



# LE PHISHING ET LE CRACK WIFI, QU'EST-CE QUE C'EST ?

Lycée Bellepierre - BTS SIO  
Vendredi 11 mars 2022

VALI ADAM Sameer, ROBERT Matthieu, HAMIDI  
Ambdil, MAILLOT Samuel, CLAIN Maxime,  
TIVERNÉ Timothée, VORANGINE Uldrick

## Qu'est-ce que le phishing ?

Le mode d'attaque le plus utilisé:

01

## Qu'est-ce que le crack WiFi

C'est lorsqu'un cybercriminel prend le contrôle d'un routeur sans le consentement de son propriétaire.

04

## Les stats. de phishing

Nombre d'e-mails de phishing en augmentation depuis 2016

02

## Comment procèdent-ils ?

Attaque par dictionnaire  
Man of the middle

05

## Exemples & actualités

Faits divers sur le phishing

03

## Les contres mesures

Comment s'en protéger ?

06

# 01 Qu'est-ce que le phishing ?

La technique la plus  
répandue



# DÉFINITION

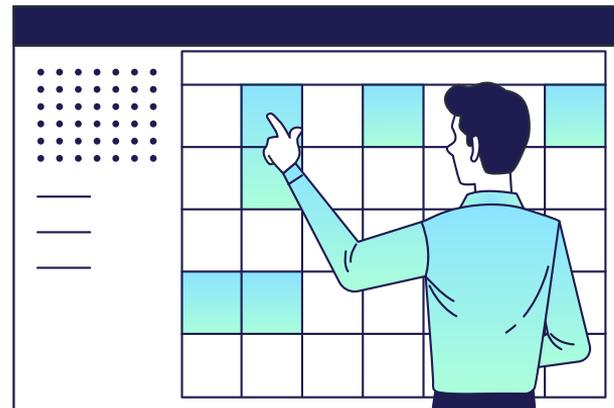
Consiste à usurper l'identité d'un tiers de confiance (banque , entreprise, commerce en ligne ...) via un e-mail ( environs 96% des cas ) ou encore par sms afin de tromper sa victime.



# 02

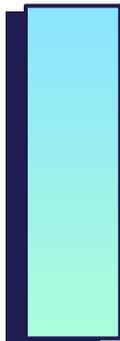
## Les statistiques

Quelques chiffres  
concernant le phishing



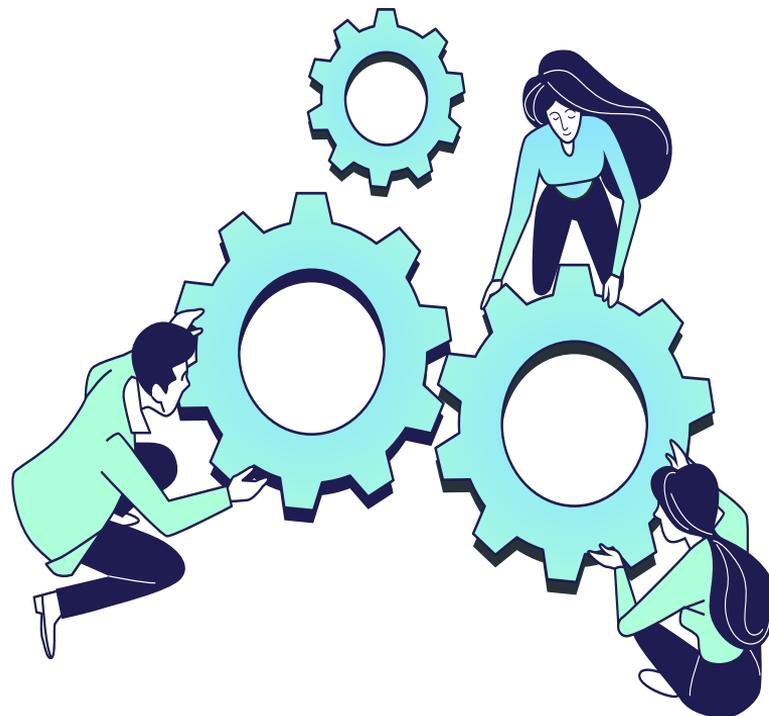
# STATISTIQUES

2020  
JANVIER



+27% de sites  
répertoriés

2021  
JANVIER

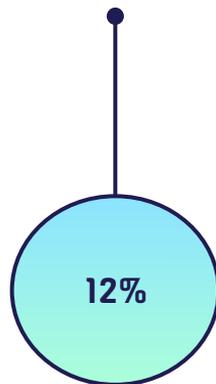


# Phishing par mail



**Ont ouvert  
des mails**

**Ont cliqué  
sur les liens**



**Ont partagé  
des  
données  
sensibles**

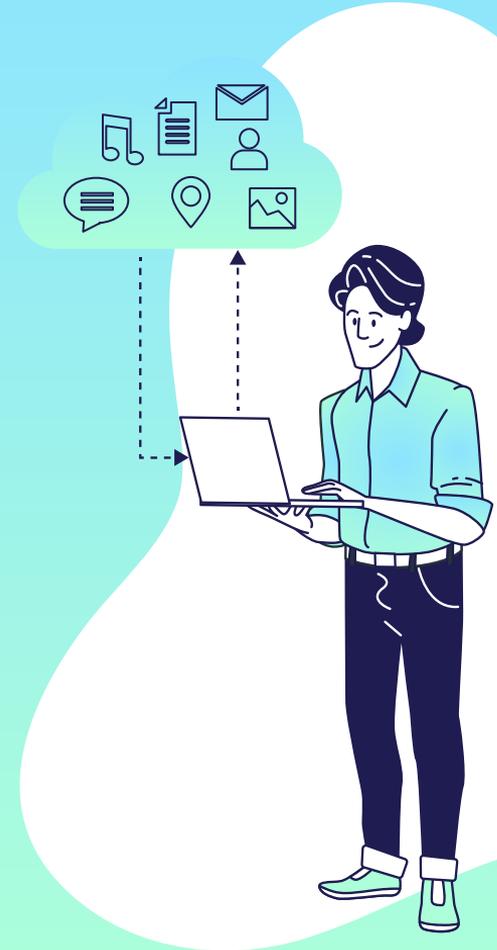
# STATISTIQUES



- 80% des failles causées par le phishing.
- 57% des entreprises ciblées
- 94% de phishing par mails

03

# Exemples & Actualités



# Phishing Boulanger

La victime :

Faux lien :  
Https / lettre  
modifié

**am** Alain MICHEL  
@alainmi11

Oh flûte...  
Je reçois un mail de #phishing très bien fait,  
imitant une confirmation de commande chez  
@boulanger avec un lien pour annuler la  
commande.  
Je suis le lien, j'arrive sur une page d'un site  
contrefait et là, surprise...  
1/3

2:15 PM · 30 déc. 2021

**am** Lire la conversation complète sur Twitter

18 Répondre Copier le lien

Faux site :  
Faire attention  
à l'orthographe

# DIVERS

2014

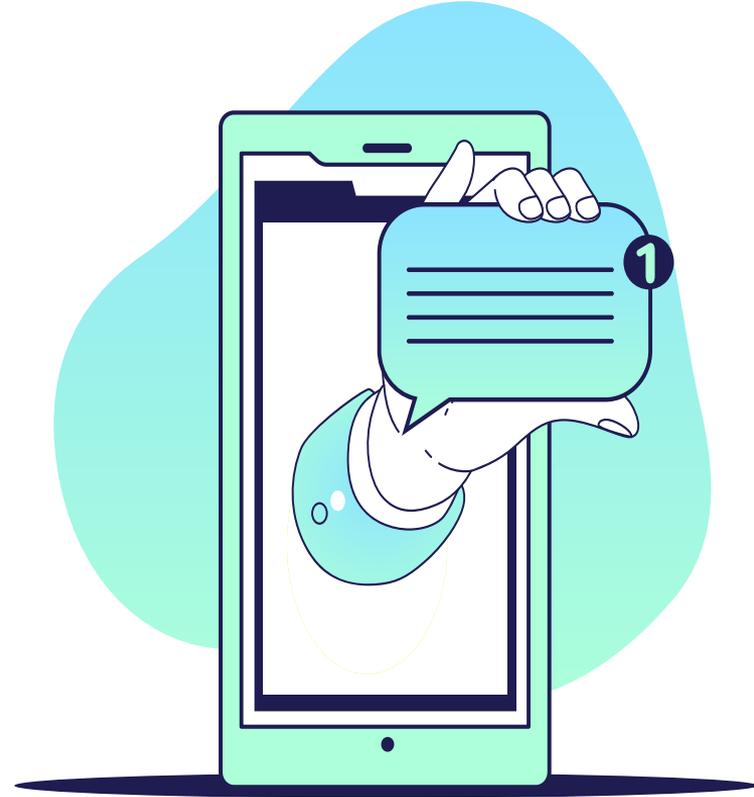
**Home Depot**

53 millions de mails volés

**Anthem Inc.**

78.8 millions de données volées

2015

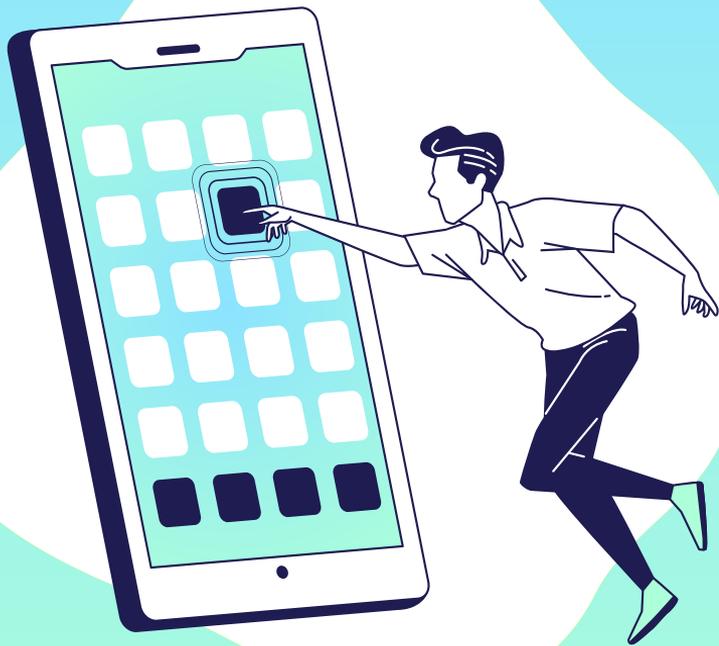




# 04 LE CRACK WIFI



- Contournement de sécurité**
- Vulnérabilité non corrigée**



**Comment  
procèdent-ils ?**



## Attaque par dictionnaire

-Tester une série de mot de passe



## Man Of The Middle

-Scan du réseau

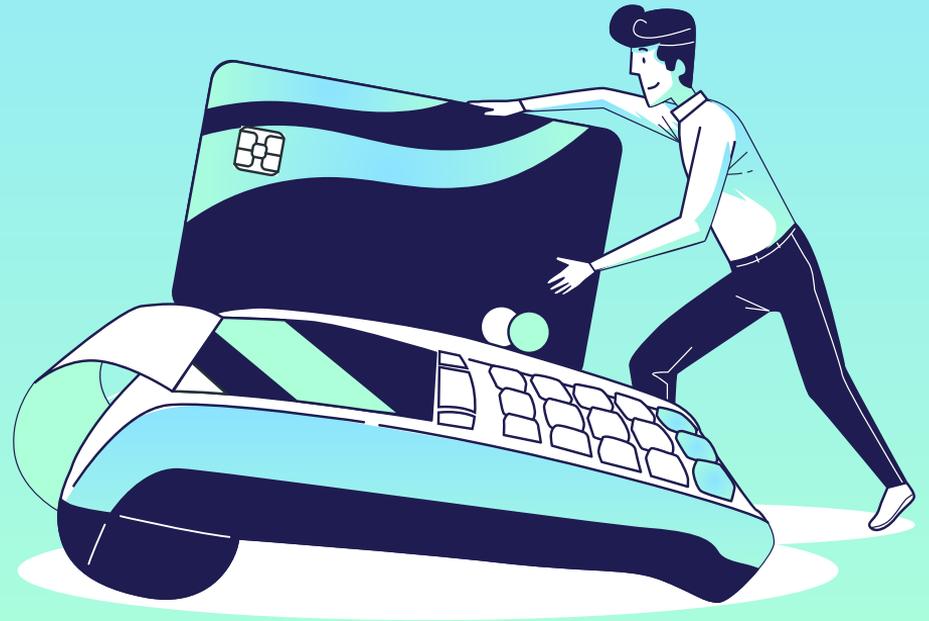
-Usurpation du SSID

-Récupération du mot de passe



06

# Les contre mesures





- Non-diffusion SSID
- WPA2 entreprise
- Activation programmée
- Filtrage adresse Mac
- Désactivation DHCP

## Bonnes pratiques à adopter

Que faire lorsque ça arrive ?

01

## Réactions à avoir

Quelles sont les bonnes réactions à adopter ?

04

## Côté utilisateur

Que doit faire l'utilisateur ?

02

## En tant que victime

Comment réagir en tant que victime ?

05

## Côté prestataire

Que doit faire le prestataire ?

03

## En tant que fournisseur de service

Comment réagir en tant que fournisseur de service ?

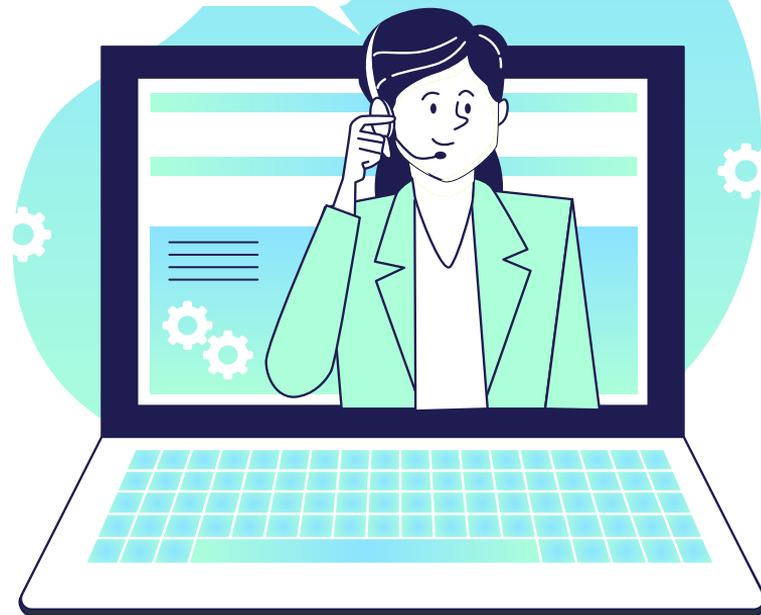
06

01

# Les bonnes pratiques?



# LES BONNES PRATIQUES



**Ce que les utilisateurs et les prestataires doivent faire.**

# 02 Côté utilisateur



# - Formation des utilisateurs :

---

- Vérifier l'adresse mail/son contenu



- Avoir des mots de passes différents

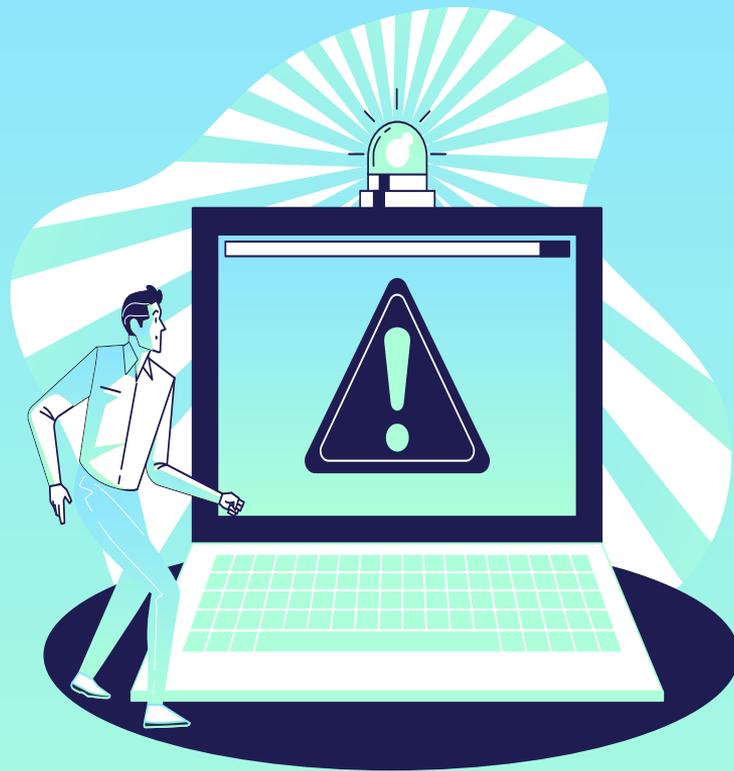


- Utilisation de A2F (double authentification)



03

# Côté prestataire



# Différents moyens de se protéger :

---

- **Déposer un droit d'auteur**



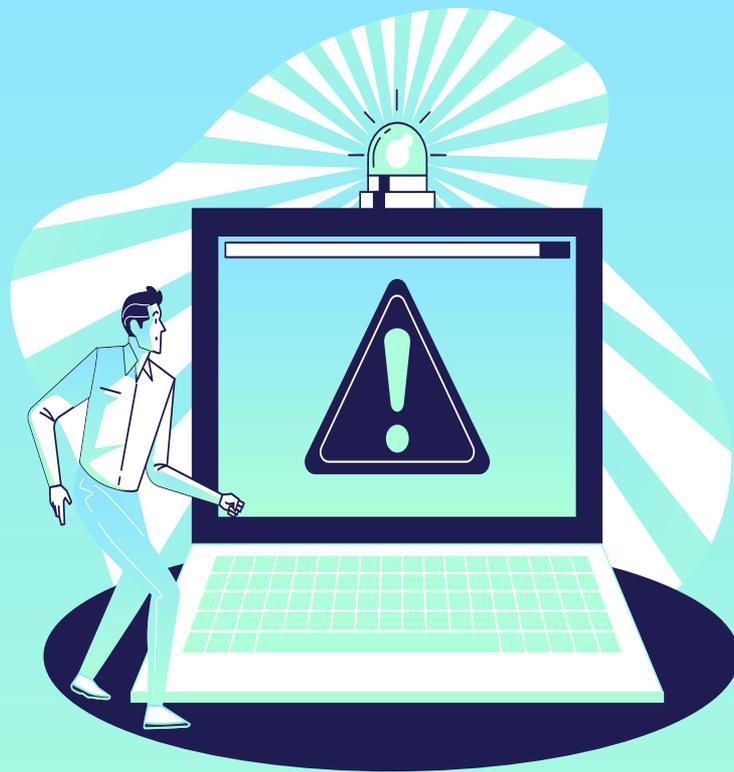
- **Utiliser des filigranes pour les images**



- **Vérifier le contenu d'un site grâce à des outils en ligne (Google Alert...)**



# 04 RÉACTIONS À AVOIR





# Que faire si l'on est touché par du phishing ?

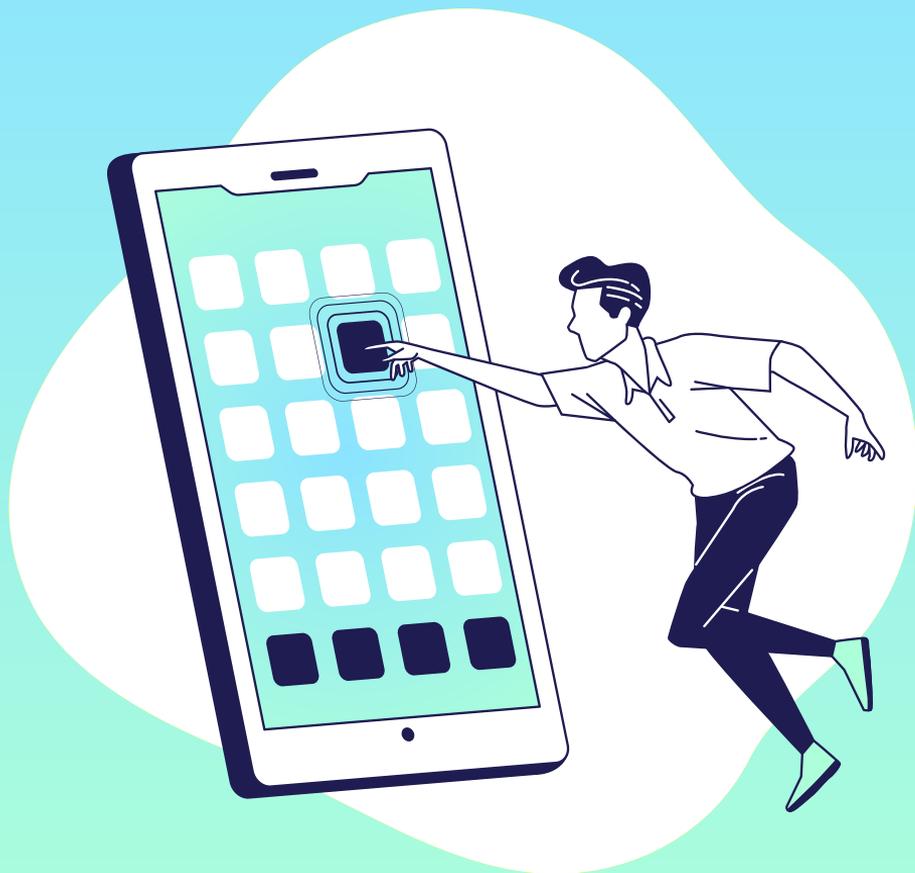
Signalement de phishing au sein de Phishing Initiative ([Phishing Initiative](#))

## 1 - Lutter contre le Phishing

Bloquer les sites sur les navigateurs, signaler le spam sur <https://www.signal-spam.fr/>

## 2 - Diminuer l'impact

Protéger autrui d'éventuelles attaques.



05

**EN TANT QUE  
VICTIME ?**

# Comment réagir à un fishing 1/2



## Changer de Mot de passe

Si vous avez malencontreusement communiqué un mot de passe, changez-le immédiatement sur le site ou service concerné, ainsi que sur tous les autres sites ou services sur lesquels vous utilisez ce mot de passe compromis (tous nos conseils pour gérer au mieux vos mots de passe).



## Signalez

Si vous avez cliqué sur le lien, vérifiez l'adresse du site Internet qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper.



## Besoin de plus de conseils

Pour être conseillé dans vos démarches, contactez la plateforme Info Escroqueries du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits de 9h à 18h30 du lundi au vendredi).

# Comment réagir à un fishing 2/2



## Conservez les preuves

Faites des captures d'écran et, en particulier, le message d'hameçonnage reçu.



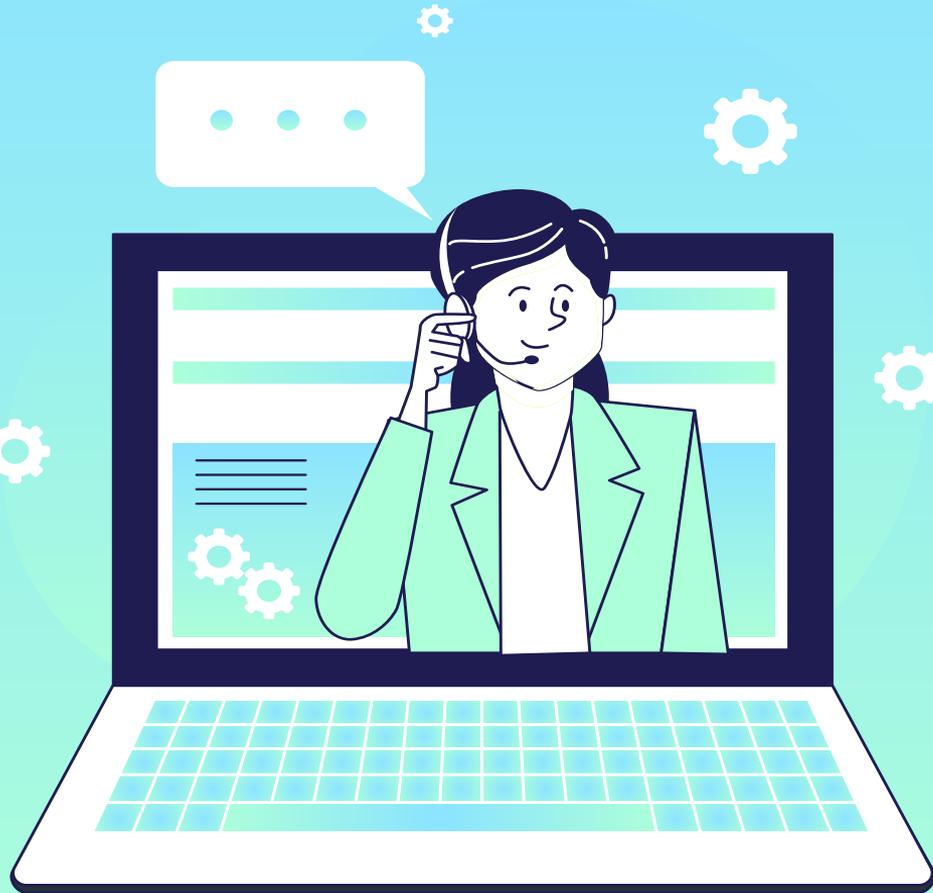
## Contactez le Prestataire

Contactez l'organisme concerné pour signaler l'acte si vous avez constaté des débits frauduleux sur votre compte, faites opposition immédiatement auprès de votre organisme bancaire ou financier..



## Déposer plainte

Si vous avez constaté que des informations personnelles servent à usurper votre identité ou si vous constatez des débits frauduleux sur vos comptes bancaires, déposez plainte au commissariat de police ou à la brigade de gendarmerie dont vous dépendez.

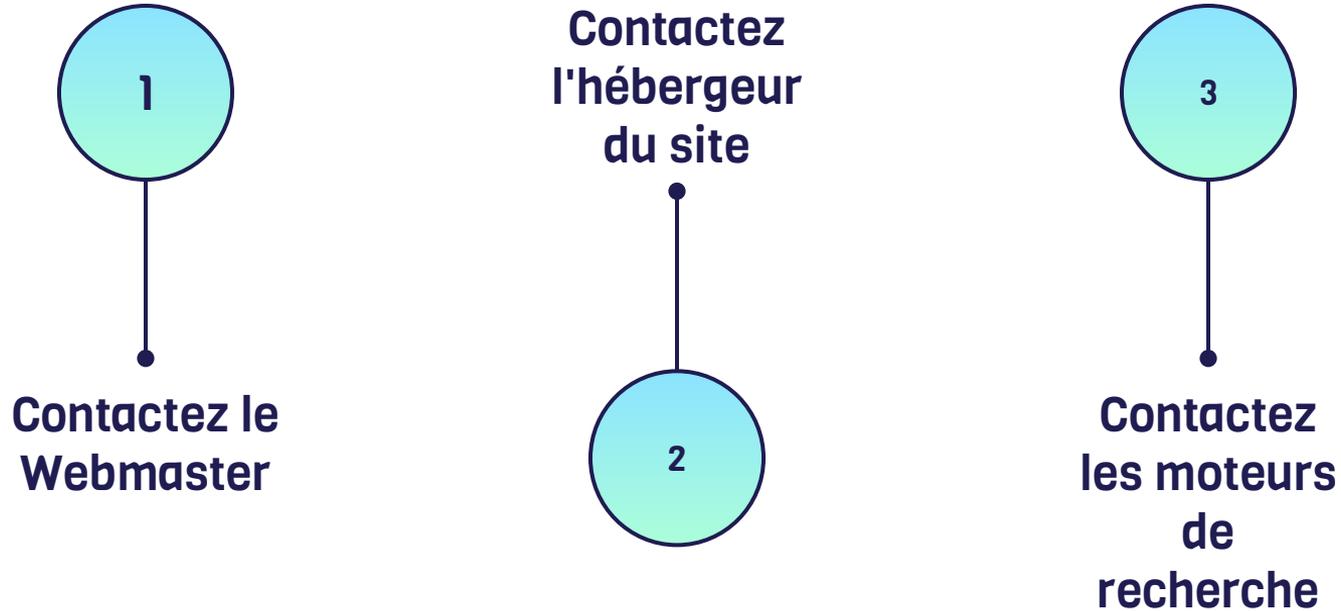


# 06

## En tant que fournisseur de service

## Côté Fournisseur

---



**Quels sont les risques  
pour les pirates ?**

**01**



**02**

**L'actualité en Ukraine**

# 01

# LES RISQUES

Sanctions Pénales



# Selon la LOI GODFRAIN

RELATIVE À LA FRAUDE INFORMATIQUE



Selon les infractions  
retenues



De 2 ans  
d'emprisonnement &  
30 000€

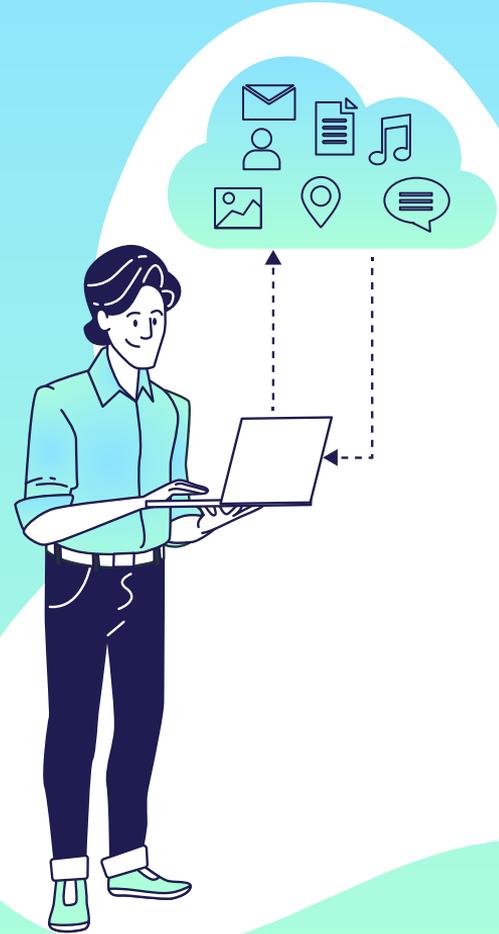


10 ans  
d'emprisonnement &  
150 000€



02

# Actualité Ukraine





## ATTAQUE SATELLITE

- Perte de contrôle d'éoliennes
- Panne de réseau internet

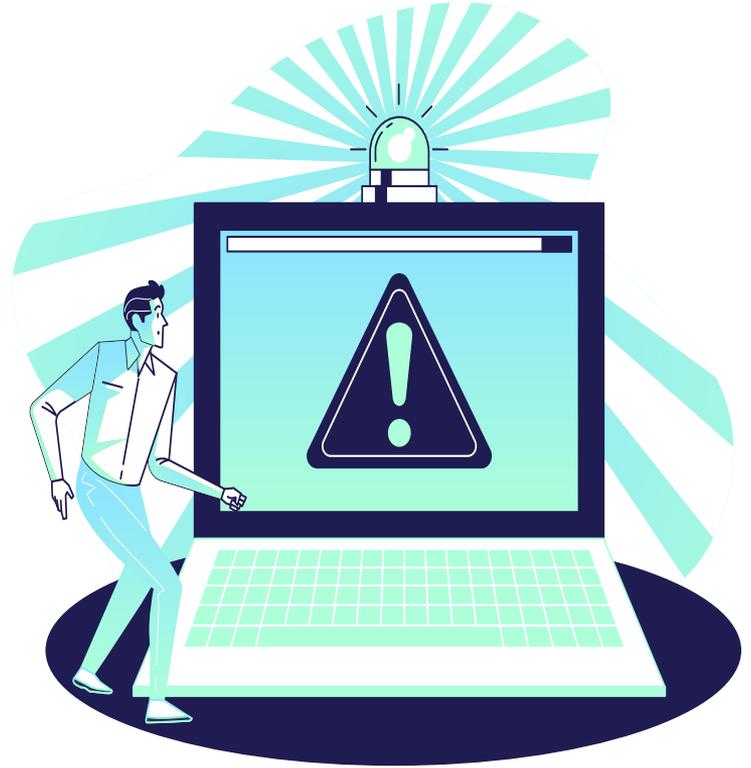
# Malware

## 1 - HermeticWiper

Suppression de  
données/Corruption

## 2 - Cyclops Blink

Exfiltration de données et  
blocage de pare-feu





## MESURES DE L'ANSSI

L'ANSSI a mis en place le CERT-FR sur les tensions internationales, dans lequel, l'ANSSI fait le point sur l'état de la menace et partage des bonnes pratiques à suivre.

# Liens utiles

## 1 - Signalement de phishing

<https://phishing-initiative.fr/contrib/>

## 2 - Démonstration sur le phishing Hack Academy

<https://www.youtube.com/watch?v=RupAsjOSuOc>

