
Avant de Cliquer

Informations générales

SIRET

83208005500011

Responsable(s)

Stéphane Tabia et Carl Hernandez

Adresse

129 Rue Édouard Delamare Deboutteville

76160

Isneauville

France

Tél

0611127986

<https://www.avantdecliquer.com>

stephane@avantdecliquer.com

Présentation

Activité détaillée

Spécialiste en cybersécurité protégeant les entreprises contre l'hameçonnage, le phishing, les cyberattaques, le spear phishing et e-mails frauduleux qui sont devenus un véritable fléau pour les entreprises.

Avant de Cliquer crée sur mesure pour chaque salarié puis anime sur la durée, un programme de sensibilisation et de mise en situation, qui permet aux salariés de monter en compétence et à l'entreprise d'être davantage résiliente.

90 % des Cyberattaques ont pour origine un e-mail qu'un utilisateur sensibilisé n'aurait pas cliqué. Antivirus, pare-feux et autres logiciels de sécurité ne peuvent empêcher qu'un utilisateur effectue une action dangereuse. Seule une équipe sensibilisée par notre solution anti-phishing vous garantit de maintenir sur la durée un niveau élevé de vigilance des utilisateurs.

Une fois ce constat fait, [comment se protéger du phishing](#) ?

Voici comment Avant de Cliquer fonctionne

- 1- Nous sensibilisons les utilisateurs à l'aide de modules d'e-learning de 1 à 3 minutes.
- 2- Notre algorithme intelligent envoie aux utilisateurs des e-mails qu'ils ne devraient pas cliquer.
- 3- Les utilisateurs peu vigilants sont sensibilisés sur l'instant. Au moment où une erreur qui aurait pu être fatale est commise, l'utilisateur est invité à suivre une sensibilisation de 1 à 3 minutes, concernant l'e-mail qu'il a cliqué par manque de vigilance.
- 4- La gouvernance, la direction, le DSI, le responsable du système d'information ont accès à un tableau de bord permettant de piloter le cyber risque, de constater les améliorations, et de documenter les mesures organisationnelles proactives mises en place.

Sensibiliser les utilisateurs est une tâche laborieuse, coûteuse et chronophage.

Notre solution de [sensibilisation à la cybersécurité](#) est non intrusive et ne nécessite aucune modification de l'infrastructure de votre système d'informations. Confiez-nous cette responsabilité et concentrez-vos équipes informatiques sur des tâches à plus haute valeur ajoutée.

Pour en savoir plus :

- <https://videas.fr/share/d8baa00b-740b-4363-ad17-f72c3aeb1f4c/>
- <https://videas.fr/share/82d82df5-a807-4e26-aa6b-854d650e9b4b/>