Phished

Automated Security Awareness Training qui fonctionnent vraiment !

La plate-forme belge Phished fournit des simulations automatisées d'hameçonnage ainsi que des formations interactives à la cybersécurité et Threat Intelligence. Grâce à Phished, vos clients réduisent de 96 % les risques d'être victimes d'hameçonnage. Sans aucune intervention manuelle de leur part.

Comment fonctionne Phished ?

Intégration simplifiée dans Outlook

À intervalles réguliers, l'utilisateur reçoit un courriel simulant un hameçonnage, qu'il doit signaler comme tel en cliquant sur un bouton dans Outlook. La fréquence à laquelle ces simulations sont envoyées est négociée avec le client. La gestion de chaque e-mail de faux hameçonnage ne dure pas plus de 2 minutes et reste donc très accessible à tous. Les e-mails ne sont pas envoyés simultanément à tous les utilisateurs, leur contenu est également différent.

Formations interactives

Chaque utilisateur est invité à suivre une courte formation interactive tous les 15 jours. Elle dure 5 minutes environ et l'informe de divers risques et malentendus concernant la cybersécurité. Ses connaissances sont testées à l'aide de quelques questions. Les séances sont réparties sur des périodes assez longues afin de rappeler régulièrement à l'utilisateur la nécessité de rester attentif et conscient des dangers.

Compte rendu individuel

Le comportement de chacun est enregistré dans un rapport et exprimé sous forme de score comportemental. Chaque résultat est comparé à ceux des collègues, entre départements d'une même entreprise ou au niveau global.

90 % des cyberattaques commencent par une erreur humaine !

L'hameçonnage est le cas typique de tentative de cyberattaque. Les spécialistes sont unanimes à ce sujet : la formation des utilisateurs par la prise de conscience est aujourd'hui devenue indispensable.

Les techniques d'hameçonnage évoluent sans cesse

En cybersécurité, tout le monde est conscient que le maillon faible, c'est l'humain. C'est toujours à lui qu'il incombe de réagir, ou non, à une question contenue dans un e-mail, de cliquer sur un lien suspect, de partager ses propres données...
Mais pour remplir correctement leur travail, les collaborateurs doivent avoir accès à Internet et au courrier électronique. Impossible, par conséquent, de les bloquer. Cependant, ils peuvent également devenir des ressources, ce que l'on appelle "firewall-humains".

Avec Phished, l'utilisateur est entraîné par le biais de simulations d'hameçonnage et de formations interactives, pour améliorer sa capacité à détecter de faux e-mails ainsi que d'autres risques pour sa propre cybersécurité. Et celle de l'entreprise. Tout comme chacun est conscient de certains périls et veille à sa propre sécurité physique (par exemple en fermant la porte de son habitation), chacun, et pas seulement les spécialistes en IT, doit également s'impliquer dans la cybersécurité.

Afin de duper les utilisateurs, les pirates ne cessent de mettre au point de nouveaux modes opératoires toujours plus rusés. C'est pourquoi il faut affiner constamment les connaissances.

Que procure Phished ?

- Des **simulations automatisées** d'hameçonnage, créées par intelligence artificielle, dans plusieurs langues courantes, personnalisées pour chaque destinataire.
- Des **simulations manuelles** sont possibles à l'aide d'un puissant éditeur.
- **Tous les types** d'hameçonnages courants : spear phishing, fraude CEO, NSFW, faux e-mails relatés à l'emploi et au secteur d'activité de l'entreprise, smishing...
- Des formations localisées basées sur **l'intelligence artificielle**, données dans la Phished Academy (infographies, vidéos, jeux de questions-réponses) sur des sujets variés concernant la cybersécurité.
- Des comptes rendus élaborés des prestations du personnel : pour chaque utilisateur, par département, par site ou par comparaisons entre sociétés actives dans un même secteur.
- Des mesures approfondies **de sécurité et de respect de la vie privée** : certification ISO 27001, RGPD, chiffrement d'enveloppe.
- Activer les utilisateurs avec **le bouton Phished Report** : il scanne tous les messages suspects, même ceux qui ne sont pas des simulations.

PHISHED

Intéressé par nos services ?
N'hésitez pas à nous contacter !
www.clearmedia.be

ClearMedia NV
Merksemsesteenweg 148
2100 Deurne

+32 3 658 00 36
info@clearmedia.be
BE 0831 425 897

ClearMedia
A Proximus company