Alerte ! Un phishing élaboré vise les utilisateurs de Gmail

Alerte ! Un phishing élaboré vise les utilisateurs de Gmail

Une attaque au phishing particulièrement élaborée sévit depuis quelque temps contre les utilisateurs de comptes Gmail, ce qui amène amène plusieurs spécialistes à inviter le public à la prudence.

En matière de phishing – les escroqueries consistant à se faire passer pour un tiers de confiance afin de dérober les informations bancaires ou personnelles de sa cible –, la dernière arnaque en cours contre les utilisateurs de Gmail, particulièrement répandue en 2016, s'avère très efficace, au point de duper des utilisateurs chevronnés.
Comme la majorité des tentatives, cette arnaque commence par l'envoi d'un email a priori banal, provenant généralement d'un contact de notre carnet d'adresse qui a déjà été victime de ce phishing. La manœuvre frauduleuse mise sur sa prétendue pièce jointe.
En cliquant sur ce fichier a priori inoffensif – qui est en réalité une capture d'écran avec un lien et pas une véritable pièce jointe – pour en avoir un aperçu, l'utilisateur se retrouve sur une nouvelle page qui l'invite à se reconnecter à son compte Gmail. Apparence, URL (un « data:text » suivi de l'adresse « https://accounts.google.com » rassurante mais qui ouvre en fait un script)… tout semble conforme à un véritable formulaire Google. Mais en tapant son adresse et son mot de passe, la cible vient de succomber au piège.
Une victime décrit ainsi son expérience malheureuse : « Les attaquants se connectent immédiatement à votre compte dès qu'ils en ont le mot de passe, et ils utilisent l'une de vos pièces jointes, combinée à un véritable titre de mail, pour l'envoyer à vos contacts. Ils ont par exemple accédé au compte d'un élève et en ont extrait un calendrier d'entraînement sportif pour en faire une capture d'écran et l'ont ensuite associée à un titre de mail relativement en rapport pour l'envoyer aux autres membres de l'équipe. »

GOOGLE RECOMMANDE LA VALIDATION À DEUX ÉTAPES
Pour éviter de devenir la dernière victime de ce phishing élaboré, la vigilance reste de mise, notamment en vérifiant systématiquement la présence du cadenas sécurisé dans la barre d'adresse. Mais surtout en activant la validation en deux étapes : à chaque connexion à Google, en plus de votre mot de passe, vous devez saisir un code qui vous est communiqué sur votre téléphone.
Aaron Stein, de Google Communications, recommande d'ailleurs cette méthode dans un communiqué qui se veut rassurant : « Nous sommes au courant de ce problème et nous continuons d'améliorer notre défense. Nous contribuons à la protection des utilisateurs contre le phishing de multiples manières, notamment grâce à la détection de [mail frauduleux] par machine learning . »
Gmail permet aussi à ses utilisateurs, en quelques clics, de signaler qu'un contenu reçu dans sa boîte mail relève du phishing.
Fin novembre, des professeurs et des journalistes avaient reçu une alerte de Google contre des tentatives d'intrusion.

Vous souhaitez organiser une campagne de sensibilisation pour vos salariés, agents ou membres , n'hésitez pas à nous solliciter.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Prudence : un phishing élaboré vise les utilisateurs de Gmail – Tech – Numerama