Stengelin

# LIVRE BLANC

Mai 2023

# Sécurité

## de vos données

# 3 Réflexes à s'approprier

01 Le phising

02 Le rançongiciel

03 Vol de mot de passe

## Notre expert

Benjamin Forgette
Associé du cabinet

# 01 Le phising

## Qu'est-ce que c'est ?

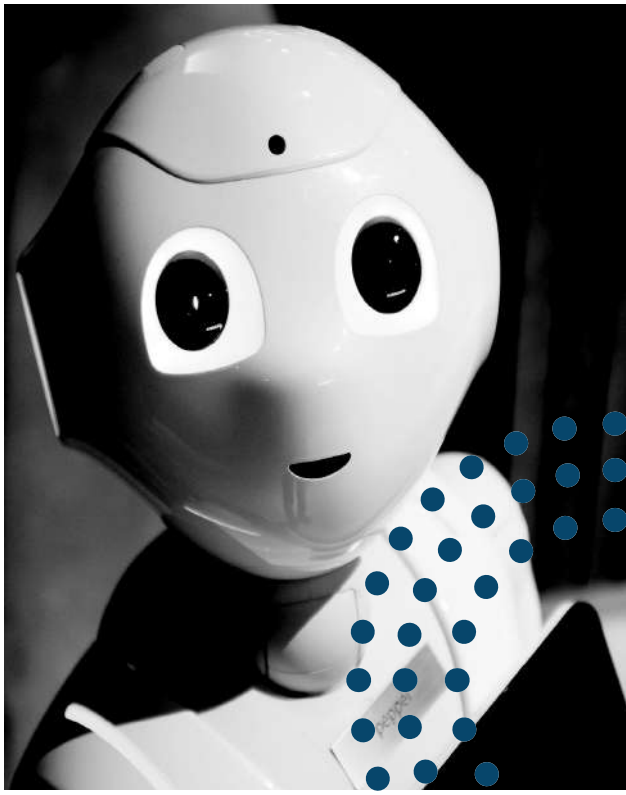
Le **phishing** ou hameçonnage consiste à faire croire à la victime qu'elle communique avec un tiers de confiance **dans le but de lui soutirer des informations personnelles** (numéro de carte bancaire ou mot de passe).

Le plus fréquemment le phishing est réalisé par le biais de **faux sites internet** (boutiques en ligne, sites web administratifs...).

**Attention, ils peuvent être des copies parfaites de l'original.**

## Passez en mode « Protection » avec ces 4 pratiques

- Si vous réglez un achat, vérifiez que vous le faites sur un site web sécurisé dont l'adresse commence par **« https ».**
- Si un courriel vous semble douteux, **ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient.** Il est préférable de **se connecter en saisissant l'adresse officielle** dans la barre d'adresse de votre navigateur.
- Ne communiquez jamais votre mot de passe. Aucun site web fiable ne vous le demandera !
- **Vérifiez que votre antivirus est à jour** pour maximiser sa protection contre les programmes malveillants.



# 02 Le rançongiciel

## Qu'est-ce que c'est ?

Les **rançongiciels** (ou ransomware) sont des **programmes informatiques malveillants** de plus en plus répandus.

Avec quel objectif ? **Chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.**

## Adoptez ces 3 automatismes

### Sauvegardez

**Effectuez des sauvegardes régulières** de vos données.

### Vérifiez la provenance

**N'ouvrez pas les messages dont la provenance ou la forme est douteuse.**

### Identifiez les extensions

Apprenez à **identifier les extensions douteuses des fichiers :** si elles ne correspondent pas à ce que vous avez l'habitude d'ouvrir, ne cliquez pas !

# 03 Le vol de mot de passe

## Qu'est-ce qu'un vol de mot de passe ?

Le vol de mot de passe consiste à **utiliser des logiciels destinés à tenter un maximum de combinaisons possibles dans le but de trouver votre mot de passe.** Cette méthode a pour but **d'usurper votre identité** ou celle de votre entreprise.

## 4 réflexes à s'approprier

01 **Utilisez un mot de passe anonyme !** Aussi, évitez d'avoir recours aux noms de vos enfants, de vos animaux ou d'autres informations susceptibles de figurer sur vos réseaux sociaux pour composer votre mot de passe.

02 **Construisez des mots de passe compliqués :** utilisez des lettres, des majuscules et des caractères spéciaux.

03 **N'utilisez pas le même mot de passe partout !**

04 Enfin, pensez à **changer régulièrement votre mot de passe.**

Stengelin

**STENGELIN**
**185, rue de Bercy 75012 Paris**
**21 - 37, rue de Stalingrad 94110 Arcueil**

Ce document est partagé à titre informatif. L'équipe Stengelin reste à votre écoute pour toute demande complémentaire afin de vous accompagner et de vous conseiller au mieux dans vos démarches.