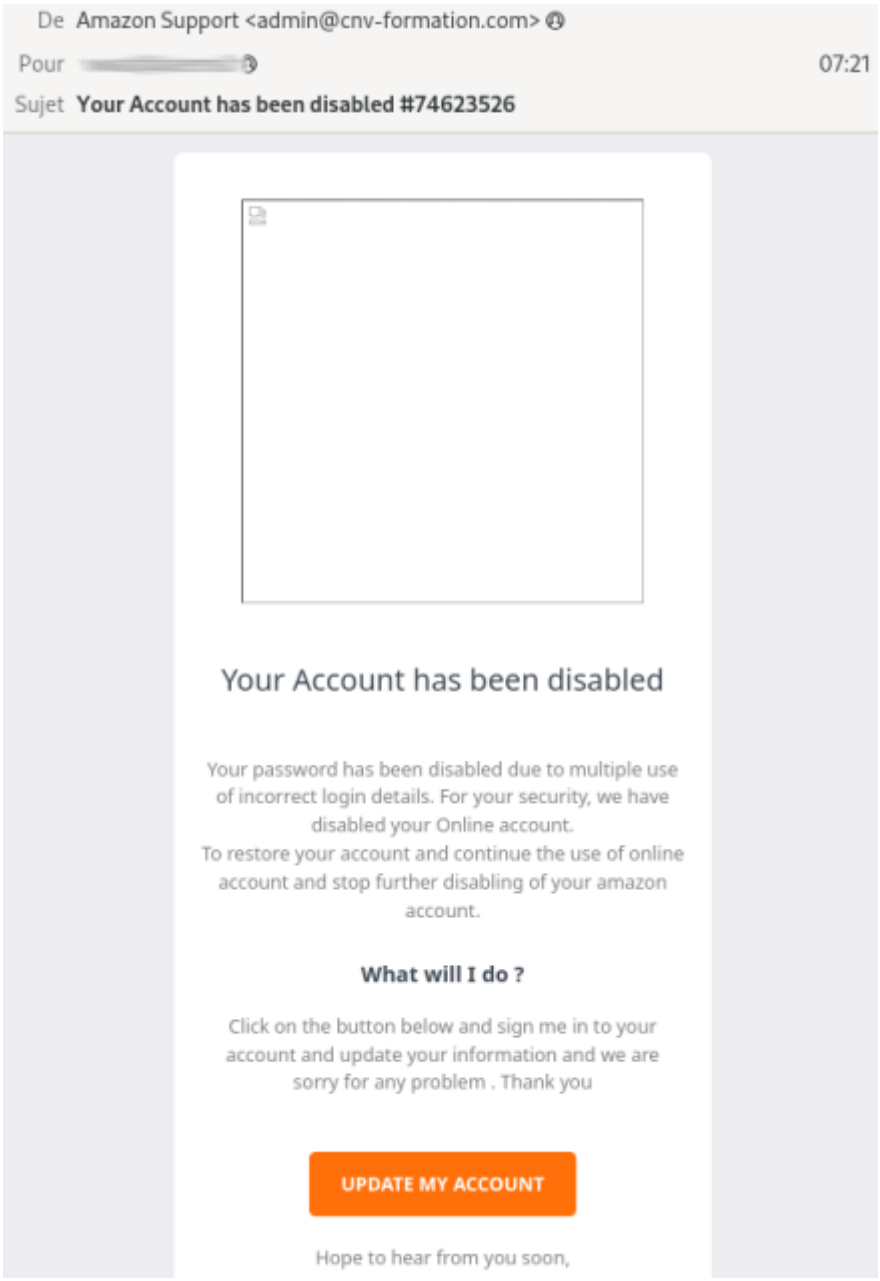
Votre compte Amazon a été désactivé

J'ai identifié un e-mail frauduleux Amazon.




```
Your Account has been disabled Your password has been disabled due to
multiple use of incorrect login details. For your security, we have disabled
your Online account. To restore your account and continue the use of online
account and stop further disabling of your amazon account. What will I do ?
Click on the button below and sign me in to your account and update your
information and we are sorry for any problem . Thank you UPDATE MY ACCOUNT
```

```
Hope to hear from you soon, Amazon Service Team . © 2023 Amazon. All rights reserved.
```

En français :

```
Votre compte a été désactivé. Votre mot de passe a été désactivé en raison de plusieurs tentatives de connexion infructueuses. Pour des raisons de sécurité, nous avons désactivé votre compte en ligne. Pour rétablir votre compte et continuer à utiliser votre compte en ligne, ainsi que pour éviter toute désactivation ultérieure de votre compte Amazon. Que dois-je faire ? Cliquez sur le bouton ci-dessous, connectez-vous à votre compte et mettez à jour vos informations. Nous nous excusons pour tout désagrément. Merci. METTRE À JOUR MON COMPTE Nous espérons avoir de vos nouvelles bientôt. L'équipe du service client Amazon. © 2023 Amazon. Tous droits réservés.
```

Analyse du message

L'expéditeur

Dans cet exemple, l'adresse e-mail de l'expéditeur est `admin@cnv-formation.com`. Bien que cela puisse sembler légitime à première vue, il est important de noter que l'expéditeur prétend être Amazon Support, mais l'adresse e-mail ne correspond pas à un domaine associé à Amazon. Méfiez-vous des différences entre l'adresse e-mail de l'expéditeur et le nom de l'entreprise prétendument représentée.

Le lien présent dans le message

Dans cet e-mail, un lien est fourni pour prétendument identifier l'adresse e-mail de réception : http://account.login.notification.sqzgjfptizldxbqvaueh.hivegroup.biz/5kDWjV6InU?q=4979325635&id=503&e=adresse@mail.fr

Il est crucial de maintenir une vigilance constante face à de telles tentatives de phishing. Il est impératif de ne jamais cliquer sur des liens suspects ou fournis dans des e-mails non sollicités. Les cybercriminels recourent fréquemment à des techniques d'ingénierie sociale pour inciter les utilisateurs à divulguer leurs informations personnelles ou à infecter leurs appareils avec des logiciels malveillants.

Dans notre cas, il est important de noter qu'en cliquant sur le lien fourni, nous sommes redirigé vers une page blanche. Cependant, il est essentiel de comprendre que cela ne signifie pas nécessairement qu'aucune information n'a été transmise lors de cette redirection. Les attaquants peuvent utiliser diverses techniques pour masquer leur activité, y compris la redirection vers des pages vides.

De plus, on peut noter que le lien contenu dans le message redirige vers le domaine `hivegroup.biz`, qui ne semble pas être lié à Amazon ou à `cnv-formation.com`. Il convient également de souligner que le site `cnv-formation.com` affiche actuellement une page de non disponibilité, ce qui soulève davantage de doutes quant à la légitimité de l'e-mail reçu. Dans de tels cas, il est préférable de faire preuve de prudence et de contacter directement l'entreprise présumée par des moyens de communication officiels pour vérifier l'authenticité de la demande ou de l'information reçue.

En somme, il est primordial de rester vigilant face aux tentatives de phishing et de toujours vérifier attentivement les détails des e-mails suspects, tels que l'adresse e-mail de l'expéditeur, les liens inclus et la cohérence avec les informations connues sur l'entreprise prétendument représentée.

Décryptage technique

Examinons les autres informations de l'en-tête :

```
Message-ID: <0f27e14af9f7646f4a3079d272b69dc768db26@cnv-formation.com>
```

L'en-tête indique que le message provient du domaine “cnv-formation.com”. Encore une fois, cela ne correspond pas au domaine d'Amazon. Si vous recevez un e-mail prétendant provenir d'une entreprise spécifique, vérifiez que le domaine de l'expéditeur correspond à celui utilisé par cette entreprise.

```
Received: from 36.91.14.228 (unknown [10.5.10.1])
    by mail.bulukumbakab.go.id (Postfix) with SMTP id A82893E9F0
```

Dans cet exemple, le message a été reçu à partir d'une adresse IP inconnue, “36.91.14.226”, qui n'est pas associée à Amazon ou à un serveur de confiance. La localisation du serveur est souvent un indicateur important pour détecter les tentatives de phishing.

Examinons les informations DNS associées à `cnv-formation.com` :

```
❯ dig cnv-formation.com TXT

...
;; QUESTION SECTION:
;cnv-formation.com.     IN    TXT

;; ANSWER SECTION:
cnv-formation.com.  600    IN    TXT    "v=spf1 +all"
cnv-formation.com.  600    IN    TXT    "1|www.cnv-formation.com"
```

Les enregistrements DNS de type TXT indiquent des informations de configuration SPF (Sender Policy Framework) pour le domaine `cnv-formation.com`. SPF est un mécanisme utilisé pour spécifier les serveurs de messagerie autorisés à envoyer des courriers électroniques au nom d'un domaine spécifique.

Dans le cas de `cnv-formation.com`, l'enregistrement SPF indique `v=spf1 +all`, ce qui signifie que toutes les adresses IP sont autorisées à envoyer des courriers électroniques en utilisant ce domaine. Cela indique une configuration SPF très permissive, car le “+” après “spf1” signifie “tous les serveurs sont autorisés”. Cela facilite l'usurpation d'identité ou le spam en utilisant ce domaine.

Il est recommandé d'examiner d'autres facteurs tels que la présence de DKIM (DomainKeys Identified Mail) et de DMARC (Domain-based Message Authentication, Reporting, and Conformance), ainsi que de prendre en compte d'autres techniques de protection contre le courrier indésirable, comme les filtres anti-spam.

Conseils d'usage

01 - Conseils d'usage

Évitez les liens suspects dans les e-mails, accédez directement aux sites officiels

Il est préférable de ne pas se précipiter et de ne pas cliquer sur les liens proposés dans les mails. Au lieu de cela, il est recommandé d'accéder au portail client en utilisant l'adresse que vous connaissez habituellement. Ouvrez un navigateur Internet séparé et saisissez manuellement l'adresse officielle du site web dans la barre d'adresse. Cela garantit que vous accédez directement au site réel et non à une version potentiellement falsifiée. Pour faciliter l'accès au site web légitime, enregistrez l'adresse officielle dans vos signets ou favoris. Ainsi, vous pourrez y accéder rapidement et éviter les erreurs de saisie d'adresse.

Lorsque vous saisissez l'adresse manuellement, assurez-vous de vérifier attentivement que vous avez correctement orthographié le nom de domaine. Les cybercriminels peuvent utiliser des noms de domaine similaires pour créer des sites Web trompeurs. Soyez particulièrement vigilant avec les fautes de frappe courantes ou les remplacements de caractères (par exemple, “rn” à la place de “m” dans “amazon”).

1 adresse-mail dédiée pour 1 site

Utiliser une adresse e-mail dédiée à chaque site ou inscription est une bonne pratique pour protéger votre vie privée et réduire les risques de phishing. Voici quelques avantages de cette approche :

- Isolation des communications : En utilisant une adresse e-mail unique pour chaque site ou service, vous pouvez isoler les communications et les notifications liées à ce compte spécifique. Cela rend plus facile la gestion des e-mails et vous permet de filtrer les messages indésirables plus facilement.
- Détection rapide des tentatives de phishing : Si vous commencez à recevoir des e-mails suspects ou non sollicités sur une adresse spécifique, cela peut indiquer une tentative de phishing ou une violation de données. Vous pourrez ainsi réagir rapidement en prenant les mesures appropriées pour sécuriser vos comptes.
- Protection de la vie privée : En utilisant des adresses e-mail dédiées, vous limitez les chances que votre adresse principale soit exposée à des tiers non fiables. Cela peut aider à réduire le spam et les e-mails non sollicités.

L'utilisation d'un gestionnaire de mots de passe peut faciliter la gestion de plusieurs adresses e-mail ou alias. Il vous permet de stocker en toute sécurité vos informations et d'accéder facilement aux

différentes adresses e-mail associées à vos comptes.

Cependant, rappelez-vous qu'il est toujours important d'être vigilant et de prendre d'autres mesures de sécurité, telles que l'utilisation de mots de passe forts et uniques pour chaque compte, la vérification de l'authenticité des e-mails reçus et la sensibilisation aux techniques de phishing.

Une méthode courante pour avoir une adresse e-mail dédiée par site est d'utiliser le symbole “+” dans votre adresse e-mail existante. Voici comment cela fonctionne :

- Commencez avec une adresse e-mail principale : Tout d'abord, vous devez avoir une adresse e-mail principale à partir de laquelle vous allez créer des adresses dédiées. Par exemple, supposons que votre adresse principale soit “exemple@gmail.com”.
- Utilisez le symbole “+” : Lorsque vous vous inscrivez sur un site, ajoutez le symbole “+” suivi d'un identifiant unique avant le signe “@” dans votre adresse e-mail principale. Par exemple, si vous vous inscrivez sur un site appelé “siteexemple.com”, vous pouvez utiliser l'adresse “exemple+siteexemple@gmail.com”.
- Recevez les e-mails sur votre adresse principale : Les e-mails envoyés à votre adresse dédiée avec le symbole “+” seront automatiquement acheminés vers votre adresse principale. Vous recevrez donc tous les e-mails sur votre boîte de réception principale (“exemple@gmail.com”).

Cette méthode vous permet de créer des adresses e-mail dédiées pour chaque site ou service auquel vous vous inscrivez, tout en les faisant tous atterrir dans votre boîte de réception principale. Cela vous aide à garder une trace de l'origine des e-mails et à identifier tout site ou service qui pourrait partager votre adresse e-mail avec des tiers non autorisés.

Il est important de noter que tous les fournisseurs de services de messagerie ne prennent pas en charge le symbole “+”. Dans ce cas, vous pouvez envisager d'utiliser des services de messagerie tiers qui offrent des fonctionnalités d'alias d'e-mail pour créer des adresses dédiées.

N'oubliez pas que l'utilisation de cette méthode ne garantit pas une sécurité absolue, et il est toujours essentiel de rester vigilant face aux tentatives de phishing et de prendre d'autres mesures de sécurité pour protéger vos informations personnelles en ligne.

Afficher les messages en texte brut

Pour améliorer la sécurité des e-mails est d'afficher les messages en texte brut plutôt qu'en format HTML. Voici les avantages de cette approche :

- Élimination des contenus potentiellement dangereux : L'affichage des e-mails en texte brut désactive l'exécution automatique de contenu potentiellement dangereux, tels que les scripts ou les images malveillantes. Cela réduit le risque de téléchargement involontaire de logiciels malveillants ou de l'ouverture de liens nuisibles.
- Protection contre les techniques de dissimulation : Certains e-mails de phishing utilisent des techniques sophistiquées pour dissimuler des liens ou des pièces jointes malveillantes dans le format HTML. En affichant les e-mails en texte brut, vous pouvez voir directement les adresses e-mail et les liens tels qu'ils sont écrits, ce qui facilite la détection des anomalies ou des tentatives de tromperie.
- Réduction des risques de suivi : Les e-mails HTML peuvent contenir des balises de suivi

invisibles qui permettent aux expéditeurs de savoir si vous avez ouvert l'e-mail et si vous avez cliqué sur les liens. En affichant les e-mails en texte brut, vous pouvez éviter ce type de suivi indésirable.

Pour activer l'affichage des e-mails en texte brut, consultez les paramètres de votre client de messagerie ou de votre application de messagerie. Les étapes précises peuvent varier en fonction du logiciel que vous utilisez, mais recherchez des options telles que “affichage en texte brut” ou “désactiver le formatage HTML”.

Cependant, notez que l'affichage des e-mails en texte brut peut également désactiver certains aspects de mise en forme ou d'affichage visuel. Si vous décidez d'activer cette option, soyez prêt à accepter ces compromis pour améliorer la sécurité de vos communications par e-mail.