6 façons dont votre adresse courriel peut être exploitée par des escrocs

Que peuvent faire les escrocs avec votre compte de messagerie?
Renseignez-vous sur les informations que quelqu'un peut obtenir simplement à partir de votre adresse courriel.
Simon Batt :

Cela peut sembler étrange au début, mais un compte de messagerie est une mine d'or pour les escrocs.
Un pirate informatique peut faire plus que mettre la main sur votre recette convoitée de casserole de poulet; Ils peuvent causer des dommages à votre identité et à vos finances.

Alors, pourquoi les escrocs veulent-ils votre adresse courriel? Que peut faire un escroc avec votre adresse e-mail et votre numéro de téléphone?
Et que pouvez-vous faire s'ils déchiffrent votre mot de passe?

Que peut faire un escroc avec mon adresse courriel ?

Les escrocs accèdent généralement à une adresse courriel via des attaques par force brute ou par une fuite de base de données.
Une fois qu'ils ont obtenu l'accès, ils peuvent effectuer plusieurs actions avec votre compte de messagerie.

1. Ils peuvent usurper votre identité

Il est de notoriété publique que vous ne devriez jamais faire confiance à un courriel qui n'est pas de quelqu'un en qui vous avez confiance.
En tant que tels, ces courriels affirmant que vous avez gagné 4 millions de dollars à une loterie à laquelle vous n'avez jamais participé ne trompent plus les gens aussi facilement.

Cependant, les escrocs trouvent un moyen de contourner ce problème.
Bien que le conseil nous rende plus critiques à l'égard des courriels envoyés par un étranger, il nous rend également plus confiants à l'égard des courriels envoyés par des personnes que nous connaissons et aimons.

Les escrocs utilisent cette faiblesse en piratant des comptes de messagerie, puis en utilisant ce compte pour contacter les amis et la famille de la victime.
Si l'escroc est doué pour usurper l'identité de personnes, il peut tromper les contacts de la victime en leur faisant croire qu'ils parlent à la victime.

À partir de ce moment, l'escroc peut demander à la victime de faire ce qu'elle veut.
Ils peuvent prétendre qu'ils ont des problèmes financiers, demandant à leurs amis de transférer de l'argent au pirate.
Ils pourraient envoyer un lien vers un programme malveillant et prétendre qu'il s'agit d'une vidéo de l'ami faisant quelque chose d'embarrassant.

En tant que tel, vous devez faire preuve de prudence, même si c'est soi-disant votre bon ami qui vous envoie un courriel.
En cas de doute, essayez de les contacter par téléphone ou par une autre méthode comme les médias sociaux pour voir si leur demande est légitime.

2. Ils peuvent déchiffrer les mots de passe de vos autres comptes

Crédit d'image: mishoo / DepositPhotos

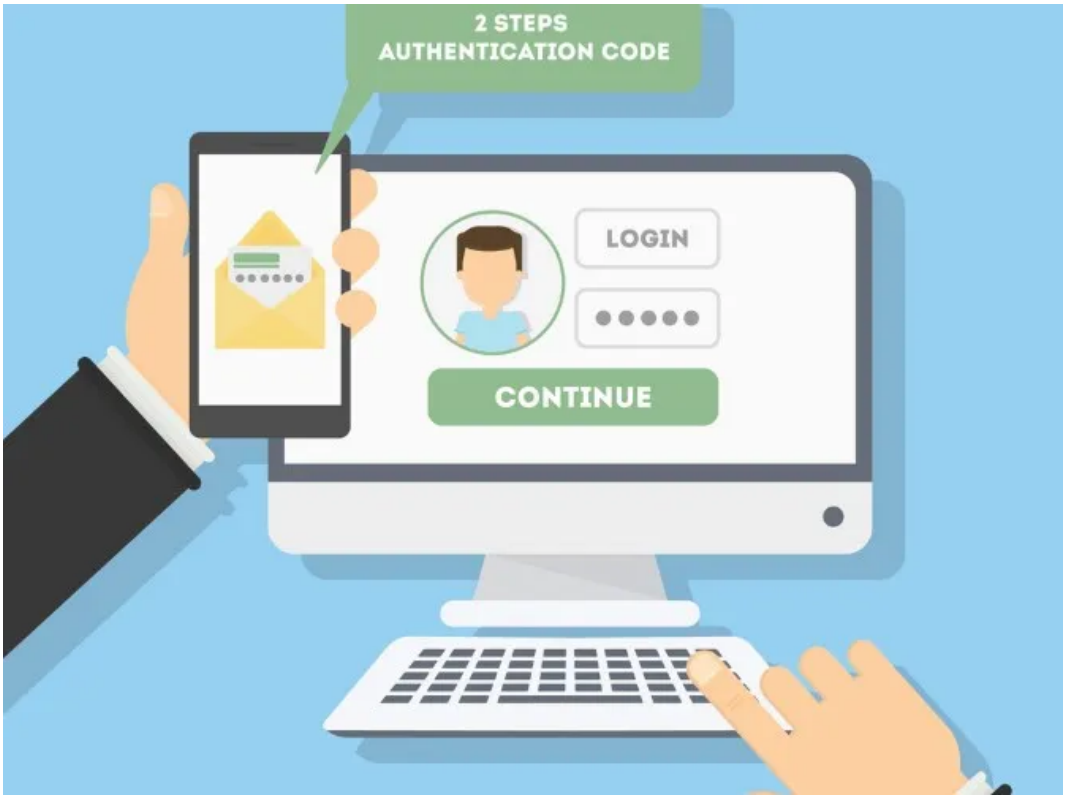
Si vous vous inscrivez à un site Web avec des pratiques de sécurité médiocres, ils vous enverront un courriel confirmant votre nom d'utilisateur et votre mot de passe lorsque vous vous y inscrivez.
Tout cela sera bien en vue pour quiconque accède à votre courrier électronique.

La plupart des sites Web ne divulguent pas ou ne peuvent pas divulguer le mot de passe dans le courriel d'inscription pour cette raison (bien que certains sites qui stockent les mots de passe en texte brut le fassent).
Ces courriels sont toutefois susceptibles de mentionner votre nom d'utilisateur dans l'e-mail d'inscription, qu'un pirate peut utiliser pour accéder à ce compte.

Par exemple, si vous utilisez le même mot de passe sur votre compte de messagerie pour tout le reste, le pirate a déjà le mot de passe dont il a besoin pour accéder à vos autres comptes.

Si vous ne le faites pas, le pirate peut toujours demander une réinitialisation du mot de passe de chaque site.
Le site Web envoie un courriel de réinitialisation à votre compte, que le pirate peut ensuite utiliser pour le modifier à sa guise.

3. Ils peuvent l'utiliser pour déchiffrer l'authentification à deux facteurs basée sur le courrier électronique (2FA)



Crédit d'image: inspiring.vector.gmail.com/ DepositPhotos

Parfois, un pirate aura le mot de passe du compte de quelqu'un d'autre, mais sera arrêté par un système d'authentification à deux facteurs (2FA) basé sur le courrier électronique. Les pirates peuvent passer à travers les systèmes 2FA en mettant la main sur l'endroit où les codes d'authentification sont affichés.

Si un pirate informatique accède à votre compte de messagerie, il peut passer à travers toutes les mesures 2FA basées sur le courrier électronique que vous avez configurées.

Certains sites Web vous envoient un courriel lorsqu'ils détectent un modèle de connexion inhabituel.
Ce courriel vous demandera si la tentative de connexion était authentique et vous donnera généralement un bouton pour confirmer la tentative de connexion.
Les pirates peuvent contourner cette mesure de sécurité s'ils ont votre adresse courriel en autorisant leur tentative de connexion lorsque le courriel arrive.

4. Ils peuvent collecter des informations sensibles

Si le pirate informatique a accès à un compte de messagerie professionnel, cela pourrait être dévastateur pour l'entreprise.
Tous les détails financiers sensibles, les informations de connexion de l'entreprise ou les mots de passe des verrous physiques sont tous visibles par le pirate.
Ces informations leur permettent d'effectuer des vols numériques ou physiques sur l'entreprise.

Les comptes personnels peuvent également contenir des informations sensibles dans leur boîte de réception.
Toute correspondance bancaire peut révéler des détails qu'un escroc peut utiliser pour pénétrer dans votre compte bancaire.

5. Ils peuvent voler votre identité

Si votre compte ne contient pas d'informations professionnelles sensibles, un pirate informatique peut se contenter de voler votre identité.

Un pirate peut récolter beaucoup d'informations à partir de vos courriels.
Les factures ont votre nom et votre adresse bien en vue, et l'escroc peut recueillir toutes les photos que vous avez envoyées.
Si le pirate obtient suffisamment d'informations, il peut utiliser les données pour voler votre identité et demander des services sous votre nom.

Gardez toutes les sources d'informations personnelles que vous avez sur Internet à l'abri des regards indiscrets.
Il vaut la peine d'en apprendre davantage sur les informations utilisées pour voler votre identité afin que vous sachiez ce que vous pouvez partager et ce qu'il faut cacher.

6. Ils peuvent apprendre quand vous êtes dehors

Si un pirate trouve des billets de transport ou des détails de réservation pour un hôtel dans votre courriel, il saura que vous êtes hors de la maison pendant ces jours.
Combinez cela avec votre adresse récoltée à partir d'une facture, et un escroc sait quand et où cambrioler votre maison.

Il est essentiel de garder vos plans de voyage et vos lieux secrets, sinon vous courez le risque d'attirer des cambrioleurs dans votre propriété.
Même les billets pour un évènement peuvent indiquer les heures de votre absence.

Il existe de nombreuses façons pour les cambrioleurs de savoir quand vous êtes en vacances, alors gardez les choses silencieuses pendant votre absence.
Ne vous inquiétez pas; vous pouvez toujours télécharger ces instantanés de plage et selfies lorsque vous rentrez chez vous!

Que faire si un escroc a votre adresse courriel

Si un escroc possède votre compte de messagerie, vous devez essayer de changer le mot de passe immédiatement.
Si le pirate n'a pas envisagé de le changer, vous aurez le temps de définir un mot de passe différent et plus fort et de forcer le pirate à partir.

Malheureusement, les pirates changeront probablement le mot de passe pour vous verrouiller.
Dans ce cas, vous devrez passer par la page d'assistance de votre fournisseur de messagerie pour le déverrouiller à nouveau.
Ils demandent généralement des informations de connexion passées et peuvent exiger une preuve d'identité pour rendre votre compte.

Une fois que vous avez changé votre mot de passe pour quelque chose de plus fort, essayez d'ajouter une mesure de sécurité 2FA à votre compte.
Même si un pirate récupère votre mot de passe, il doit également avoir le jeton 2FA sous la main, ce qui est plus facile à dire qu'à faire.

Si cela vous intéresse, assurez-vous d'apprendre à sécuriser vos comptes Gmail et Outlook avec 2FA.

Se protéger des escrocs

Vous ne craignez peut-être pas qu'un pirate informatique accède à votre compte de messagerie, mais pensez à toutes les informations qu'un étranger peut obtenir en lisant votre courrier.
Les comptes de messagerie compromis sont des mines d'or potentielles pour les escrocs, il vaut donc la peine de garder le vôtre en sécurité avec un mot de passe robuste.

Maintenant que vous savez comment protéger votre compte, il est temps d'apprendre à repérer un faux courriel.
Après tout, si vous êtes conscient des techniques de l'escroc pour vous faire croire qu'il s'agit de quelqu'un d'autre, cela réduit considérablement le risque que vous tombiez dans son piège.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230803
"C'est ensemble qu'on avance"