FORTRA™

GUIDE (TERRANOVA SECURITY)

Comment protéger vos données des attaques d'ingénierie sociale

TABLE DES MATIÈRES

Qu'est-ce que l'ingénierie sociale?

L'ingénierie sociale est une technique de manipulation utilisée par les cybercriminels pour inciter les gens à effectuer une action à l'avantage du criminel. Ces cybercriminels sont des escrocs qui utilisent la technologie pour tromper leurs victimes.

Toute cyberattaque réussie qui utilise l'ingénierie sociale exploite un instinct humain de base : la confiance. Une fois ce lien établi, un fraudeur peut voler des données sensibles et les utiliser pour commettre d'autres crimes dans le futur.

Prenons l'exemple suivant : un cybercriminel espère convaincre un employé de divulguer des mots de passe qui protègent des données organisationnelles confidentielles. Pour ce faire, il peut utiliser des tactiques d'ingénierie sociale et masquer ses intentions réelles derrière un message qui semble provenir d'un centre d'assistance, d'un fournisseur de service ou d'un système, et demandant la validation d'un compte.

Dans d'autres cas, les victimes d'attaques d'ingénierie sociale croient qu'elles aident une connaissance à régler un problème urgent. En réalité, elles s'exposent à des brèches de sécurité qui peuvent causer la fuite de données ou l'installation d'un maliciel sur les appareils ou les réseaux de l'entreprise.

Il suffit d'un courriel, d'un appel téléphonique ou d'un message texte qui semble provenir d'une personne ou d'une organisation connue pour se faire prendre au piège. Lorsque la tromperie fonctionne et que l'attaque réussit, les cybercriminels peuvent exposer des données sensibles et les utiliser à leur avantage, ou prendre le contrôle d'appareils, de systèmes et de réseaux.

Selon des données de 2020, le tiers de toutes les brèches sont causées par une forme d'hameçonnage ou d'ingénierie sociale. Il peut être difficile de se protéger contre cette dernière puisque la technologie ne peut arrêter 100 % des attaques, et que les êtres humains sont de nature imprévisible. Pour éviter de tomber dans ce genre de piège, tous les membres d'une organisation doivent demeurer vigilants.

Pourquoi l'ingénierie sociale est-elle si efficace

En bref, l'ingénierie sociale est dangereuse parce que les gens font des erreurs.

Même si les victimes savent qu'elles doivent se méfier des courriels qui, par exemple, leur promettent un remboursement, ou des appels téléphoniques qui les menacent d'être arrêtées si elles refusent de divulguer des informations sensibles, elles peuvent toujours être prises au dépourvu.

La réussite des arnaques d'ingénierie sociale se base sur la réaction instinctive de l'humain à faire confiance à l'expéditeur d'un message, qui l'emporte souvent sur les habitudes établies de sensibilisation à la cybersécurité. Le fait d'être occupé, de ne pas être suffisamment attentif, d'être complaisant ou simplement d'oublier les règles de base de la cybersécurité – toutes ces erreurs peuvent amener les utilisateurs à être trop confiants.

Pour toutes ces raisons, il n'est pas rare que certaines personnes soient victimes à répétition d'attaques d'ingénierie sociale. En effet, pour changer les comportements humains individuels, particulièrement lorsqu'il s'agit d'inverser des mauvaises habitudes, il ne suffit pas de savoir quoi repérer.

Parce qu'elle permet d'exploiter les faiblesses d'un réflexe humain, il est beaucoup plus facile pour les cybercriminels d'utiliser l'ingénierie sociale pour pirater une personne que de pirater les systèmes ou le réseau d'une organisation.

En priorisant une approche à la cybersécurité centrée sur les personnes, vous pouvez fournir à l'ensemble de vos utilisateurs les outils nécessaires pour esquiver les tentatives d'ingénierie sociale et protéger leurs données en tout temps.

Par conséquent...

Le nombre de brèches de données a connu une croissance significative dans les dernières années. Les cyberattaques ont exposé plus de quatre milliards de dossiers d'utilisateurs dans la première moitié de 2019 seulement. Ajoutez à cela les cliqueurs en série et des formations en sensibilisation à la sécurité inefficaces pour que le facteur de risque d'une organisation augmente substantiellement.

Comment les attaques d'ingénierie sociale exploitent les émotions humaines

Les meilleurs exemples d'ingénierie sociale sont ceux qui jouent toutes les bonnes notes sur la gamme émotionnelle de la victime. Si l'utilisateur ne possède pas la formation appropriée pour reconnaître les scénarios d'une attaque d'ingénierie sociale commune, ils peuvent être difficiles à identifier.

Voici certaines des émotions exploitées par les cybercriminels pour commettre une arnaque d'ingénierie sociale :

Peur

Dans la plupart des cas, la manipulation par la peur implique une menace avec des conséquences graves si la victime ne réagit pas rapidement. Il peut s'agir d'un message vocal affirmant que vous êtes sous enquête pour fraude fiscale et vous ordonnant de rappeler immédiatement pour prévenir une enquête criminel. Cette forme de leurre est très puissante, en particulier pendant la saison des impôts où le stress concernant les finances est élevé.

Cupidité

Imaginez que vous puissiez transférer 10 $ à un investisseur et voir ce montant augmenter à 10 000 $, le tout sans effort de votre part. Les cybercriminels jouent avec la confiance et la cupidité pour convaincre leurs victimes qu'elles peuvent obtenir quelque chose gratuitement. Un courriel composé avec soin peut amener les victimes à partager leurs informations bancaires en échange de la promesse que des fonds leurs seront transférés sous peu.

Curiosité

Des évènements bénéficiant d'une large couverture médiatique peuvent servir à profiter de la curiosité humaine et à inciter les victimes à agir. Par exemple, après le deuxième écrasement d'un Boeing MAX8, des cybercriminels ont envoyé des courriels avec des pièces jointes contenant prétendument des fuites d'information concernant l'incident. En cliquant sur la pièce jointe, un logiciel malveillant était installé sur l'ordinateur de la victime.

Serviabilité

En faisant une recherche sur une organisation, les cybercriminels peuvent cibler une poignée d'employés avec un courriel semblant provenir de leur(s) gestionnaire(s). Le courriel demande aux victimes d'envoyer leurs identifiants et mots de passe à leur « gestionnaire » pour des raisons administratives ou comptables, en précisant que ces informations sont nécessaires pour que tous reçoivent leur paie à temps. Le ton urgent déclenche notre instinct naturel à vouloir aider.

Sécurité

Ironiquement, beaucoup d'attaques d'ingénierie sociale s'articulent autour d'une demande visant à protéger les données sensibles des utilisateurs. Elles peuvent prendre la forme d'un courriel envoyé par le soutien à la clientèle d'un détaillant en ligne de confiance et demandant des informations sur votre carte de crédit pour sécuriser votre compte. En tirant profit de l'image de marque d'une entreprise, et même de certaines parties de son site Web, les cybercriminels réussissent à faire paraître ces messages encore plus réels.

Comment repérer les tactiques communes d'ingénierie sociale

En fin de compte, la force du facteur humain de la cybersécurité est limitée par sa capacité à détecter et à éviter les menaces.

Chaque personne au sein d'une organisation, des employés de première ligne aux gestionnaires et aux dirigeants, doit savoir à quoi ressemble une attaque d'ingénierie sociale. Autrement, le risque d'exposition de données ou de systèmes par une pièce jointe ou un lien malveillant peut augmenter significativement.

Examinons de plus près les différentes formes que peuvent prendre les tentatives d'ingénierie sociale.

Appâtage

L'appâtage est un type d'attaque d'ingénierie sociale qui peut survenir en ligne et en personne et qui promet quelque chose à la victime en échange d'une action. Par exemple, brancher une clé USB ou télécharger une pièce jointe en échange d'un accès à vie à des films gratuits. L'ordinateur et le réseau peuvent être la cible d'un maliciel qui capture les données d'accès ou envoie de faux courriels.

Suppression d'un maliciel

Les cybercriminels envoient un message indiquant que l'appareil de la victime est contaminé par un virus ou un logiciel malveillant, et proposant de lui vendre un outil qui permettra de le supprimer. Selon l'arnaque, le criminel s'en tient à voler les informations de carte de crédit de la victime ou en profite pour installer un vrai maliciel ou rançongiciel sur l'ordinateur. Gardez l'œil ouvert pour les maliciels – près de 95 % des charges sont livrées de cette façon.

Hameçonnage

L'hameçonnage englobe un large éventail de tactiques sournoises, y compris des courriels trompeurs, des faux sites Web et des messages textes fallacieux. Ils ont tous le même objectif : voler des données confidentielles appartenant à un individu ou à une organisation. En général, les attaques d'hameçonnage fonctionnent lorsqu'elles semblent provenir d'une connaissance ou d'une organisation de confiance.

Prétexter

Il s'agit d'une technique d'ingénierie sociale qui utilise une fausse identité pour amener la victime à partager des informations sensibles. Par exemple, le cybercriminel peut savoir que la victime a récemment acheté un article chez Apple et prétendra être un représentant du service à la clientèle pour obtenir ses informations de carte de crédit ou d'autres détails confidentiels.

Contrepartie

L'arnaque de la contrepartie (ou quid pro quo) compte sur un échange d'information pour convaincre la victime d'agir. Souvent, un service est offert en échange d'un bénéfice. Une technique commune implique que le criminel se fasse passer pour un employé du soutien informatique. Il appelle les victimes ayant récemment ouvert des tickets d'assistance technique et leur promet de régler un problème de virus en échange de leurs données d'accès.

Harponnage

Le harponnage est un cybercrime qui utilise des messages pertinents et bien conçus pour mener des attaques ciblées contre des individus et des entreprises. Les pirates recueillent des données sur leurs cibles et utilisent ces informations pour envoyer des courriels qui semblent familiers aux victimes. Même si le harponnage est surtout utilisé pour voler des données, il peut également permettre d'installer un maliciel ou un rançongiciel sur l'appareil de la victime.

Talonnage

Le talonnage est une technique d'ingénierie sociale qui mise sur la confiance pour accéder physiquement à un bâtiment ou à la zone sécurisée d'un bâtiment. Le criminel peut simplement entrer par une porte ouverte en suivant quelqu'un de près ou demander l'accès en prétendant avoir oublié sa carte magnétique. Cette arnaque met l'emphase sur le besoin de prêter attention aux gens qui traînent près de la porte et de ne pas hésiter à demander une identification.

Hameçonnage vocal

L'hameçonnage vocal (vishing) utilise des appels téléphoniques ou la messagerie vocale pour convaincre les victimes qu'elles doivent agir rapidement. Généralement, les messages font planer la menace d'une action judiciaire ou d'une attaque criminelle. Par exemple, un criminel pourrait laisser un message vocal incitant la victime à réinitialiser ses informations bancaires parce que son compte a été piraté.

Attaque de point d'eau

L'attaque de point d'eau (water-holing) cible un groupe d'utilisateurs ainsi que les sites Web qu'ils fréquentent. Le cybercriminel explore ces sites Web à la recherche d'une faille de sécurité puis les infecte avec un maliciel. L'un des membres du groupe ciblé est éventuellement contaminé par le maliciel. Cette technique d'ingénierie sociale est très spécifique et difficile à détecter.

Comment protéger vos données des attaques d'ingénierie sociale en 7 étapes

Le simple fait d'organiser un séminaire ponctuel sur l'ingénierie sociale, ou de demander à vos utilisateurs de visionner quelques vidéos éducatives sur le sujet, ne permettra pas de protéger pleinement les données de votre organisation.

Investissez plutôt dans la réussite de vos employés en construisant, entretenant et optimisant une infrastructure de formation en sensibilisation à la sécurité. Cela contribuera à maintenir tout le monde à jour sur les plus récentes menaces et aidera les utilisateurs à retenir les informations et les compétences qui permettront d'assurer une cybersécurité constante.

Voici quelques éléments clés à considérer :

1. Investissez dans le changement de comportement

Pour réduire efficacement le risque humain, mettez l'emphase sur une formation en sensibilisation à la sécurité qui encourage le changement de comportement. Tirez profit d'outils comme les simulations d'hameçonnage et de rançongiciels, ainsi que des évaluations de cybersécurité qui permettront de renforcer votre organisation.

2. Formez vos employés avec du contenu efficace

Un contenu éducatif de qualité est sans doute le facteur le plus important de toute initiative de sensibilisation à la sécurité. Utilisez des ressources comme les cours en ligne, les modules de micro et de nanoapprentissage et les nanovidéos pour former votre équipe sur les arnaques d'ingénierie sociale. La présentation d'exemples concrets permet également de montrer à quel point il est facile pour quiconque d'être pris au dépourvu par des tactiques liées.

3. Exposez les utilisateurs à des simulations d'hameçonnage pratiques

Le contenu éducatif est important, mais il est grandement amélioré lorsque combiné à des simulations pratiques qui permettent de tester les connaissances de l'utilisateur dans un environnement sécuritaire. Utilisez les simulations d'hameçonnage et d'autres mises en scène pour approfondir les expériences d'apprentissage et contribuer à la promotion d'un changement de comportement positif.

4. Des informations à jour pour tous

Le contenu et les simulations doivent être continuellement mis à jour et redéployés pour s'assurer que chacun est connaît les cybermenaces en circulation. En partageant cette information avec les employés, vous augmentez les chances qu'ils soient en mesure d'identifier et d'éviter les tentatives d'ingénierie sociale.

5. Créez et encouragez une culture axée sur la sécurité

L'un des aspects sous-estimés du processus de protection des données concerne la culture de sécurité d'une organisation. En commençant par le sommet, la création et la promotion d'un environnement propice au changement de comportement doit représenter une priorité majeure. Cela permettra de stimuler l'apprentissage et de soutenir une sensibilisation à la sécurité unilatérale. Encouragez les utilisateurs à rapporter les activités suspectes, même après qu'ils aient été victimes d'une attaque.

6. Encouragez et récompensez les ambassadeurs des organisations

Durant le processus de formation en sensibilisation à la sécurité, il est important d'identifier et de récompenser des ambassadeurs de programme internes pour maintenir un niveau d'intérêt élevé. Créez un groupe interne de héros de la cybersécurité engagés à maintenir la sécurité de votre organisation afin d'encourager l'adhésion de tous les employés.

7. Du soutien continu avec des campagnes engageantes

Utilisez des outils de communication engageant et planifiez des communications et des campagnes en continu sur l'ingénierie sociale, la cybersécurité et l'hameçonnage. Cela contribuera à alimenter les conversations et la sensibilisation aux risques qui peuvent émaner de courriels, d'URL, de pièces jointes et d'appels téléphoniques suspects, et de toute autre forme d'attaques d'ingénierie sociale.

Ressources supplémentaires

Billets de blogue

- 9 exemples d'attaques d'ingénierie sociale
- Ce que la fraude chez Twitter a révélé sur l'ingénierie sociale
- Principaux types de courriels d'hameçonnage

Livres numériques gratuits

- Améliorez les stratégies et les défenses de votre organisation contre l'hameçonnage (en anglais)
- The Human Fix to Human Risk (en anglais)

Cyberpédia

- Ingénierie sociale
- Hameçonnage

Ressources (en anglais)

- Principaux faits, tableaux et statistiques sur la cybersécurité pour 2020 (CSO Online)
- Rapport d'enquête sur les brèches de données 2020 (Verizon)
- Rapport QuickView sur les brèches de données 2019 (RiskBased Security)

FORTRA™

Fortra.com

À propos de Fortra

Fournisseur de logiciels de cybersécurité unique sur le marché, Fortra propose à ses clients un futur à la fois plus simple et plus résilient. Nos experts et notre portefeuille, riche de solutions évolutives et intégrées, offrent aux entreprises du monde entier une maîtrise et un équilibre accrus. Acteurs du changement positif, nous vous accompagnons à chaque étape de votre parcours de cybersécurité et vous aidons à garder l'esprit serein. Pour en savoir plus, rendez-vous sur fortra.com/fr.

 (fta-tn-gd-0424-r1-79d)