N’importe qui peut être victime d’escroquerie et d’hameçonnage, avec des exemples

Blog de formation en sensibilisation à la sécurité

Roger Grimes :

J’ai récemment lu un article sur une femme brillante et sophistiquée qui a été victime d’une escroquerie incroyable.
Par incroyable, je veux dire que la plupart des gens qui lisent ou entendent parler de cela ne peuvent pas croire que c’est un succès.

Un groupe se faisant passer pour un employé d’Amazon et divers organismes d’application de la loi américains ont réussi à convaincre une femme de retirer 50 000 dollars de son compte bancaire en espèces et de les remettre à un parfait inconnu dans la rue.
C’est une histoire folle et la plupart d’entre nous ne se laisseraient pas piéger par ce qui lui est arrivé.

Je pense que la plupart des gens ne peuvent pas croire qu’elle l’a fait et beaucoup pensent qu’elle est soit stupide, soit trop naïve.
Ce n’est pas vrai.

L’intelligence et l’intelligence de la rue n’ont pas grand-chose à voir avec le fait que vous soyez finalement escroqué ou non.
Je pense que le fait d’être intelligent et « intelligent dans la rue » peut vous rendre moins susceptible d’être victime d’une arnaque dans de nombreuses situations, peut-être dans la plupart des scénarios.
Mais des médecins, des avocats, des ingénieurs, des propriétaires d’entreprises prospères, des scientifiques spécialisés dans les fusées et même des lauréats du prix Nobel de physique ont été escroqués avec succès.
Beaucoup de gens qui pensaient qu’ils étaient super intelligents et non arnaqueurs ont été arnaqués.

La vérité est que n’importe qui peut être victime d’une arnaque. N’importe qui peut être victime d’hameçonnage.
N’importe qui est susceptible d’être victime de la « bonne » arnaque dans les bonnes conditions.
Et si vous pensez que vous n’êtes pas escroqué ou que vous ne pouvez pas être hameçonné, cette attitude pourrait nuire à vos propres intérêts à long terme.

Il peut s’agir d’une escroquerie multicanal très sophistiquée ou simplement des conditions et des circonstances appropriées.
Je connais des gens très brillants et compétents qui se sont fait piéger en cliquant sur un lien malveillant simplement parce qu’ils étaient très occupés et qu’ils essayaient de faire 10 choses en même temps.
Ils n’étaient pas attentifs et concentrés, et cela leur a coûté cher.

Parfois, c'est simplement que l'escroquerie est arrivée avec des attributs particuliers au moment exact où la personne était confrontée à une situation similaire.
Je connais une personne qui vient de signaler une expérience négative d'Uber et qui a ensuite reçu un courriel de « Uber », a cliqué sur le lien inclus et s'est retrouvée avec un logiciel malveillant sur son téléphone.
Une autre personne m'a raconté qu'elle avait reçu une demande de l'adresse courriel de son ex-femme pour trois cartes-cadeaux juste avant Noël et qu'elle élevait trois enfants. Cela semblait être une demande plausible.

Quelle que soit la raison, nous sommes tous vulnérables aux escroqueries et aux attaques de phishing.
Et si vous pensez que ce n'est pas le cas, vous mangerez peut-être une humble tarte un jour.

Quelques exemples d'escroqueries réalistes

Permettez-moi de vous donner quelques exemples d'escroqueries et d'événements d'hameçonnage uniques qui peuvent mener à des compromissions indésirables contre n'importe qui, si les circonstances s'y prêtent.

Faux support client

Une fois, après ne pas avoir obtenu satisfaction concernant un nouveau réfrigérateur coûteux que j'ai acheté, frustré, j'ai posté ma plainte sur la page Facebook du vendeur.
En quelques minutes, quelqu'un utilisant une adresse courriel très valide liée au domaine du fournisseur, m'a envoyé un courriel pour me dire qu'il avait lu ma plainte.
C'était quelque chose comme customerservice@GEresolutiondesk.com.

Ils se sont excusés et m'ont proposé de m'envoyer immédiatement un réfrigérateur de remplacement.
Tout ce que j'avais à faire était de leur donner les informations de ma carte de crédit afin qu'ils puissent me facturer si je ne renvoyais pas l'ancien réfrigérateur comme promis.
J'ai failli tomber dans le panneau.
Ce n'est que par hasard que j'ai appelé le numéro légitime 1-800 du vendeur avec lequel je traitais déjà depuis des mois pour obtenir plus d'informations que j'ai appris que le courriel que j'avais reçu était une arnaque complète.

Fausse invitation à une conférence

Je suis invité à prendre la parole lors de conférences sur une base quotidienne.
Une fois, j'ai reçu une demande pour prendre la parole lors d'une conférence à l'étranger, tous frais payés, et le vendeur a dit qu'ils paieraient pour la visite de ma femme et moi et nous emmèneraient à travers le pays sur divers sites touristiques.
Ils m'ont dit que beaucoup de mes amis de l'industrie y allaient aussi.
Bien que je ne reçoive pas ce type d'offre tout le temps, cela m'est arrivé à quelques reprises dans le passé.

Qui n'a pas envie d'un voyage gratuit dans un pays étranger pour faire une présentation rapide ?
J'ai répondu que je serais heureux d'accepter la demande.
Ils m'ont envoyé un e-mail contenant un lien d'inscription au site Web.
J'ai cliqué sur le lien et cela m'a amené sur le site Web de la conférence.
Ce site Web m'a demandé de créer un compte ou de me connecter à l'aide de n'importe quelle liste de

connexions partagées communes (OAuth)**, par exemple en utilisant mon compte Google, LinkedIn ou Apple.
J'avais fait beaucoup de recherches sur OAuth à l'époque et j'ai décidé de regarder le code sous-jacent.

***OAuth** (**O**pen **Auth**orization) est un protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur.*

*OAuth **n'est pas** un protocole d'authentification, mais de « délégation d'autorisation ».*

OAuth permet à l'utilisateur de donner, au site ou logiciel « consommateur », l'accès à ses informations personnelles qu'il a stockées sur le site « fournisseur » de service ou de données, ceci tout en protégeant le pseudonyme et le mot de passe des utilisateurs.
Par exemple, un site de manipulation de vidéos pourra éditer les vidéos enregistrées sur Dailymotion d'un utilisateur des deux sites, à sa demande.

Ce n'était pas du tout OAuth.
Toute personne qui cliquerait sur ces liens partagerait son nom d'utilisateur et son mot de passe OAuth avec le site Web étranger.
J'ai rapidement reculé.
Tout cela n'était qu'une arnaque.
Voici un exemple de ce genre d'attaque.

Conduite d'eau défectueuse

Beaucoup de gens me disent qu'ils ne peuvent pas se faire arnaquer.
Quand je suis assez ennuyé, je leur demande s'ils seront prêts à parier 1 000 $ que je ne peux pas les arnaquer ?
Je veux dire par là, puis-je créer une fausse expérience d'escroquerie avec laquelle ils s'engagent, qui, s'il s'agissait d'une arnaque réelle, aurait abouti à leur exploitation ? Beaucoup ont accepté mon pari.
J'ai toujours réussi à les arnaquer.

Un stratagème courant que j'utilise consiste à rechercher leur adresse postale actuelle, ainsi que leur numéro de téléphone et une adresse courriel personnelle ou un service qu'ils utilisent (par exemple, Google, Hotmail, leur banque, leur courtier en valeurs mobilières, etc.).
Je passe au peigne fin leurs publications passées sur des sites de blogs pour apprendre toutes les informations que je peux à leur sujet, puis je les utilise dans mon escroquerie.

Par exemple, je leur enverrai un faux message texte apparaissant comme un numéro de téléphone dans leur indicatif régional local, semblant provenir du service d'eau ou d'assainissement de leur comté.
Je leur enverrai un texto du genre : « Avertissement sur l'eau et l'assainissement du comté de Monroe !
Il y a eu un bris majeur de conduite d'eau qui a eu un impact sur votre résidence située au 500 Lorelane Place, Key Largo, FL.
Veuillez ne pas boire ou utiliser l'eau du comté jusqu'à nouvel ordre.
Souhaitez-vous être avisé lorsque la conduite d'eau principale est réparée et qu'il est à nouveau possible de boire l'eau en toute sécurité (O/N) ?

Ils répondent toujours que oui.

Ensuite, je leur envoie un autre message indiquant : « Vous recevrez un code de confirmation à 6 chiffres d'un autre numéro pour confirmer votre inscription aux mises à jour de statut proactives.
Veuillez retaper ce code en réponse à ce message pour confirmer votre inscription. Ensuite, je me rends sur leur service de messagerie privé (par exemple, Google Gmail), leur banque (par exemple, Morgan Stanley) ou leur compte d'actions (par exemple, Fidelity Investments) et je leur dis que j'ai perdu mon mot de passe ou mon code d'identifiant à deux facteurs MFA.

Cela met le compte en mode de récupération de compte.
Le service enverra presque toujours un code de confirmation au numéro de téléphone valide de l'utilisateur.
Ainsi, la victime obtient le code de confirmation à 6 chiffres qu'elle attendait et le saisit à nouveau en réponse à mon invite précédente.
Une fois qu'ils ont tapé le code (ils le font toujours), je révèle que c'est moi qui ai envoyé les messages, et si j'avais été un mauvais acteur, j'aurais pu prendre le contrôle de leur compte personnel.

Arrivée d'une nouvelle autoroute

Un autre stratagème de test que j'utilise consiste à demander à une femme adulte d'appeler la victime et de lui dire ce qui suit : « C'est l'enquête et l'ingénierie de Bintner.
Je tiens à confirmer que nous avons votre permission d'être dans votre cour au 500 Lorelane Place, Key Largo, pour prendre des mesures d'arpentage demain matin !
La victime dit toujours quelque chose comme : « Quoi ? De quoi parles-tu ?

L'interlocuteur répond : « Nous avons été embauchés par le comté pour mener une enquête sur l'élargissement de la route dans votre région.
Ils vont utiliser les marges de recul du comté sur votre propriété pour élargir la route.
J'ai juste besoin de votre permission pour que mes gars soient dans votre cour demain. Cela ne devrait prendre que 15 minutes et n'aura pas d'impact sur votre propriété.
Nous devons confirmer que vous nous approuvez sur votre propriété et que les animaux dangereux ne sortiront pas pendant les heures de 11 h à 13 h ?

La victime répond toujours par une autre : « Quoi ? De quoi parles-tu ?
Mon interlocuteur est entraîné à dire : « Je m'excuse.
Le comté aurait dû vous envoyer une lettre au sujet du projet et vous informer de l'arpentage requis.
Je vous prie de m'excuser de ne pas avoir reçu l'information.
Voulez-vous que je vous envoie par e-mail des informations sur le projet en cours ?

Ils disent toujours oui et me donnent leur adresse courriel (que j'ai déjà).
Ensuite, je leur envoie un document piégé.
Dès qu'ils ouvrent le fichier, j'ai gagné le pari.
Mon faux scénario dépend de l'endroit où ils vivent.
Parfois, mon appel semble provenir de la société de gestion HOA (s'ils ont un HOA) ou de la division des inondations de la NOAA (s'ils vivent près de l'eau).

Faux frais de carte de crédit

Il s'agit d'une escroquerie courante dans le monde réel.
Quelqu'un vous appelle avec un numéro qui semble provenir du dos de votre carte de crédit.
Ils vous accueillent avec un bonjour professionnel comprenant votre nom complet. Ensuite, ils disent quelque chose de similaire : « M. Grimes, nous sommes de [insérer le nom du fournisseur de cartes de crédit ici].
Nous pensons avoir détecté quelqu'un qui utilise votre carte de crédit de manière frauduleuse.
Avez-vous acheté deux billets de Dallas, au Texas, pour le Nigeria ce matin ?

Quand vous dites « Non », ils continuent.
« Nous ne pensions pas que vous l'aviez fait.
Vous êtes un client précieux et nous nous excusons pour la gêne occasionnée.
Soyez assuré que vous ne serez pas responsable des transactions frauduleuses.
Nous vous enverrons une carte de crédit de remplacement dans la nuit.
Est-ce que [le nom de votre conjoint] a aussi besoin d'une carte de remplacement ?

La victime répond : « Oui. » Ils poursuivent : « Nous nous excusons à nouveau pour la gêne occasionnée.
Avant de continuer, nous devons confirmer votre adresse.
Vous habitez à [adresse postale] ?
Votre téléphone est [numéro de téléphone] ?
Votre adresse courriel est [votre adresse courriel] ?
Les quatre derniers chiffres de votre numéro de sécurité sociale sont [les quatre derniers chiffres de votre numéro de sécurité sociale] ?
Une fois que vous aurez confirmé ces informations, ils vous diront : « Merci d'avoir confirmé votre identité. »

Ils poursuivent : « Nous avons enregistré 55 000 $ de transactions au cours des deux derniers jours.
Nous devons confirmer les transactions que vous avez créées et que nous devons payer et déterminer celles qui sont frauduleuses et dont vous ne serez pas responsable.
Avant de continuer, quel est votre nom d'utilisateur ?
La victime répond avec son nom d'utilisateur.

Ensuite, l'appelant dit : « Nous allons vous envoyer un code à 6 chiffres pour confirmer que nous parlons avec le titulaire du compte valide.
S'il vous plaît, dites-nous ce code à 6 chiffres.

À l'insu de la victime, l'escroc vient de réinitialiser son mot de passe ou son paramètre d'authentification multifacteur sur son compte de carte de crédit et le fournisseur légitime envoie maintenant à la victime un code de confirmation pour compléter le compte demandé.
Le code à 6 chiffres provient du fournisseur de la carte de crédit de la victime, qu'elle voit et répète ensuite à la personne au téléphone.
Ça y est, l'arnaque est faite.
Aujourd'hui, ils sont volés.
L'escroc les gardera au téléphone pendant encore 10 minutes pendant qu'ils utilisent le compte de la victime pour effectuer des achats frauduleux.

Révéler votre mot de passe NT Hash

Les mots de passe des utilisateurs d'ordinateurs Windows sont toujours convertis en hachages de mots de passe NT pour le stockage et l'utilisation du système.
Beaucoup de gens ne se rendent pas compte que je peux vous envoyer un courriel et que si vous ouvrez ce message et/ou cliquez sur le lien à l'intérieur, je peux capturer à distance votre hachage NT, que je reviens ensuite à son mot de passe équivalent en texte clair (si votre mot de passe n'est pas assez fort).
Cela peut se faire de différentes manières.

J'ai écrit pour la première fois à ce sujet en 2019 et c'est toujours un problème aujourd'hui.
Il nécessite l'utilisation d'un bogue non corrigé, impliquant souvent Microsoft ou un logiciel tiers, mais ces types de bogues se produisent systématiquement une ou deux fois par an depuis des décennies.
Voici la dernière itération d'il y a quelques mois.

Le résultat final est que je peux vous envoyer un courriel et tout ce que vous avez fait a été d'ouvrir le courriel pour voir ce qu'il disait (ou vous devrez peut-être être amené à cliquer sur un lien).
Mais vous ne voyez rien.
Il ne vous est pas demandé d'ouvrir un fichier, d'exécuter du contenu ou quoi que ce soit d'autre.
Mais à l'insu de la victime, son navigateur est invité à envoyer l'authentification Windows intégrée pour se connecter à un site Web hébergeant le contenu lié impliqué, et à partir de là, l'attaquant peut obtenir le hachage de votre mot de passe NT, et si votre mot de passe n'est pas assez fort (12 caractères ou plus), obtenir probablement votre mot de passe en texte clair.
Cette astuce fonctionne généralement avec n'importe quel système d'exploitation ou navigateur qui prend en charge l'authentification Windows intégrée (qui est courante sur iOS, Google Chrome, Linux, etc.).

Ami passe-temps

Les pirates se lient souvent d'amitié avec les gens dans leurs forums de loisirs.
Dites que vous aimez voler, les chiens ou sculpter.
De nombreuses personnes qui ont des passe-temps rejoignent des sites Web et des blogs liés aux passe-temps.
Les attaquants se lient souvent d'amitié avec des victimes potentielles, leur disant à quel point ils admirent leur intérêt pour ce passe-temps, et deviennent des « amis » en ligne. Le pirate passera des mois à cultiver la relation, pour gagner la confiance de la victime. Souvent, le personnage du pirate sera une version superbe du sexe opposé, qui comprend des déclarations séduisantes.
Puis, à une date ultérieure, envoyez un e-mail avec un lien contenant du contenu malveillant.
Cela arrive tout le temps.
Trop de victimes accordent trop de confiance à des personnes qu'elles n'ont jamais rencontrées.
La CISA met en garde contre ce type d'attaque.

Fausses offres d'emploi

J'ai déjà abordé ce sujet à de nombreuses reprises, y compris ici, mais de nombreuses victimes sont devenues des victimes à cause de « GRANDES » fausses offres d'emploi. Soit ils sont approchés après avoir placé un CV sur un site d'emploi légitime, soit la fausse entreprise les approche.
Ils prétendent avoir le « job parfait ».
Il offre tous les avantages, vous paie trop, des vacances illimitées et vous pouvez choisir si vous travaillez au

bureau ou entièrement à distance.
Comme tu veux.

Ils vous « interviewteront », vous laisseront parler et, à partir de cette conversation, mettront à jour l'offre d'emploi pour avoir d'autres choses qui vous intéressent, comme une voiture de luxe, une garde d'enfants gratuite ou une allocation mensuelle de garde d'enfants ou de tuteur parental.
Ils contactent généralement LinkedIn ou un autre site où ils ont créé un faux compte qui semble appartenir à une autre entreprise notable dans votre domaine d'intérêt.
Ils utilisent de vrais noms et des photos de vraies personnes qui appartiennent à la vraie entreprise.

De nombreux employés qui se sont vu offrir et accepter ces faux emplois de fausses entreprises ont été personnellement victimes ou ont fini par installer un logiciel « nécessaire » qui s'avère être un cheval de Troie qui attaque leur employeur actuel.
C'est très, très courant.

Remplacement de faux matériel

Une autre escroquerie difficile à repérer est lorsque les victimes utilisant du matériel particulier, généralement des portefeuilles de crypto-monnaies matériels, reçoivent de nouveaux faux appareils de crypto-monnaies « mis à jour ».
Ces appareils arrivent dans des boîtes d'expédition conçues pour ressembler aux vraies boîtes.
L'appareil est un véritable appareil de remplacement, sauf qu'il a été modifié de manière malveillante d'une manière ou d'une autre.
Le remplacement contient une lettre avec un papier à en-tête d'apparence officielle, du PDG, informant la victime d'un problème qui ne peut être résolu qu'en remplaçant son matériel actuel par le nouveau matériel.

Si la victime est amenée à utiliser le remplacement, le pirate prend le contrôle de l'utilisation de la victime et vole quelque chose (par exemple, des cryptomonnaies, de l'argent, des informations, etc.).
Habituellement, ces escroqueries matérielles impliquent des personnes qui achètent et stockent des crypto-monnaies, mais j'ai également vu de fausses clés USB et de faux logiciels envoyés.
Une victime que je connais a reçu une version mise à jour de Microsoft Office sur une clé USB (malveillante), le tout marqué pour donner l'impression qu'il provenait vraiment de Microsoft.

Voici un exemple d'attaque réelle.
Dans ce cas, les escrocs ont envoyé les portefeuilles matériels cryptographiques malveillants de remplacement à des personnes qui utilisaient réellement le produit et qui étaient au courant d'une compromission de ce fournisseur quelques mois auparavant. Ainsi, les victimes ont été informées par l'entreprise légitime de la compromission et de l'utilisation possible de leurs informations.
Le faux matériel était accompagné d'une lettre prétendant provenir du PDG faisant référence à la même attaque précédente que pour la raison pour laquelle le remplacement était nécessaire.
Donc, ça avait l'air très légitime.
Je suis étonné que certaines des victimes potentielles aient réalisé qu'il s'agissait d'une arnaque.
Je pense que j'aurais facilement pu craquer pour celui-ci.

Tous ces exemples ci-dessus démontrent que toutes les escroqueries ne sont pas faciles à repérer.
De nombreuses escroqueries sont très sophistiquées et peuvent se dérouler sur plusieurs mois.
Et si vous me dites que vous n'auriez pas été pris dans l'une de ces escroqueries, c'est génial.
Mais je pense que la plupart des gens seraient tombés dans au moins un de ces exemples d'escroqueries et je sais que n'importe qui peut se faire arnaquer.
Tout ce qu'il faut, c'est le bon scénario d'escroquerie au bon moment et dans les bonnes circonstances.

Si vous croyez que vous n'êtes pas escroqué, vous vous préparez peut-être à une future tarte humble.
Je connais des dizaines de personnes qui pensaient qu'elles ne pourraient jamais se faire arnaquer... jamais...
Ils ont appris différemment.

Il est préférable d'avoir l'état d'esprit que vous pourriez être susceptible d'être victime d'une future escroquerie... que personne n'est parfait.
Et restez vigilants, éduqués et sceptiques à cette fin.
Si vous pensez que vous pourriez être victime d'une arnaque, vous serez probablement mieux préparé que si vous pensez que vous ne pouvez pas l'être.
C'est aussi simple que cela.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240227
"C'est ensemble qu'on avance"