aux vraies. Pensez bien à tous les éléments mentionnés ci-dessus avant de vous décider à cliquer.



Jetez-y un œil en cas de doute.

IsItPhishing.AI est un outil gratuit qui analyse en temps réel l'URL et la page Internet pour voir s'il s'agit de phishing.