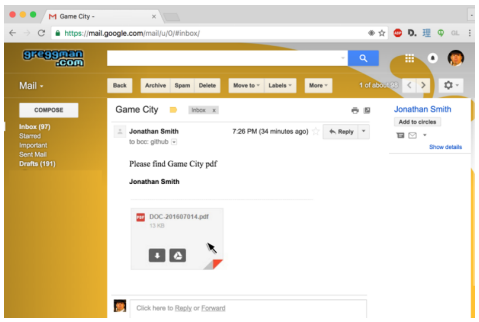
Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

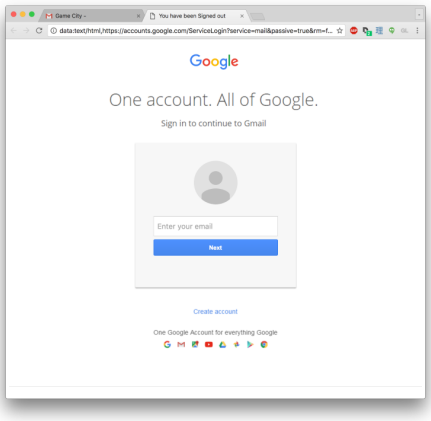
Une arnaque au phishing particulièrement élaborée vise les utilisateurs de la messagerie de Google.



Crédit : Greggman

Ce mail semble contenir une pièce jointe

Une arnaque au phishing au mode opératoire à la sophistication inédite sévit depuis plusieurs semaines sur la messagerie Gmail. L'attaque, qui vise à dérober des informations personnelles afin de les réutiliser à l'insu de l'utilisateur, prend la forme d'un mail envoyé par un contact contaminé. **Il continent une pièce-jointe et un message lapidaire du type « voici le pdf demandé ».** Un clic sur la pièce-jointe renvoie l'utilisateur vers une page à l'apparence de Google Drive et lui demande de s'identifier pour la visualiser. Une fois l'opération effectuée, l'assaillant prend possession du compte de la victime, peut à son tour envoyer le mail de hameçonnage à tous ses contacts et se livrer à des usurpations d'identité ou à des escroqueries.



Crédit : Greggman

Cette page ressemble à la page d'accueil Gmail

Comme l'explique un blogueur américain qui s'est fait piéger par l'arnaque, la pièce-jointe est en fait une image intégrée dans le corps du mail associée à un lien renvoyant automatiquement vers une page web. L'url contient « https://accounts.google.com » et laisse à penser qu'il s'agit du véritable site de Google. Mais elle débute par data « :text/html » et contient un script aspirant l'identifiant et le mot de passe de la victime lorsqu'ils sont renseignés dans le formulaire.

Dans un communiqué, Google dit avoir pris connaissance du problème. « Nous continuons de renforcer nos moyens de défense contre cela. Nous faisons de notre mieux pour protéger nos utilisateurs de différentes manières, en détectant les messages de phishing grâce au deep learning, en adressant des alertes de sécurité lorsque plusieurs liens suspicieux arrivent dans les mails, en repérant des tentatives de connexion douteuses, etc. Les utilisateurs peuvent aussi activer la validation en deux étapes pour ajouter une protection supplémentaire à leur compte », écrit Google dans un communiqué.

Comment fonctionne le phishing

Contraction des mots « fishing » (pêche en français) et « phreaking » (terme désignant le piratage des lignes électroniques) – le phishing est **une technique dite de « hameçonnage » basée sur de faux mails** qui visent à collecter les données bancaires ou les mots de passe des clients. À partir de ces documents, les pirates peuvent ensuite se livrer à des usurpations d'identité et à des escroqueries.

Ces faux courriels se présentent souvent comme des courriers envoyés par une source sûre, comme le Trésor public ou les banques. Trompées par l'expéditeur supposé, les victimes fournissent souvent elles-mêmes leurs propres données personnelles. Une autre possibilité consiste à envoyer des SMS ou des mails malveillants en masse qui contiennent un lien permettant d'installer, sans le savoir, un logiciel pirate qui pourra récupérer les données personnelles des personnes ainsi trompées.

Surveiller les mails et leur orthographe

Il s'agit donc de surveiller les mails et leur contenu. Les courriels émanant d'une structure officielle (la banque, EDF, ou la caisse d'allocations familiales par exemple) ne demandent jamais à leurs clients de saisir leurs informations personnelles directement dans un mail mais depuis un site Internet crypté. Dans ce cas, **un petit cadenas apparaît systématiquement à gauche de l'URL** du site pour garantir la confidentialité des informations.

Par ailleurs, en cas d'information importante, une banque ou un opérateur contactent généralement leurs clients par courrier ou par téléphone. Les mails utilisés dans le cadre des tentatives d'escroqueries font souvent état de **situations alarmistes** et comportent des **fautes d'orthographes** ou de syntaxe laissant penser que le message a été rédigé par un logiciel de traduction automatique.

Vérifier les adresses électroniques et les URL des sites internet

Dans certains cas de phishing, les victimes sont redirigées vers un faux-site, qui ressemble comme deux gouttes d'eau au site officiel. Il faut alors vérifier que l'URL est bien la même que celle du site copié. En général, elle est beaucoup plus longue et compliquée et on peut remarquer que, dans le corps du mail, le texte affiché sous forme de lien ne correspond pas du tout au lien réel, dont l'adresse s'affiche lorsqu'on positionne le curseur dessus. Dans le cas de l'arnaque aux faux mails de la Cpam, on peut s'apercevoir que l'adresse de réclamation ne correspond pas à celle d'un organisme officiel puisqu'elle se termine en « gmail.com ».

Original de l'article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s'en protéger

---

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 DIRTEF 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 : Une nouvelle arnaque au phishing sur Gmail, comment s’en protéger