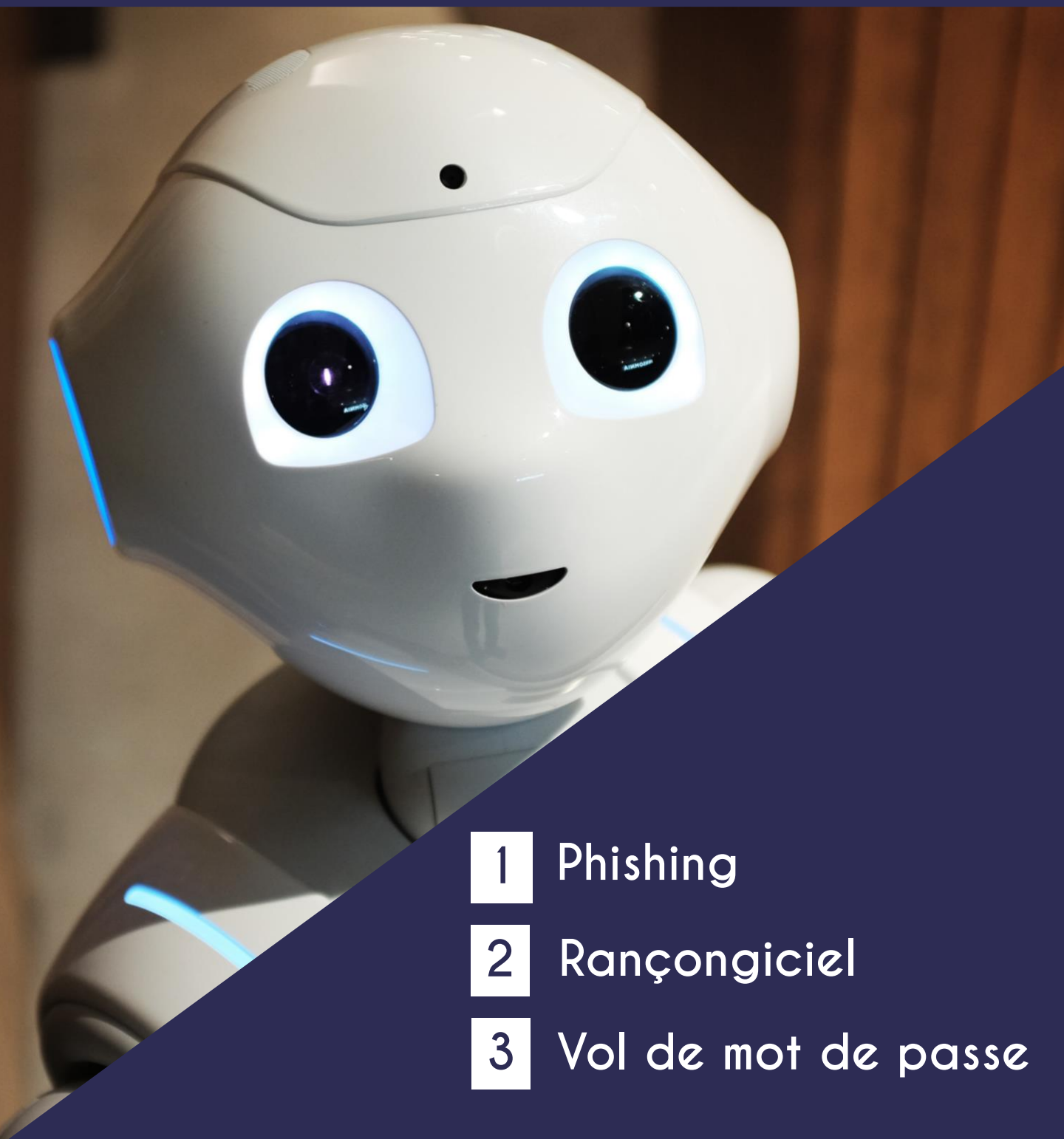
Le livre blanc

Sécurité de vos données

Quelques réflexes à s'approprier



1 Phishing

2 Rançongiciel

3 Vol de mot de passe

Stengelin

1 Le phishing

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.**

PASSER 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.

3 Le Rançongiciel

QU'EST-CE QU'UN **RANÇONGICIEL** ?

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

1 Sauvegardez !

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

2 Vérifiez la provenance

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

3 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 !

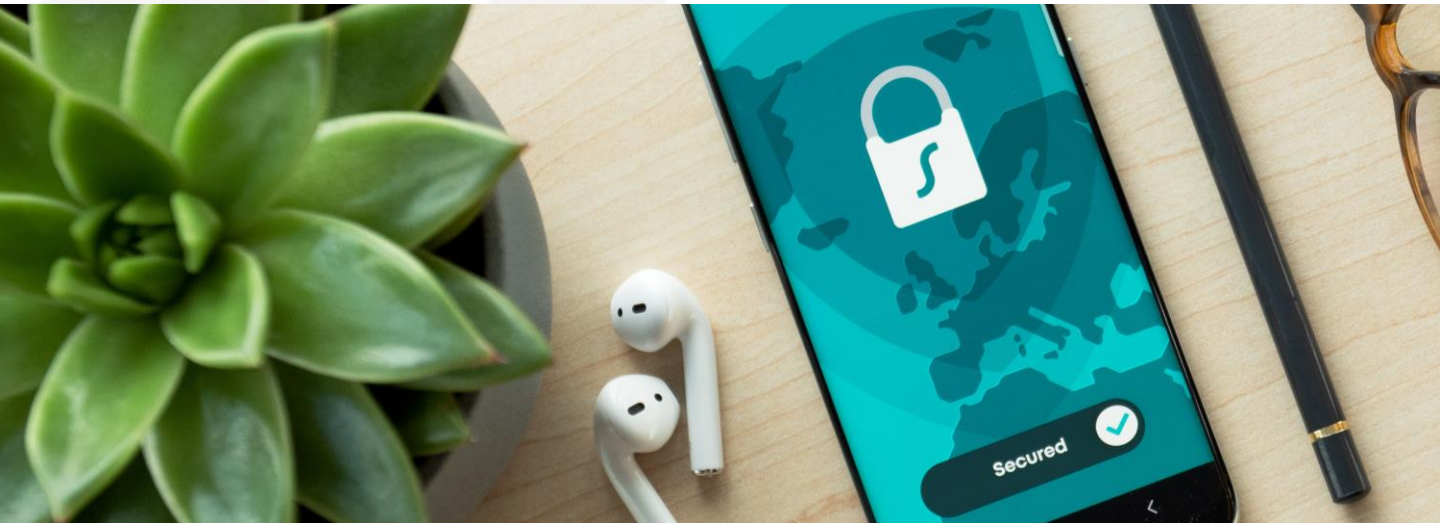
3 Le vol de mot de passe

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

- **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.
- **Construisez des mots de passe compliqués** : utilisez des lettres, des majuscules et des caractères spéciaux.
- **N'utilisez pas le même mot de passe partout !**
- Enfin, pensez à **changer régulièrement votre mot de passe**.



Vous voulez en savoir plus ?

CONTACTEZ-NOUS
NOUS RÉPONDRONS À VOS QUESTIONS

01 42 41 01 01

contact@stengelin.fr

Cabinet Paris
207 rue de Bercy
75012 Paris

Cabinet Arcueil
21-37 rue de Stalingrad
94110 Arcueil

Stengelin