GottaPhish

L'harponnage en toute simplicité.

Qui sommes nous ?

GottaPhish est une startup française qui innove dans les outils de formation au risque phishing.

Notre objectif ?
Renforcer la cybersécurité des organisations en sensibilisant et en formant les employé(e)s aux menaces cyber, grâce à des approches ciblées et adaptées.

Nos engagements :

- Travailler en étroite collaboration avec votre équipe pour personnaliser nos solutions à vos besoins spécifiques.
- Fournir un soutien continu et des mises à jour pour assurer que vos équipes restent informées des dernières menaces.
- Évoluer et adapter nos services pour répondre aux défis changeants de la cybersécurité.

58% des employés se font piéger par du phishing.
Ce chiffre chute à **10%** lorsqu'ils ont été sensibilisés.

+47,2 %

Hausse des attaques phishing en 2023.

562,4 M

Mails de phishing détectés au premier trimestre 2023

66 %

Taux d'attaques de spear phishing responsables des violations.

Les 2 formes de phishing :

Phishing
(hameçonnage)

- Technique frauduleuse visant à voler des informations personnelles en se faisant passer pour une entité de confiance.
- Envoi du même email à tous les employés d'une entreprise.

Spear phishing
(harponnage)

- Même technique frauduleuse, c'est une forme ciblée de phishing.
- Personnalisation des attaques avec des informations spécifiques sur la victime pour augmenter le taux de réussite.

Notre solution GottaPhish :

1. Nos outils de spear phishing

2. Nos outils de formation et sensibilisation

Trello

Bonjour William

Nous avons détecté une activité inusuelle sur votre compte Trello qui requiert votre attention immédiate. Pour assurer la sécurité de vos données, nous avons temporairement limité l'accès à certaines fonctionnalités de votre compte.

Vérifier Activité

Si vous n'avez pas effectué ces activités ou si vous avez des soupçons concernant l'accès à votre compte, il est crucial que vous agissiez rapidement pour sécuriser vos informations.

Cordialement,

L'équipe de sécurité Trello

E-mail de **phishing générique**, non adapté à un réceptionniste.

Cible : William

Métier : Réceptionniste

Entreprise : IHG

Booking

Bonjour William,

Nous avons le plaisir de vous informer que le paiement pour la réservation d'un de vos clients a été effectué avec succès sur Booking.com.

Une carte bleue virtuelle a été générée pour cette transaction et est désormais disponible pour votre utilisation. Vous pouvez accéder aux détails de la carte bleue virtuelle en cliquant sur le lien suivant : booking

Nous vous remercions de votre collaboration et restons à votre disposition pour toute question ou assistance supplémentaire.

Cordialement,

L'équipe Booking.com

E-mail de **spear phishing** créé par GottaPhish, adapté à un réceptionniste.

Cible : William

Métier : Réceptionniste

Entreprise : IHG

1 Renseignement source ouverte :

🔍 Méthodologie pour la détection des sujets de phishing :

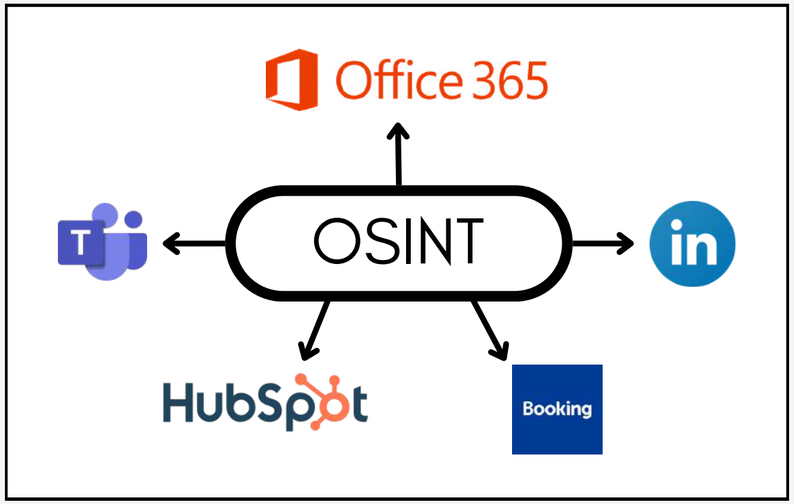
OSINT – Recherche des informations directement sur internet (LinkedIn, Teams, etc.)

En têtes d'emails – Détection automatique de tous les outils.

Connexions OAuth – Retrouver les applicatifs via les historiques des connexions OAuth.

🎯 Objectifs :

Scénarios de spear-phishing ciblés
Cartographie des usages
Détection du Shadow IT
Sensibilisation aux risques des outils personnels



La particularité de GottaPhish :

GottaPhish usurpe les **outils externes** que vous utilisez mais aussi...

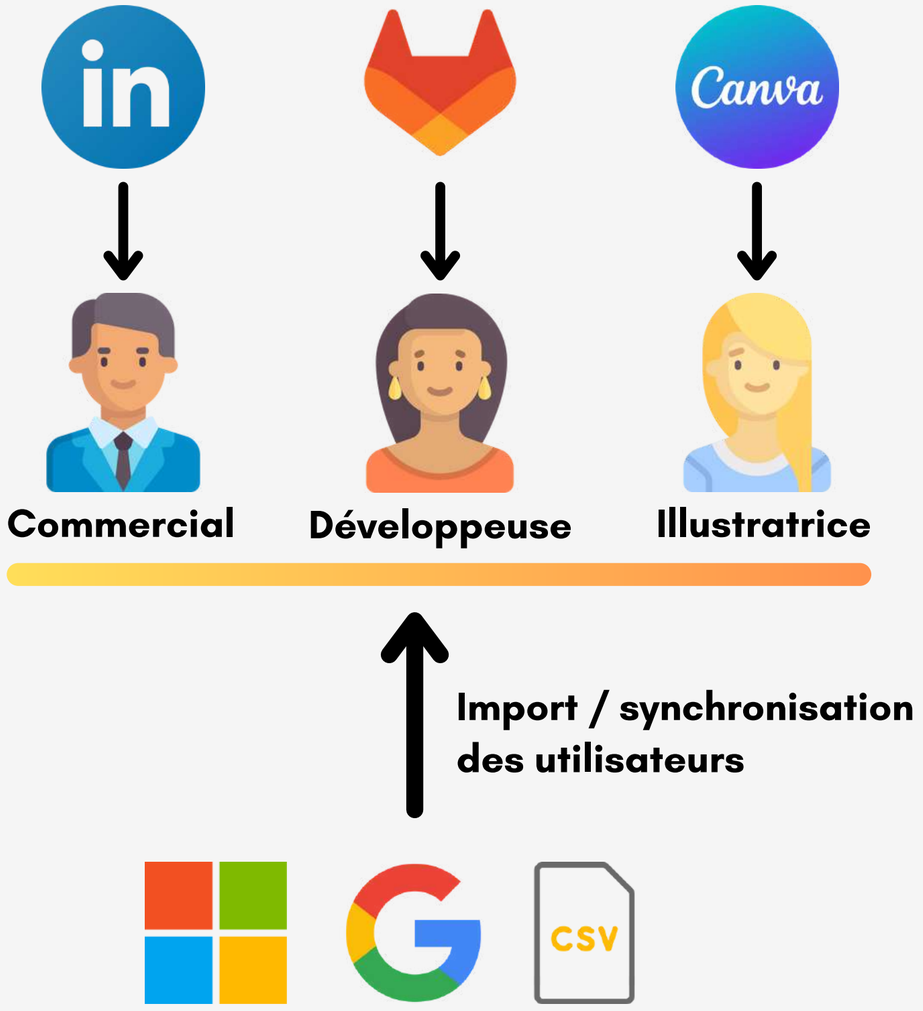
Les outils internes

Intranet

Les collaborateurs

2 Création des e-mails :

Génération d'e-mails personnalisés par **IA** selon le profil des employés *(commercial, développeur, etc.)* et les mails précédemment reçus.



3 Création de sites de phishing :

- **Copie** d'un site existant avec interception des identifiants de l'employé(e).

- **Achat** d'un nom de domaine similaire au site existant :

linkedin.com

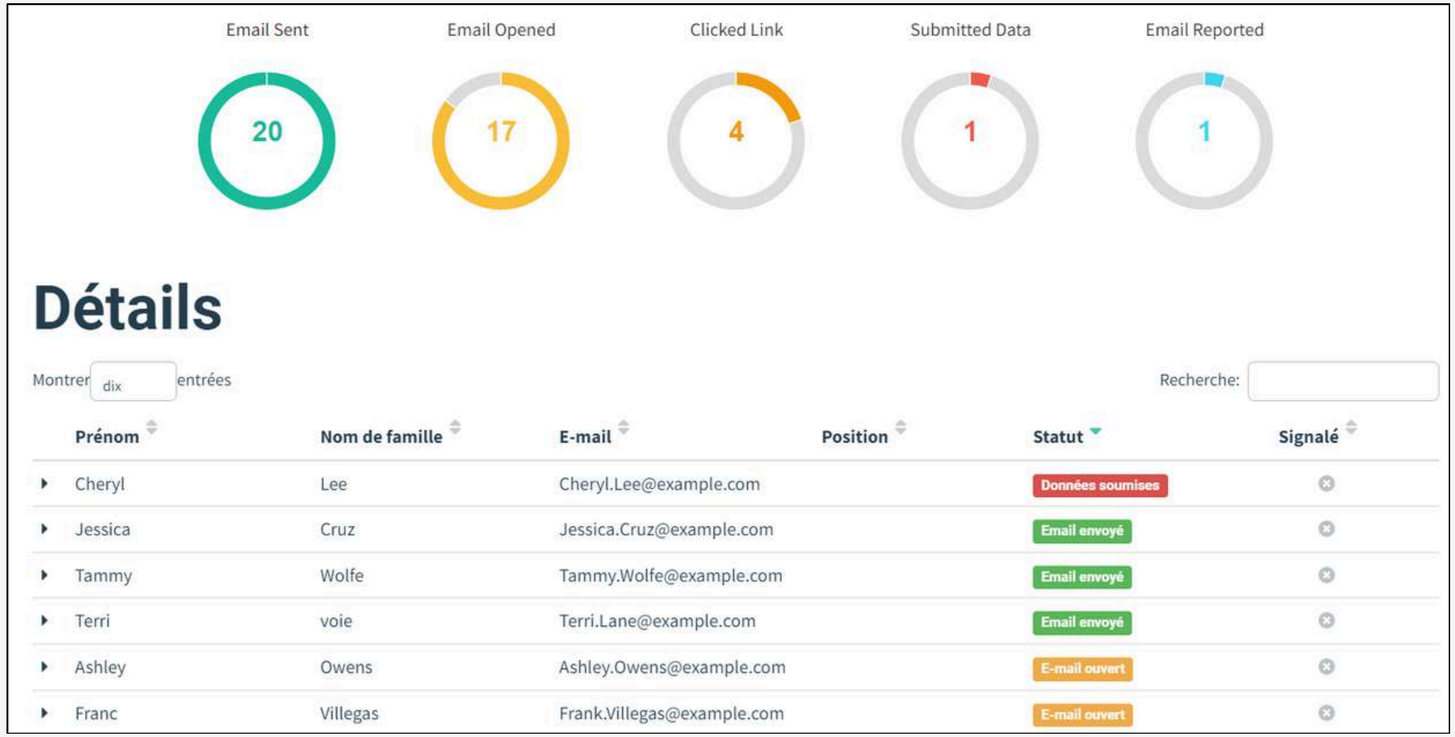
↓

espacelinkedin.com

4 Visualisation et export :

KPI Suivis par GottaPhish

- Taux d'ouverture
- Taux de clics
- Taux de soumission
- Taux de réponse
- Temps de réaction
- Types de scénarios efficaces
- Outils SaaS exploités
- Vulnérabilités humaines
- Mise à jour des navigateurs
- Évolution dans le temps
- Impact des formations



Des intégrations multiples

GottaPhish s'adresse aux entreprises ayant des besoins élevés et propose une intégration complète avec tous les systèmes d'antispam.

Microsoft Gmail proofpoint.

Une option red team

GottaPhish teste la résilience du SI face à des attaques externes.

Une startup innovante et locale

GottaPhish est implanté dans votre région et vous accompagne dans la mise en place chez vos clients. Nous vous apportons une réelle valeur ajoutée à votre offre en cybersécurité.

Notre option red team :

GottaPhish permet d'évaluer la résilience de l'entreprise face à des menaces anonymes.

2 cas d'usage de notre option :

1. **Tester la résistance** de votre blue team face à des attaques réalistes.

2. **S'infiltrer dans le SI** (Système d'Informations) lors de pentest afin de compromettre l'entreprise et identifier ses faiblesses.

Notre option permet :

- **Automatisation** complète des campagnes de phishing
- **Intelligence artificielle** pour générer des emails indétectables
- **Bypass** des filtres de sécurité & MFA
- **Suppression automatique** des traces après chaque campagne

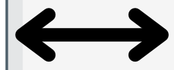
Fonctionnalités techniques clés :

- **Emails hautement délivrables** (SPF, DKIM, DMARC automatiques)
- **Génération IA & camouflage avancé** pour contourner les filtres de sécurité
- **Score de délivrabilité** en temps **réel** avant envoi
- **Rotation automatique** des noms de domaines pour éviter le blacklistage
- **Profilage avancé** des cibles (OS, navigateur, IP, vulnérabilités)
- Techniques de **Bypass MFA** (Evilnginx, phishing proxy…)
- Suivi & reporting avancé avec **indicateurs clés et recommandations**

Notre SaaS hybride pour sécuriser vos données sensibles

- **Elle combine :**

Une partie qui est **hébergée dans le cloud** *(ex: interface, automatisation, analyses, etc.)*

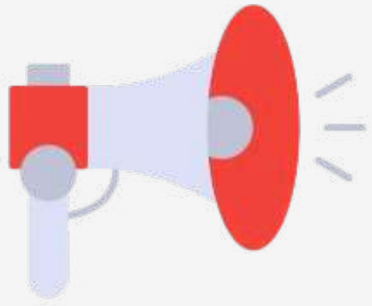


Et une partie installée **localement chez vous** *(ex: stockage des données sensibles, exécution des payloads, etc.)*

- Vous pouvez **garder la main** sur vos données critiques (ex : logs, identifiants, infrastructures sensibles).
- Tout en **utilisant les services cloud** pour automatiser les campagnes de phishing, suivre les résultats, ou générer des rapports.
- Cela répond aussi à **certaines politiques RGPD ou internes** qui interdisent l'hébergement externe de données sensibles.

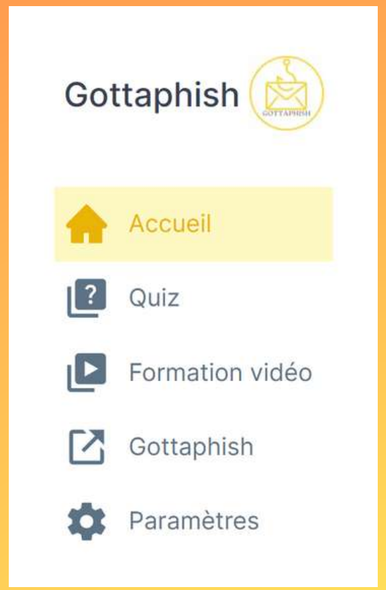
Sensibiliser et former vos employé(e)s aux risques du phishing

En analysant les comportements de vos employé(e)s aux campagnes simulées, notre plateforme propose **deux systèmes de formation** d'e-learning interactifs.



L'objectif de nos formations :

- Renforcer la posture de **sécurité** de votre entreprise en formant vos employé(e)s à reconnaître et à éviter les tentatives de phishing
- **Réduire le risque** de compromettre des données sensibles et des accès.



Notre formation courte :

Cette formation est **directement disponible** après engagement.

Ce système de formation comprend :

- Un **quiz** selon votre expertise (*débutant*, *intermédiaire*, *expert*).
- Des **vidéos** pour apprendre à **reconnaître** et à se **protéger** des attaques de phishing.

Lorsque qu'un employé échoue à la campagne de phishing et clique sur le lien, il est automatiquement redirigé vers cette formation interactive pour le sensibiliser.

Disponible en :

Français

Anglais

Notre formation longue :

Cette formation est **accessible à tout moment sur Moodle**, ce qui permet aux utilisateurs d'apprendre à leur rythme et selon leur disponibilité.

Ce système de formation comprend :

- Une **communication** et une **collaboration** (chat et wiki).
- Une **évaluation** et un **feedback** (tests, ateliers et feedback disponible par le DSI).
- Un **suivi des progressions** grâce à un MOOC (*parcours d'apprentissage adaptatif*) et un glossaire (*base de données pour les termes techniques ou spécifiques*).
- Les **rapports** et **analytics** (achèvement d'activité et rapports des résultats).

Disponible en :

Français

Anglais

Pourquoi nous choisir ?

Email de phishing ciblés

- Messages **IA adaptés** au poste, et au contexte
- Contenu dynamique pour éviter les filtres de sécurité et renforcer le **réalisme**

Usurpation crédible

- **Nom de domaines, mails, personnalisés** pour imiter les services internes de votre entreprise

Pages sur-mesure

- **Reproduction fidèle** des pages de connexion
- Collecte des identifiants dans un environnement **indétectable**

Profilage avancé

- Identification de l'OS, navigateur, IP, et vulnérabilités pour **affiner les attaques**

Attaques adaptées

- Scénarios de relance automatiques selon la **durée de votre choix** (journalier, mensuel, etc.)

Analyses détaillées

- **Rapports détaillés** pour chaque campagne (nombre d'ouverture, de liens cliqués, etc.)

contact@gottaphish.com

Thibault DACCORD
+ 33 7 49 25 66 38

Merci !

Un cyber café ?

GottaPhish