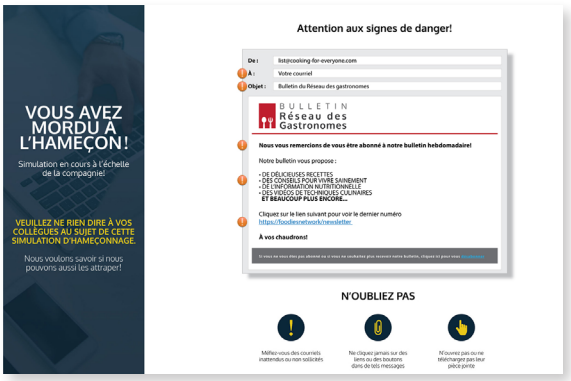
PLATEFORME DE SIMULATIONS DE PHISHING

TERRANOVA SECURITY

Les simulations de phishing en temps réel constituent un moyen rapide et efficace de sensibiliser les utilisateurs et d'augmenter leurs niveau de vigilance aux attaques de phishing, notamment : les logiciels malveillants, les ransomwares, le spear phishing, la fraude du chef d'entreprise (CEO Fraud) et BEC. Les simulations permettent de renforcer les capacités de détection et d'intégrer les bonnes pratiques de cybersécurité dans votre entreprise.

Les entreprises du monde entier utilisent la puissante plateforme de simulations de phishing de Terranova Security pour mesurer la vulnérabilité des utilisateurs face aux menaces de phishing tout en renforçant leur vigilance face aux cyber-attaques.



QUATRE MOYENS D'AUGMENTER L'EFFICACITÉ DES SIMULATIONS DE PHISHING

1. Atteignez tous vos utilisateurs avec des simulations évolutives

La solution cloud évolutive est conçue pour prendre en charge un grand nombre d'utilisateurs et accroître l'agilité de l'entreprise, tout en prenant les mesures nécessaires pour sécuriser vos données et garantir la confidentialité et la conformité à l'échelle de l'entreprise.

2. Planifiez vos simulations avec la distribution flexible et personnalisable

Planifiez vos simulations à l'avance et organisez l'envoi des messages par lots sur une période donnée. La flexibilité de la personnalisation et de la distribution sont également des fonctionnalités importantes. Simulations planifiées / automatisées et aléatoires.

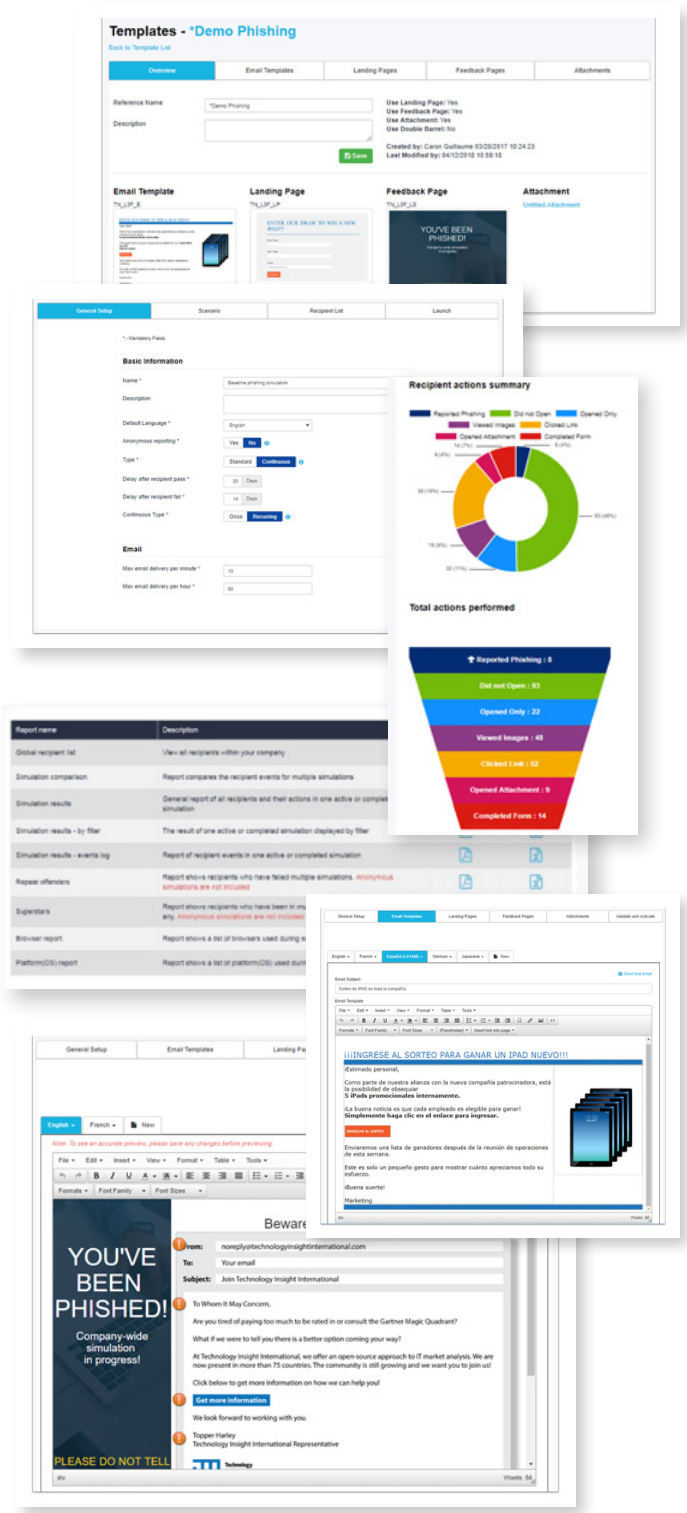
3. Ciblez les utilisateurs à haut risque en fonction des rapports ciblés et exhaustifs

Créez une liste d'utilisateurs à cibler en fonction des résultats des simulations précédentes. Les fonctionnalités de la plateforme doivent produire des rapports permettant aux entreprises de suivre les utilisateurs qui ont échoué la simulation et ainsi bâtir une nouvelle liste ou un nouveau groupe et recibler cette clientèle spécifique.

4. Affichez les résultats de la campagne par listes ou groupes cibles

Créez des listes spécifiques et affichez les résultats en fonction du pays, de la division, du département ou d'autres paramètres. Les entreprises doivent avoir l'option de sélectionner les utilisateurs ciblés pour une campagne donnée, que ce soit au hasard parmi l'ensemble des utilisateurs, à partir d'une liste préétablie ou d'un département spécifique.

FONCTIONNALITÉS CLÉS POUR DES SIMULATIONS DE PHISHING CIBLÉES ET UNE EXPÉRIENCE MULTILINGUE



Scénarios personnalisables basés sur des exemples réels

Profitez d'une riche sélection de scénarios (courriers électroniques, pages de renvoi et matériel d'apprentissage) facilement personnalisables et les simulations évolutives basées sur les menaces les plus courantes.

Phishing automatisé et aléatoire

Configurez vos simulations pour une exécution automatique et continue exploitant plusieurs scénarios. Choisissez le mode aléatoire pour augmenter la difficulté à détecter les simulations.

Analyses et rapports

Observez les résultats de votre campagne et découvrez le pourcentage d'utilisateurs ayant signalé, ouvert un email de simulation, visionné des images, cliqué sur des liens et ouvert des pièces jointes.

Générez des rapports prédéfinis avec des données détaillées sur les résultats de la simulation, des clics répétés, des superstars et des comparaisons entre les simulations.

Mises à jour mensuelles des fonctionnalités et des scénarios

Profitez des mises à jour mensuelles pour obtenir les derniers scénarios de phishing élaborés par des experts du secteur et tirez parti des plus récentes fonctionnalités de notre plateforme SaaS.

Formation juste à temps

Combinez le potentiel d'apprentissage du phishing avec la formation juste à temps. Redirigez les utilisateurs vers une page d'apprentissage avec du matériel de formation approprié lié au comportement que vous souhaitez améliorer.

DEMANDEZ VOTRE ESSAI GRATUIT DE 30 JOURS DE SIMULATION DE PHISHING:

TERRANOVASECURITY.COM

TERRANOVA SECURITY