MASCOT
en Bourgogne-Franche-Comté

GUIDE DE BONNES PRATIQUES & SÉCURITÉ

Comment identifier les fausses réservations et vous protéger contre l'escroquerie et le piratage

Les hébergeurs touristiques sont régulièrement ciblés par des tentatives d'escroquerie ou de piratage informatique. Ces attaques prennent souvent la forme de **faux e-mails de réservation** ou de messages urgents simulant une demande de devis, un problème de paiement ou une confirmation.

Ce guide vous donne des réflexes simples pour identifier les pièges, vérifier l'authenticité des messages et savoir comment réagir.

Table des matières

Mission d'Accompagnement, de Soutien et de Conseil aux Offices de Tourisme
5 avenue Garibaldi • 21000 Dijon • Tél : 03.80.28.02.99
Email : contact@mascotbfc.com • Site web : www.mascotbfc.com
SIRET : 77819345800032

Avec le soutien financier du Conseil régional
RÉGION BOURGOGNE FRANCHE COMTÉ

1. Les typologies d'arnaques les plus fréquentes

➢ L'arnaque au sur paiement / faux virement (Chèque ou virement international) :

Un prétendu client réserve pour une longue période et propose un acompte ou un paiement direct. Il envoie un montant supérieur au montant demandé (souvent en prétextant une erreur ou des frais de transport/agence à régler) et vous demande de lui recréditer la différence par virement immédiat (PCS, Western Union, Wafacash, etc.). Quelques jours plus tard, le chèque initial revient impayé ou le virement d'origine est annulé.

➢ La pièce jointe piégée (Logiciel malveillant / Ransomware) :

L'e-mail contient une pièce jointe nommée *"Contrat_de_reservation.pdf.exe"*, *"Liste_des_voyageurs.zip"* ou un document Word demandant d'activer les macros. L'ouverture de ce fichier installe un virus capable de bloquer votre ordinateur ou d'intercepter vos mots de passe.

➢ L'hameçonnage (Phishing) de compte ou de plateforme :

Le message ressemble à s'y méprendre à un e-mail officiel (Booking, Airbnb, Abritel, votre banque, votre logiciel de gestion) vous informant d'un problème sur une réservation ou d'une mise à jour de compte. Le lien présent dans l'e-mail vous renvoie vers un faux site destiné à voler vos identifiants ou vos coordonnées bancaires.

➢ Le faux client étranger pressé (Ingénierie sociale) :

Le client prétexte être un professionnel, un diplomate ou une famille à l'étranger qui ne peut échanger que par e-mail ou WhatsApp. Il demande un traitement d'urgence et cherche à contourner vos règles habituelles de réservation ou de paiement sécurisé.

2. La grille de vérification : Les 6 réflexes avant de répondre ou de cliquer

Avant toute action face à une demande de réservation suspecte, appliquez le protocole **V.É.R.I.F.** :

1. **Vérifier l'adresse de l'expéditeur :** Ne vous fiez pas au nom d'affichage. Regardez **l'adresse e-mail exacte après l'arobase (@).** Une adresse du type contact@booking-reservation-support.com ou jean.dupont8976@gmail.com au lieu du domaine officiel doit vous alerter.
2. **Éviter :**

1. **de cliquer sur les liens :** Ne cliquez jamais sur un lien vous demandant de vous connecter à votre compte professionnel. Ouvrez vous-même votre navigateur, tapez l'adresse officielle de votre plateforme/banque et connectez-vous directement.
2. **d'ouvrir des pièces jointes suspectes :** Méfiez-vous des fichiers compressés (.zip, .rar) ou des exécutables (.exe). Les contrats ou listes de voyageurs doivent préférablement être transmis sous format PDF classique.

3. **Refuser les modes de paiement atypiques :** N'acceptez jamais de rembourser un surplus ou de payer un prestataire tiers. Exigez des règlements via vos canaux habituels (carte bancaire via votre passerelle sécurisée, virement SEPA direct, chèque après vérification de solvabilité).

4. **Inspecter le ton et l'orthographe :** Un langage approximatif, l'utilisation systématique de la traduction automatique, un manque de précision sur votre hébergement (ex: *"Je veux louer votre propriété pour 3 semaines"* sans citer le nom du gîte) sont des signaux très fréquents. Soyez très attentif, l'IA est souvent utilisée et peut produire un contenu contextualisé crédible.

5. **Favoriser les autres moyens de contact :** Si le message prétend émaner d'un organisme ou d'un client connu, appelez directement le numéro officiel (et non celui indiqué dans le message suspect) pour vérifier.

3. Centre de ressources : Où s'informer et se former ?

Pour vous informer sur les cybermenaces, former votre équipe et adopter de bonnes pratiques informatiques :

- **Cybermalveillance.gouv.fr :** La plateforme nationale de prévention et d'assistance face au risque numérique. Vous y trouverez des fiches pratiques (phishing, rançongiciels, sécurisation de messagerie) et des guides d'hygiène informatique.
- **Service-Public.gouv.fr :** Fiches d'information sur les droits, les escroqueries courantes et la réglementation des paiements.
- **CNIL (Commission Nationale de l'Informatique et des Libertés) :** Guides pratiques sur la sécurité des données clients et le respect du RGPD au sein de votre établissement.

4. Déclaration et signalement : Que faire en cas de tentative d'arnaque ou de piratage ?

Si vous êtes confronté à une tentative d'arnaque ou si vous avez été piégé, voici les plateformes officielles auprès desquelles intervenir :

➢ A. En cas de simple tentative (sans préjudice subis)

- **Signaler un e-mail de phishing / hameçonnage :**
  - **Signal Spam :** Permet de signaler les e-mails frauduleux ou indésirables pour faire bloquer les émetteurs.
  - Signalement de SPAM par SMS ou MMS : 33700
  - **Phishing Initiative :** Permet de transmettre l'URL d'un faux site ou d'une fausse page de réservation pour demander son blocage dans les navigateurs web.
- **Signaler un contenu illicite ou une escroquerie en ligne :**
  - **PHAROS (internet-signalement.gouv.fr) :** Plateforme du Ministère de l'Intérieur pour signaler tout contenu ou comportement suspect sur Internet.
  - Signal Arnaques : site communautaire, sans vérification de la véracité des arnaques signalées
- **Assistance téléphonique gratuite :**
  - **Info Escroqueries (Ministère de l'Intérieur) :** 0 805 805 817 *(numéro vert gratuit)*.

➢ B. En cas d'attaque avérée, piratage ou perte financière

- **Déposer une plainte / Déclarer l'escroquerie :**
  - **THÉSÉE sur MaSécurité.gouv.fr :** Dispositif officiel de dépôt de plainte ou de signalement en ligne pour les arnaques et piratages sur Internet.
  - **17Cyber :** Diagnostic en ligne guidé pour obtenir les démarches urgentes à réaliser en fonction du piratage subi.
- **Prévenir les organismes financiers :**
  - En cas de virement ou de saisie de coordonnées bancaires sur un faux site, **contactez immédiatement votre banque** pour faire opposition et tenter de bloquer la transaction.

➢ C. Partager l'information auprès de votre réseau

Dans tous les cas, prévenez par email votre Office de tourisme pour qu'il partage l'information au réseau (institutions touristiques et socios-professionnels).

Trouvez les coordonnées de votre office de tourisme de référence.

NOTA BENE

AVANT TOUT SIGNALEMENT SUR DES SITES COMME SIGNAL ARNAQUES, SOYEZ CERTAIN QU'IL S'AGIT BIEN D'UNE ARNAQUE POUR EVITER TOUT RISQUE DE RECOURS EN DIFFAMATION