Transcritpion de l'infographie

# Courriel inquiétant : exemple de situation

## 1. Vous recevez un mail inquiétant.

- Expéditeur :servlce-abonr:iement@seoure-pay.fr
- Destinaire : sophie.dupony@email.com
- Sujet : prélèvement à venir
- Coprs du message : bonjour sophie dupont, un prélèvement de 71€ sera effectué prochainement pour le renouvellement de votre abomnement.
  Si vous n'êtes pas à l'origine de cette demande,cliquez ci-dessous pour annuler : annuler mon abonnement. Merci, le service client.

## 2. Le courriel contient vos vraies données :

Votre nom, votre adresse courriel, votre identifiant fiscal, votre iban, le nom de votre banque, le nom de votre opérateur mobile.

## 3. En réalité, ces données proviennent de plusieurs fuites de données

- Fuite n°1 : site e-commerce : nom, prénom, email
- Fuite n°2 : opérateur mobile, téléphone, aresse
- Fuite n°3 : plateforme de paiement iban, bic
- Fuite n°4 : service en ligne, adresse, historique d'abonnement

Une fuite expose des informations. Plusieurs fuites exposent une personne.

## 4. Les escrocs assemblent, vous doutez moins, vous cliquez ... Et le piège se referme.

La somme de 71€ est volée car vous avez donnez votre accord en pensant avoir répondu à un message officiel du fait de la vraisemblance des informations personnelles indiquées.

# Protégez-vous !

- Ne cliquez jamais sur les liens reçus par courriel ou sms.
- Vérifiez toujours depuis le site officiel de votre organisme ou banque.
- Activez les alertes de paiement sur votre compte bancaire.
- Surveillez régulièrement vos comptes et vos prélèvements.
- Soyez méfiant même si les données semblent correctes : elles peuvent venir de fuites.