OUCH ! Décembre 2024

OUCH!

SANS SECURITY AWARENESS

La lettre d'information mensuelle de sensibilisation à la sécurité

Comprendre les mystères : comment les cybercriminels volent vos mots de passe

Un cauchemar numérique : l'exposition non désirée de Lisa

Lisa, une graphiste douée pour la créativité, vit une grande partie de sa vie en ligne. Elle s'occupe de ses comptes bancaires, elle fait ses achats en ligne, et elle communique en ligne sur diverses applications et sites. Un jour, elle remarque des prélèvements bizarres sur son compte bancaire, des achats qu'elle n'avait pas effectués, sur des magasins sur lesquels elle ne s'était pas rendue. Ses comptes de réseaux sociaux ont commencé à publier des messages publicitaires étranges, et ses amis ont signalé qu'ils recevaient des emails inhabituels de sa part.

La panique s'est emparée de Lisa quand elle a réalisé qu'elle avait perdu son identité digitale. Ses photos personnelles avaient fuité, et ses conversations privées avaient été postées publiquement. Ses clients ont commencé à remettre en question sa fiabilité, et sa réputation a pris un coup. Après avoir consulté des cybercriminels experts, Lisa a découvert que ses mots de passe avaient été compromis. Des cybercriminels avaient accédé à ses comptes les plus confidentiels, démantelant son univers numérique pièce par pièce. Mais la question se pose : comment cela s'est-il produit ?

Les tactiques sournoises des cybercriminels : cinq méthodes courantes

Les acteurs de la cybermenace emploient diverses techniques pour récupérer les mots de passe. Voici cinq façons courantes dont ils pourraient se servir pour obtenir les vôtres comme ils ont obtenu ceux de Lisa :

1. **Les attaques d'ingénierie sociale**

   L'ingénierie sociale consiste pour les attaquants à se faire passer pour quelqu'un que vous connaissez ou en qui vous avez confiance, et à vous inciter à faire quelque chose que vous ne devriez pas faire. Ils envoient des emails ou des messages qui semblent légitimes, créant souvent un fort sentiment d'urgence, de peur ou de curiosité.

   Comment cela s'est produit : Lisa a reçu un email qui semblait provenir de sa banque, avec les logos officiels et une signature crédible. L'email affirmait qu'il y avait des activités suspectes sur son compte et qu'il fallait qu'elle clique rapidement sur ce lien pour confirmer son identité. Le lien menait vers un site frauduleux qui avait enregistré ses mots de passe lorsqu'elle les avait rentrés.

2. **Logiciel malveillant**

   Les maliciels sont des logiciels malveillants conçus pour infecter les ordinateurs. Une fois infectés, les cybercriminels peuvent en faire ce qu'ils veulent. Les enregistreurs de frappe (aussi appelés *voleurs d'informations*) sont un type de maliciels qui enregistre chaque frappe effectuée sur un appareil, y compris vos identifiants, vos mots de passe et vos données sensibles.

   Comment cela s'est-il produit : Lisa a téléchargé ce qu'elle pensait être un lot de polices de caractères légitimes pour ses travaux de designer. Un enregistreur de frappe s'y cachait et s'est installé sur son ordinateur. Au fil du temps, il a enregistré ses données de connexion à divers comptes et les a renvoyées à l'auteur de l'attaque.

3. **Attaques par force brute**

   Dans les attaques par force brute, les cybercriminels utilisent des outils automatisés pour essayer de nombreuses combinaisons de mots de passe jusqu'à ce qu'ils trouvent la bonne. Les mots de passe faibles sont particulièrement vulnérables avec cette méthode.

   Comment cela s'est-il produit : Lisa utilisait des mots de passe simples comme "lisa2020" pour beaucoup de ses comptes. Les attaquants ont utilisé des logiciels qui essaient systématique des mots de passe communs ce qui leur a permis de facilement obtenir l'accès à ses comptes.

4. **Les violations de données**

   Quand un site ou un service se fait pirater, il peut affecter les mots de passe de toutes les personnes qui sont enregistrées sur le serveur. Si quelqu'un utilise le même mot de passe pour plusieurs comptes, quand ce mot de passe est compromis pour un compte, alors ce mot de passe peut être utilisé pour accéder aux autres comptes de la victime.

   Comment cela s'est-il produit : Un réseau social populaire que Lisa utilisait souvent s'est également fait hacker. Puisqu'elle utilisait le même mot de passe partout, les attaquants ont accédé à ses autres comptes en utilisant ses informations d'identification qui avaient fuitées.

5. **Les titres de compétences achetés**

   Les cyber-criminels peuvent tout simplement acheter vos mots de passe sur internet, généralement sur le Dark Web. Certains cyber-criminels sont spécialisés dans le vol de mots de passe, utilisant l'une des méthodes que nous avons évoquées jusqu'à présent. Puis, ils stockent et vendent les mots de passe volés à d'autres cybercriminels.

   Comment cela s'est-il produit : Un cybercriminel a décidé qu'il voulait se faire le plus d'argent possible pendant le week-end, alors il s'est rendu sur le Dark Web et a acheté plus de 100 000 comptes compromis avec tous leurs mots de passe. L'un des comptes de Lisa était sur cette liste.

Trois étapes clés que vous pouvez suivre

Heureusement, en suivant ces trois étapes, vous pouvez protéger vos comptes et votre vie digitale.

1. Utilisez un mot de passe long et unique pour chacun de vos comptes. Nous vous conseillons d'utiliser des phrases de passe ; des mots de passe longs, constitués de plusieurs mots.
2. Utilisez un gestionnaire de mots de passe pour stocker de manière sécurisée tous vos mots de passe.
3. Activez l'authentification multifactorielle (2FA) dès que possible pour vos comptes en ligne les plus importants.

Rédacteur invité

Lekshmi Nair est un responsable de la cybersécurité avec 22 ans d'expérience dans le conseil en sécurité de l'information et la stratégie de cybersécurité. Elle est actuellement directrice principale du service de conseil en sécurité des applications chez BlackDuck Software. Elle est la fondatrice et la présidente de WiCyS India.

Ressources

Les voix fantômes : se défendre contre les attaques de clonage de voix : https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Attaques par SMS : une saga de smishing :https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
Top trois des manières dont les cyberattaquants vous ciblent :https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Le pouvoir des phrases de passe :https://www.sans.org/newsletters/ouch/power-passphrase/
Le pouvoir des gestionnaires de mots de passe :https://www.sans.org/newsletters/ouch/power-password-managers/

Traduit pour la communauté par : Juliette Busson