Les 5 techniques de phishing les plus courantes | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

L'ère des attaques ciblées est en marche

Le spam est aujourd'hui plus une nuisance qu'une réelle menace. En effet, les tentatives de vendre du vi@gra ou encore de recevoir l'héritage d'un riche prince d'une contrée éloignée ne font plus beaucoup de victimes. La majorité des solutions antispam bloquent ces emails et l'unique façon de les voir consiste à consulter votre dossier « courrier indésirable ». Toutefois, une menace bien plus sophistiquée et dangereuse atterrit dans votre boîte de réception. Vous ciblant vous et vos employés.
Connu sous le nom de « phishing » ou « hameçonnage », ces emails cherchent à piéger vos employés. Comment ? Simplement en leur demandant d'effectuer une action. Dans la vie, il y a deux façons d'obtenir ce que l'on veut : soit le demander gentiment, soit être la bonne personne (et avoir l'autorité qui convient). Le phishing et son cousin le spear phishing, rassemblent ces deux conditions. Le principe du phishing consiste à usurper l'identité d'une personne ou d'une organisation et simplement demander d'exécuter une action (modification de mot de passe, vérification d'une pièce jointe, etc.). L'attaque est orchestrée autour de deux éléments : l'email et le site web ou une pièce jointe. L'email de phishing demande à ses victimes de se connecter à une page et d'entrer leurs identifiants afin d'effectuer une action qui semble légitime. Concrètement, il s'agit par exemple de faux emails de votre fournisseur d'électricité vous avertissant de régulariser votre facture… au plus vite !

L'impact du phishing en entreprise
Des milliers de phishing sont envoyés quotidiennement (contre des millions pour le spam) par des organisations de cybercriminels ou des gouvernements étrangers (ou les deux quand ce dernier « soustraite »).
Cette menace n'est pas encore bien maîtrisée par la majorité des antispam et anti-virus sur le marché pour plusieurs raisons. Premièrement, le « faible » volume d'emails de phishing ne permet pas d'être détecté par la majorité des solutions reposant sur une base de signatures. Deuxièmement, l'email semble légitime et ne reprend pas les « codes » du spam.
Le phishing est une réelle menace pour les entreprises, car il y a deux façons d'être victime : voir sa marque usurpée ou tomber dans le piège quand on reçoit l'email.
Dans les deux cas, voici les 4 principaux dégâts que le phishing peut causer à votre entreprise :
Nuire à votre réputation si votre marque est utilisée pour duper des internautes. Bien souvent, vous ne savez même pas que votre marque est utilisée à des fins malicieuses.
Perte de données sensibles, de propriétés intellectuelles ou encore de secrets industriels.
Divulgation de vos données clients et partenaires.
Des pertes financières directes liées au vol, à des amendes ou au dédommagement de tiers.
Selon une étude de l'américain Verizon, 11% des récepteurs de phishing cliquent sur le lien !

Les 5 techniques de phishing les plus répandues
Pas si évident que cela à identifier. Tout le monde peut se laisser duper par manque de vigilance par un email de phishing, car celui ci semble légitime et original.
Voici ci-dessous les 5 techniques qu'utilisent les phisheurs pour attaquer votre entreprise. Dans nos exemples, nous parlerons de Pierre, un salarié aux responsabilités moyennes, travaillant dans le service finance de son entreprise, et qui a des journées biens remplies.
Le premier exemple de la série correspond à un phishing de masse, alors que les 4 suivants seront plus ciblés, reprenant l'art du Spear Phishing, qui nécessite des recherches avancées sur les cibles afin d'être crédible et de présenter l'autorité qui convient. Dans ces cas là, Alain sera le patron de Pierre, information facilement trouvable sur le site internet de la société.

1. Abus de confiance
Pierre reçoit un email lui demandant de confirmer un transfert d'argent. L'email contient un lien envoyant vers un site qui se présente comme celui de sa banque… mais en réalité il s'agit d'une copie, éditée, contrôlée et hébergée par des pirates. Une fois sur la page, Pierre entre normalement ses identifiants mais rien ne se passe et un message disant que le site est « temporairement indisponible » apparaît. Pierre étant très occupé, se dit qu'il s'en occupera plus tard. En attendant, il a envoyé ses codes d'accès aux pirates.

2. Fausse loterie
Pierre reçoit un email lui indiquant qu'il a gagné un prix. Habituellement Pierre n'y prête pas attention, car bien trop occupé. Toutefois, cette fois ci, l'email est envoyé par Alain, mentionnant une organisation caritative qu'ils soutiennent mutuellement. Pierre clique alors sur le lien, rien ne se passe à l'écran, mais un malware s'est installé sur son poste de travail.

3. Mise à jour d'informations
Pierre reçoit un email d'Alain lui demandant de regarder le document en pièce jointe. Ce document contient un malware. Pierre ne s'est rendu compte de rien, en ouvrant le document, tout semblait correct bien qu'incohérent par rapport à son travail. Résultat, le malware enregistre tout ce que fait Pierre sur son poste (keylogger) depuis des mois, ce qui met en danger tout le Système d'Information de l'entreprise facilitant le vol de données.

4.Appel à donation
Pierre reçoit un email du frère d'Alain, lui disant qu'il est atteint d'un cancer et que sa couverture sociale s'est arrêtée. Voulant faire bonne impression auprès de son patron, Pierre clique sur le lien et se rend sur le site de donation dédié. Pierre décide de faire une donation de 100€ et entre ses informations bancaires. Le site précise même que le don est déductible des impôts… Trop tard, Pierre a donné ses informations et se fait débiter d'un montant bien supérieur ! Sans pouvoir le déduire de ses impôts…

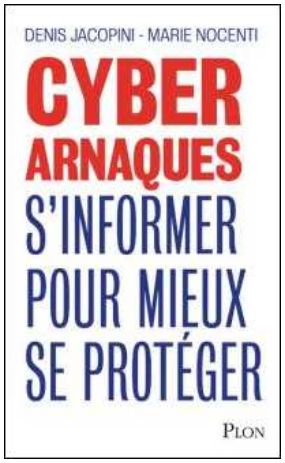
5. Usurpation d'identité
Pierre reçoit un email d'Alain, lui demandant d'effectuer un virement auprès d'un fournisseur connu au sujet d'une avance concernant un dossier urgent. Pour Pierre, il s'agit d'une tâche de routine qu'il effectue aussitôt. L'argent est envoyé sur un compte étranger, impossible à tracer et ne sera jamais retrouvé.

Les attaques de phishing et spear phishing sont en augmentation, tant sur le nombre que sur leur niveau de sophistication. Si vos employés reçoivent ce type d'email il y a de forte chance qu'ils se fassent piéger.

Qu'est ce qui peut être fait pour protéger vos employés ?
Pour se protéger contre phishing, la majorité des entreprises se contentent de leur antispam et d'autres logiciels anti-virus ou de blocage des sites web. Toutefois, face à l'augmentation et à la sophistication des attaques, cette menace nécessite une protection dédiée. Les solutions antispam et virus classiques ne sont plus suffisantes. Il reste la formation des employés, efficace mais trop peu utilisée et qui nécessite d'être régulière.
Les organisations ont besoin de solutions dédiées à cette menace qu'est le phishing qui nécessite une analyse particulière pour être identifiée et bloquée. Les cybercriminels font évoluer leurs techniques rapidement mais la riposte technologique s'organise également, et certaines solutions anti-phishing sont désormais capables de bloquer tous les types de phishing et spear phishing en analysant chaque lien ainsi que les habitudes des échanges. Mais au delà de ce socle technologique nouveau et efficace, l'arme ultime pour contrer les phishing reste l'humain, et sur ce point le travail de formation et d'éducation reste énorme !

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Les 5 techniques de phishing les plus courantes | Programmez!*