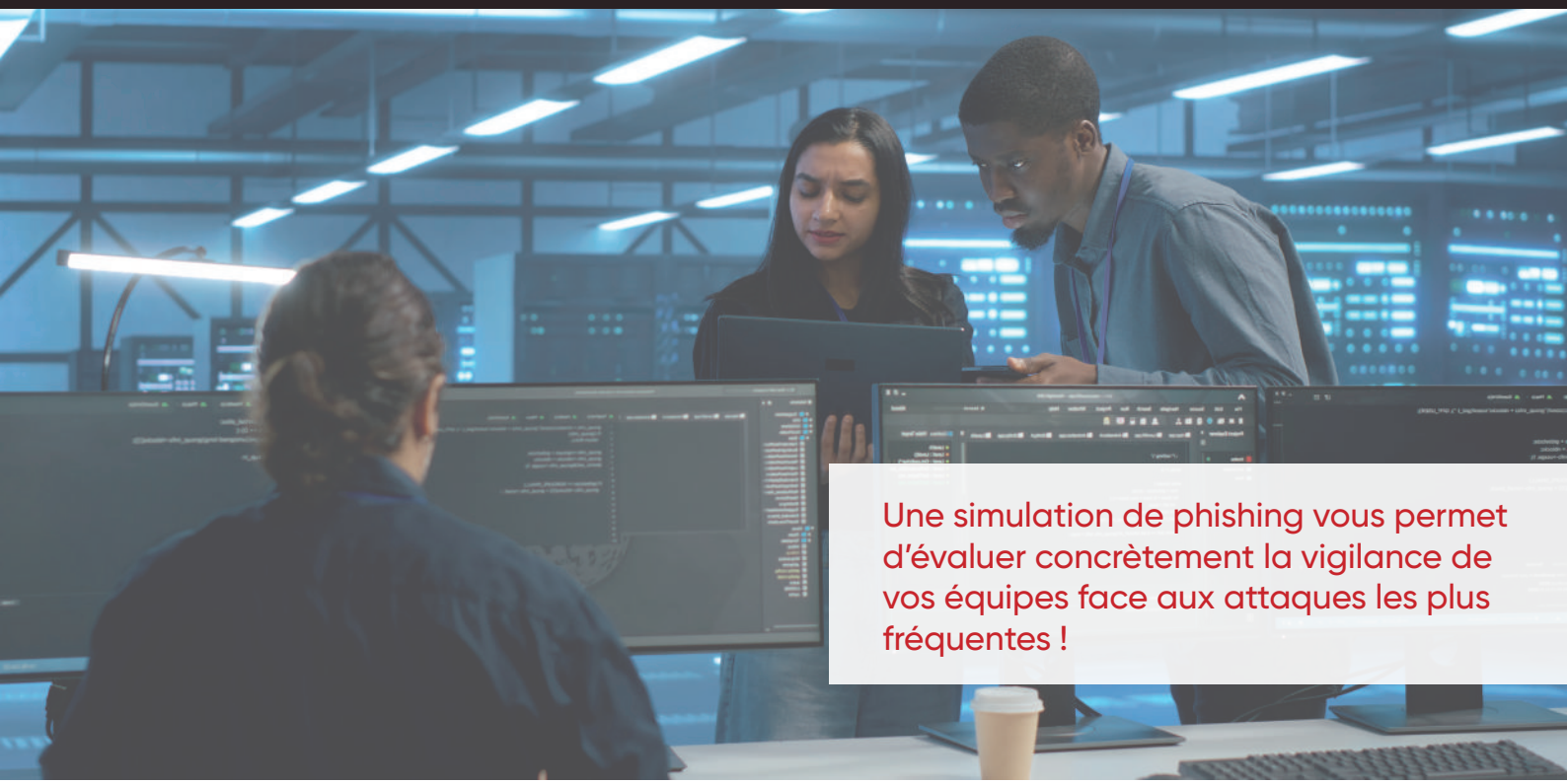
VIVALTEK | PHISHING CAMPAIGN



Une simulation de phishing vous permet d'évaluer concrètement la vigilance de vos équipes face aux attaques les plus fréquentes !

INTRODUCTION

Une attaque de phishing[1] peut **provoquer une interruption partielle ou totale de vos activités** pendant plusieurs jours, avec des conséquences directes sur la productivité, la continuité de service et la réputation de votre entreprise. Il suffit parfois d'un simple e-mail frauduleux pour compromettre un système, déclencher une infection ou ouvrir la voie à un ransomware.

En testant la vigilance de vos équipes face à ce type de menace, **vous identifiez les points faibles en amont,** réduisez les risques d'interruption coûteuse et contribuez à la protection directe de votre chiffre d'affaires.

OBJECTIFS

Évaluer la capacité des employés à détecter et réagir à des tentatives de phishing grâce à notre module de simulation d'envoi d'e-mails frauduleux.

- **Sensibiliser vos employés à réagir face aux tentatives de Phishing**
- **Identifier les vulnérabilités techniques et humaines**
- **Améliorer les procédures, formations et la stratégie anti-phishing de l'entreprise**
- **Renforcer la culture de sécurité des employés**

LES CHIFFRES CLÉS*

75 %

des entreprises françaises ont été ciblées en 2023, par des attaques de phishing, ce qui en fait la menace cyber la plus fréquente.

83 %

des entreprises (dans le monde) déclarent avoir été victimes d'au moins une attaque de phishing chaque année.

21 %

des demandes d'assistance adressées à Cybermalveillance.gouv.fr par les entreprises en 2023 concernaient des cas de phishing.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Comment fonctionne le module Phishing Campaign ?

L'évaluation débute par une **préparation des scénarios de phishing adaptés à l'entreprise**, en choisissant des thématiques crédibles (comme des mails internes, des notifications bancaires ou des faux accès cloud) pour maximiser le réalisme.

Notre module conçoit ensuite des e-mails, soigneusement élaborés pour simuler une attaque réelle, en jouant sur des techniques classiques d'ingénierie sociale : urgences, liens piégés, pièces jointes suspectes, etc.

Ces e-mails sont ensuite envoyés aux collaborateurs ciblés, sans les prévenir, afin de tester leur vigilance et observer leurs réactions face à des tentatives d'hameçonnage.

À la fin de la campagne, il dresse un **bilan détaillé des résultats,** en identifiant les points faibles (ouverture de l'e-mail, taux de clics, renseignement d'informations).

Sur quoi s'appuie le module Phishing Campaign ?

- Il s'appuie sur une **analyse complète des comportements des utilisateurs** tout au long de la simulation.
- Des indicateurs clés tels que le **taux d'ouverture des e-mails, les clics sur les liens frauduleux, ainsi que les téléchargements de pièces jointes** sont remontés dans notre module.
- Pour rendre la simulation plus réaliste et pertinente, des **scénarios personnalisés peuvent être créés en fonction de votre contexte**, et une liste ciblée d'adresses e-mail peut être définie pour tester des profils ou départements spécifiques.

Pourquoi effectuer une campagne de phishing ?

1. **Mesurer le niveau réel de vigilance et de maturité cyber des employés face aux attaques,** qui restent l'une des principales cause d'intrusion dans les systèmes. En simulant des tentatives de phishing, l'entreprise peut identifier qui clique, qui signale et qui ignore, révélant ainsi des failles humaines que les formations génériques ne corrigent pas toujours.

2. **Protéger les données sensibles,** prévenir l'introduction de ransomwares et garantir la continuité des activités, en réduisant les risques que le « maillon humain » soit exploité comme point d'entrée d'une cyberattaque coûteuse.

3. **Démontrer la vigilance et la responsabilité de l'entreprise** envers ses clients et partenaires, notamment dans le cadre des exigences RGPD², ISO ou NIS2 qui imposent de contrôler la sensibilisation et la réactivité des équipes.

4. **Préserver la réputation et la valeur de la société,** car une fuite liée à un simple clic peut engendrer des coûts bien supérieurs à ceux d'un programme proactif de tests et de formations ciblées.

L'évaluation Phishing Campaign

Permet d'évaluer la vigilance réelle des employés, d'identifier les failles humaines et de prévenir les intrusions via le facteur humain.

Elle protège les données, assure la conformité réglementaire et renforce la crédibilité de l'entreprise face aux risques cyber.

Sur quelle fréquence réaliser une campagne de phishing ?

Nous recommandons de réaliser plusieurs campagnes sur une année afin de maintenir un haut niveau de vigilance, de mesurer les progrès, et de sensibiliser durablement vos équipes aux techniques d'attaques réelles. Ce rythme s'inscrit dans une **démarche proactive de conformité aux référentiels de cybersécurité (ANSSI[3], ISO 27001, NIS2).**

Il est aussi possible de **réaliser ces campagnes de manière ponctuelle** en fonction d'événements notables tels qu'un audit de maturité du SI ou la volonté de mettre en place un plan de sensibilisation aux dangers et menaces liés à la cybersécurité.

La campagne ponctuelle permet de réagir rapidement à un contexte à risque : suspicion de compromission, arrivée d'un nouveau collaborateur, ou à la suite d'un audit ou d'un test de pénétration. Elle sert d'outil de contrôle ciblé, agile et pertinent.

Les résultats vous permettent d'**identifier les points faibles**, d'**agir rapidement**, et de transformer vos collaborateurs en première ligne de défense. Parce qu'un simple clic peut suffire à compromettre tout un système, l'erreur humaine ne doit plus être un angle mort de votre stratégie cybersécurité.

La simulation de phishing évalue **la capacité des employés à reconnaître les attaques**, identifie les failles techniques et humaines, et renforce la sensibilisation à la sécurité.

Elle permet d'adapter les procédures et les formations pour mieux **protéger l'entreprise face aux menaces.**

Lexique

[1]Phishing (ou hameçonnage) : C'est une forme d'escroquerie sur internet. Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme.

[2]RGPD (Règlement Général sur la Protection des Données) : Loi européenne qui oblige les entreprises à protéger les données personnelles de leurs clients, utilisateurs ou employés, et à être transparentes sur la façon dont ces données sont collectées et utilisées.

[3]ANSSI : Autorité française chargée de protéger les systèmes d'information sensibles, de prévenir les cyberattaques et de guider les entreprises et institutions dans la mise en œuvre de bonnes pratiques de cybersécurité.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com