YouTubeチャンネルを盗まれてしまった方へ

YouTubeコントリビューター
Masaru Kamikura

2020年1月31日版

YouTubeチャンネルはGoogleアカウントにログインして管理します。
このGoogleアカウントに何者かが不正にログインし、YouTubeチャンネルを操作すれば、あなたのYouTubeチャンネルは奪われてしまいます。

不正ログインする一般的な方法

- 個人情報等から簡単に推測できるパスワードにしている
- GoogleやYouTubeを名乗る誰かにGoogleアカウントのIDやパスワードを教えてしまう
- 偽のログイン画面にパスワードを入力してしまう
- 他のサイトと同じパスワードを使っていて、他のサイトから流出したパスワードを使ってログインする

このどれかに当てはまる場合、ご自身のパスワード管理の問題が原因で、何者かがGoogleアカウントにアクセスして、YouTubeチャンネルの管理権限が奪われている可能性があります。

パスワードはもちろん、アカウントの管理をしっかり行っているのにアカウントにログインされたような場合は、もっと深刻な問題になっている可能性があります。

Googleアカウントの管理を見直す

アカウントのパスワードは銀行の暗証番号と同じように、しっかり管理する必要があります。
YouTubeチャンネルが乗っ取られてしまった認識がある場合は、まずはGoogleアカウントの管理を見直してください。
これを先に行わないと、チャンネルを取り戻しても、また盗まれてしまいます。

パスワードをユニークで他人が想像できない物にする

まずは、Googleアカウントのパスワードを変更してください。
すでに現在のパスワードは他人に知られている可能性があるので、パスワードを変更します。

変更するパスワードは

- 他のサービスで同じ物を使っていない、これからも使わないユニークな物（そのアカウントだけで使う一意な物）

- 個人情報などから推測できない物にする（誕生日、名前等をパスワードに含めない（1月2日生まれの山田さんがyamada0102にするような事））
- なるべく長いパスワードにする（8文字以上）

という条件で設定してください。

2段階認証を設定する

2段階認証（多要素認証）を設定します。
2段階認証を設定すればパスワード入力後に、もう一つの認証が加わります。ここで追加の認証しなければログインできないので、他人がパスワードを入手しても簡単にはログインできません。

> 注意:
> 偽のログインページで自分でログインして他人にパスワードを教えているような場合は、2段階認証も自分で認証しています。
> この2段階認証を設定すれば完璧に守られるわけではありません。

Googleの2段階認証は携帯電話のSMSの登録を基本です。
さらにスマートフォンの認証アプリ、バックアップコードなども2段階認証のバックアップ用に提供されるので、これらも忘れずに設定してください。

復旧用のメールアドレス、電話番号などを設定する

Googleアカウントにアクセスできなくなった場合などに備えて、復旧用のメールアドレス、電話番号を登録します。
復旧用のメールアドレスはアクセスできなくなった場合だけではなく、Googleアカウントにログインした際にも、新規ログイン通知が届くので、仮にアカウントにログインしても通知を見れば対処が早くできるようになります。

サードパーティーのサイトやアプリを確認する

Googleアカウントは様々なサービスやアプリが簡単にアクセスできる様にアプリなどのアクセス許可をする場合があります。
アカウントへのフルアクセス（全ての情報を確認、編集できる）を要求するアプリやサービスもあります。中には不正にフルアクセスを設定している場合もあるので、そのようなアプリやサービスの権限は削除してください。
よくわからない場合は、一旦全て削除する事が推奨されます。全て削除しても本当に必要な物は再度認証すれば使えるようになります。

サードパーティーのサイトやアプリに関するヘルプ
https://support.google.com/accounts/answer/3466521

Googleアカウントのセキュリティ診断をする

上記のパスワード設定、2段階認証、サードパーティーのアクセス権限などは、Googleのセキュリティ診断で一括して設定確認できるようになっています。

Googleセキュリティ診断
https://myaccount.google.com/security-checkup

普段からアカウントへ届くセキュリティ関連のメールを確認する

アカウントへの新規ログインなどのセキュリティイベントはメールで届きます。
このようなメールは常に確認するようにしてください。

アカウントの管理体制を見直す

Googleアカウントは個人に対して提供されています。
グループや会社で利用しているような環境で、1つのGoogleアカウントを複数人でアクセスできる様にしているような場合、様々なトラブルが発生する可能性があります。

YouTubeチャンネルを複数人で管理する場合、ブランドアカウントを活用してください。

YouTubeでのブランドアカウントの仕組み
https://support.google.com/youtube/answer/9367690

YouTubeチャンネルを取り戻す方法

YouTubeチャンネルを誰かに奪われた場合、取り戻すのはかなり難しいです。
Googleはアカウントがハイジャックされた場合に備え、復旧手段もありますが、それで取り戻せるかはわかりません。

まずは前述したGoogleアカウントの管理を見直してください。
その上で、該当のGoogleアカウントにログインし、チャンネルの管理権限があるかチャンネル切り替え機能で確認してください。

チャンネル切り替え機能
https://www.youtube.com/channel_switcher

ここに該当のチャンネルがない場合、管理権限を盗まれています。

YouTubeチャンネルが盗まれた場合、復旧手段にアクセスする方法として次の方法が用意されています。

- クリエイターサポートへ連絡
- Twitterの@TeamYouTubeへ連絡
- YouTubeコミュニティ経由で復旧作業

クリエイターサポートは、YouTubeパートナープログラムに参加している場合に利用出来るサポートです。
YouTubeチャンネルを奪われた場合、このサポートにアクセスできなくなっているかも知れません。過去にやりとりした場合はその履歴から連絡出来るかも知れません。

> https://support.google.com/youtube/answer/3545535
> クリエイターサポートへの連絡方法

Twitterを利用している場合は、日本語で@TeamYouTubeにメンションを送れば反応があると思います。（この件に限らず、いきなりDMを送っても対応されません）

> https://twitter.com/TeamYouTube
> @TeamYouTubeのTwitterアカウント

どの方法も利用出来ない場合は、YouTubeコミュニティに投稿してください。

> https://support.google.com/youtube/community
> YouTubeコミュニティ

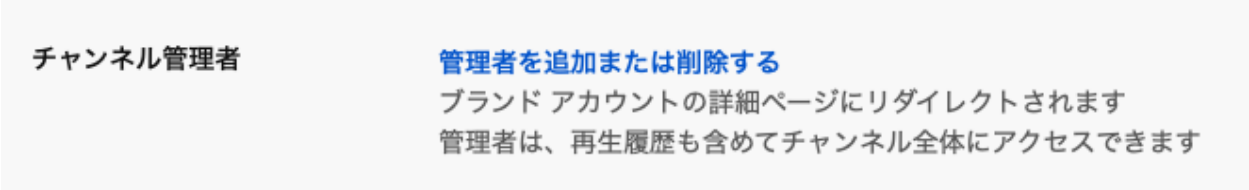
どの場合でも、最短でも数週間単位で時間がかかります。特にYouTubeのコミュニティでやりとりするはさらにその数倍の時間がかかります。

お金を払えばYouTubeチャンネルを戻すと言われた場合

YouTubeチャンネルを盗んだ犯人が、お金を払えばYouTubeチャンネルを戻すと言ってくる場合があるかも知れません。
ランサムウェア（身代金ウェア）というデータを暗号化するコンピューターウイルスがありますが、これと同じように身代金を要求する犯罪と思われます。
ランサムウェアの場合、お金を払っても戻ってこない事がほとんどだそうです。

不正なログインを認識した場合

YouTubeチャンネルを盗むことだけが目的の場合、YouTubeチャンネルをブランドチャンネルにして、チャンネルの管理権限を奪います。
メールの通知などで不正なログインが確認された場合、すぐにパスワードなどの変更後、チャンネル管理者の設定を確認してください。
https://www.youtube.com/account



この後に説明していますが、一般的なチャンネルの管理権限を奪う手法は、オーナー権限の移行が必要で、これには1日かかります。
仮に不正にログインされて初期の設定をされても、この段階で対処すればチャンネル自体が盗まれることを防げます。

チャンネルが盗まれていることがわかった場合

Googleアカウント自体にログイン出来る場合、前述したようにパスワードを変更し、2段階認証を設定し、アカウントを保護してください。
セキュリティ診断も実行して、ログインされたデバイスの状況を確認し、不審なアプリがないかなど、アカウントの状態を確認してください。

Googleアカウントにログイン出来ない場合、まずはアカウントの復旧を実行してください。

> https://support.google.com/youtube/answer/76187
> アカウントがハイジャックされた場合の対処方法
>
> https://myaccount.google.com/security-checkup
> セキュリティ診断

YouTubeチャンネルの権限移行には1日かかります

YouTubeチャンネルの管理権限を盗む方法は次のようになっています。

- 対象のGoogleアカウントにログインする
- YouTubeチャンネルがブランドアカウントで管理されていない場合、ブランドアカウントにする
- 犯人のアカウントをブランドアカウントの管理者として追加する
- 追加した管理者のアカウントをメインの管理者に変更する

最後のメインの管理者への変更には、ブランドアカウントの管理者に追加してから1日程かかるため、ログインされた事に気づけばすぐに対応できます。

ログインされた事やブランドアカウントの設定時に、Googleアカウントに設定しているメールアドレスに通知が届きます。仮にログインされたアカウントに攻撃者がログインし、そのメールを削除していても、復旧用のメールアドレスにも通知は届くので、1つのアカウントで不正アクセスの被害にあってもその事実に気づくことが可能です。

YouTubeチャンネルが盗まれる際にGoogleから通知されること

YouTubeチャンネルを盗むような、Googleアカウントに通常とは異なる環境からログインする場合、ログインした事の通知がユーザーのメールアドレス等に届きます。
偽のGoogleログイン画面にログインしようとした場合も、裏では本物のサイトにログインしているので通知があります。

普段使っている環境からアクセスしているのに、新規ログイン通知が来る場合、認証が完了し、不正ログインされている可能性もあります。

YouTubeチャンネルの管理権限を変更する際にも通知が届きます。

これらの通知を常に確認していれば、ログインされた事自体にすぐ気づけるので、チャンネルの管理権限を移動する前に対処できます。

普段のアカウントの管理が重要です。

YouTubeチャンネルを盗む理由

YouTubeパートナープログラムに参加しているチャンネルを盗めば、そこから簡単にマネタイズが可能です。
単に盗んでAdSenseの紐付けを変更するだけでもチャンネルの規模にもよりますが、収益を得ることが出来ます。

チャンネルの規模が小さい場合でも、YouTubeパートナープログラムの審査に合格しているので、チャンネルを改変して収益化出来る自分のチャンネルに作り替えてしまうことも、新規でチャンネルを作成するより簡単に出来るので需要があります。

ほとんどの場合、盗んだ本人は収益化せず、盗んだYouTubeチャンネルを規模に応じた額でブラックマーケットで販売する事になります。

Googleアカウント自体を盗むことが目的の場合

YouTubeチャンネルの管理権限を盗むのではなく、Googleアカウント自体を盗んだりすることが目的の場合があります。
この場合、さらに復旧が困難になることもあり得ます。

YouTubeからメールが届いた際に確認すべき事

YouTubeは様々なメールをYouTubeの利用者に向けて送信しています。
メールの送信者名にYouTubeとあることだけで信用せずに、本当の送信者は誰なのか、本当にYouTubeからのメールなのかを確認してください。

> 注意:
> 最終的にはメールが本物かどうかを見分けることは出来ません。基本的に全て偽物と思って行動するのが安全です。
> その理由はこちらのサイトで説明していますが、ここでは基本的な知識として確認方法を紹介しています。

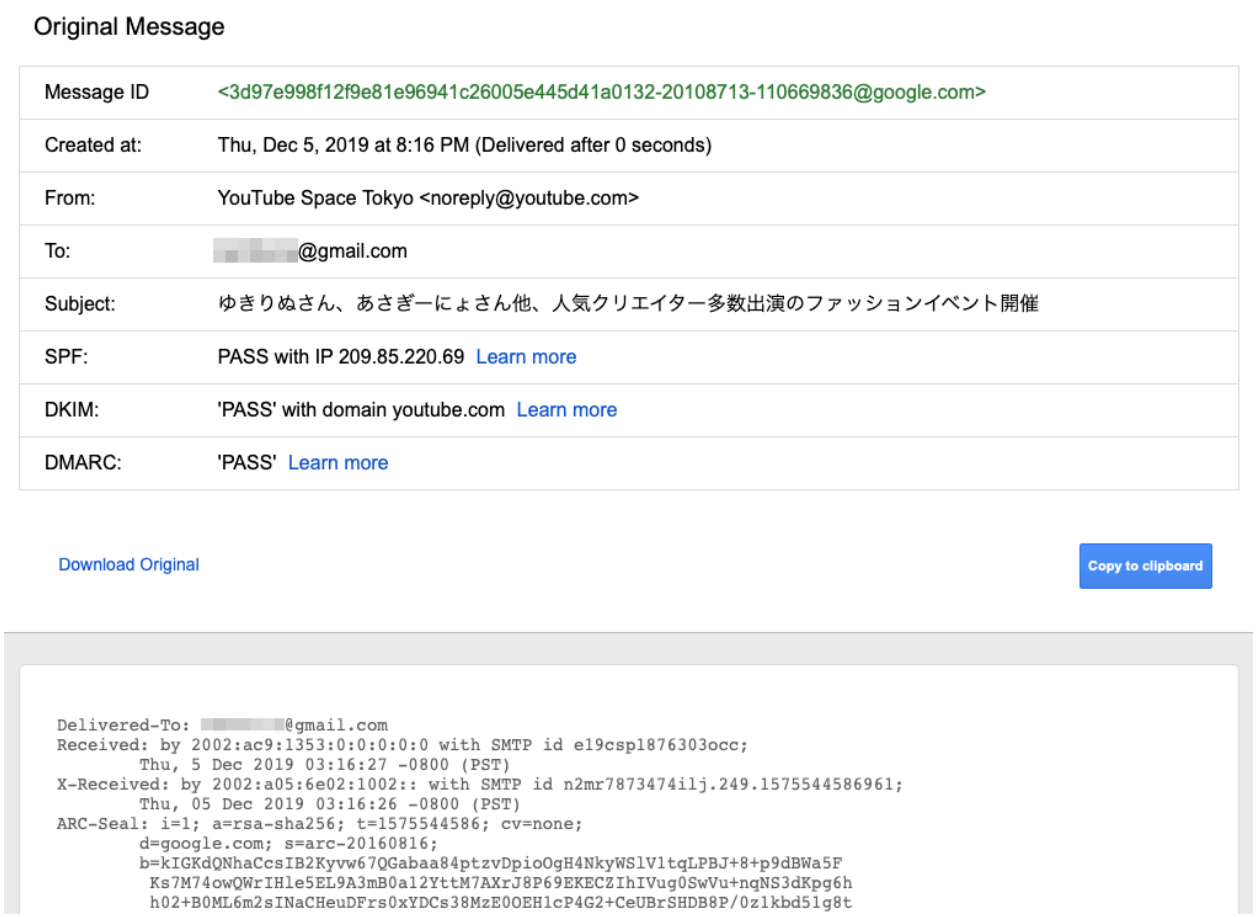
メール送信者の確認方法

送信者のメールアドレスが、@google.comや@youtube.comになっているか確認します。
この送信者のメールアドレスを偽造することも出来るので、リンクをクリックしたり、何らかのアクションが必要な場合は、メッセージのソースを表示します。

> 注意:
> スマートフォンの場合はここから説明している方法で確認するのは難しいので、確認は困難です。

Gmailの場合は、左側の「・・・」を盾にしたメニューから「メッセージのソース」を表示します。

このような画面になり、SPF、DKIM、DMARCがPASSになっていて不正なメールではないことが確認できます。
不正なメールの場合はこの画面がこの画像とは異なる状態になっていることがほとんどです。



Original Message

Message ID	<3d97e998f12f9e81e96941c26005e445d41a0132-20108713-110669836@google.com>
Created at:	Thu, Dec 5, 2019 at 8:16 PM (Delivered after 0 seconds)
From:	YouTube Space Tokyo <noreply@youtube.com>
To:	[redacted]@gmail.com
Subject:	ゆきりぬさん、あさぎーにょさん他、人気クリエイター多数出演のファッションイベント開催
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain youtube.com Learn more
DMARC:	'PASS' Learn more

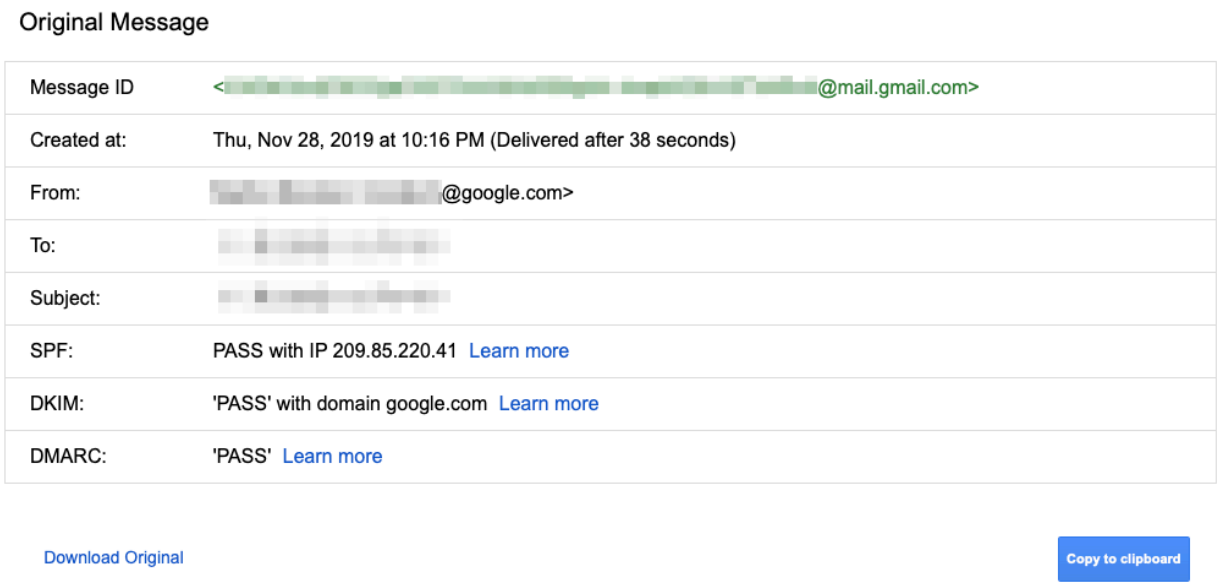
Download Original

Copy to clipboard

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:ac9:1353:0:0:0:0:0 with SMTP id e19csp1876303occ;
        Thu, 5 Dec 2019 03:16:27 -0800 (PST)
X-Received: by 2002:a05:6e02:1002:: with SMTP id n2mr7873474ilj.249.1575544586961;
        Thu, 05 Dec 2019 03:16:26 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1575544586; cv=none;
        d=google.com; s=arc-20160816;
        b=kIGKdQNhaCcsIB2Kyvw67QGabaa84ptzvDpioOgH4NkyWSlV1tqLPBJ+8+p9dBWa5F
         Ks7M74owQWrIHle5EL9A3mB0a12YttM7AXrJ8P69EKECZIhIVug0SwVu+nqNS3dKpg6h
         h02+B0ML6m2sINaCHeuDFrs0xYDCs38MzE0OEH1cP4G2+CeUBrSHDB8P/0z1kbd51g8t
```

GoogleやYouTubeの関係者からメールが直接届いた場合

YouTubeが機械的に送っているシステムから送られてくるメールや、メールマガジンなどではなくて、実際のGoogleやYouTubeの関係者が個別にメールを送ってくることもあります。
その場合も、通常 @google.comのアドレスから届くので、メッセージのソースを確認すれば @google.com から正しく送られてくることがわかります。



Original Message

Message ID	<[redacted]@mail.gmail.com>
Created at:	Thu, Nov 28, 2019 at 10:16 PM (Delivered after 38 seconds)
From:	[redacted]@google.com>
To:	[redacted]
Subject:	[redacted]
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

@youtube.comや@google.com以外から送信されたメールアドレス、送信先からのメールは何らかの詐欺メールの可能性があるので、リンクのクリックや返信、記載されている電話番号への通話はしない方がよいでしょう。

メールに関する詳細を知りたい場合は、こちらのヘルプ等を確認してください。
https://support.google.com/mail/answer/29436

紛らわしいドメインの詐欺

メールアドレスやドメインで注意したいのはホモグラフ攻撃という、紛らわしいドメイン名による詐欺です。
例えば、google.com、youtube.comはgoogle.comやyoutube.comとは違うドメインです。
このような、見た目はそのままだけど、異なるドメインを使った詐欺メールなどが今後届く可能性があるので、見た目はそのままだけど、異なる物がある事はしっかりと認識しておきましょう。

本物から送られてくる詐欺

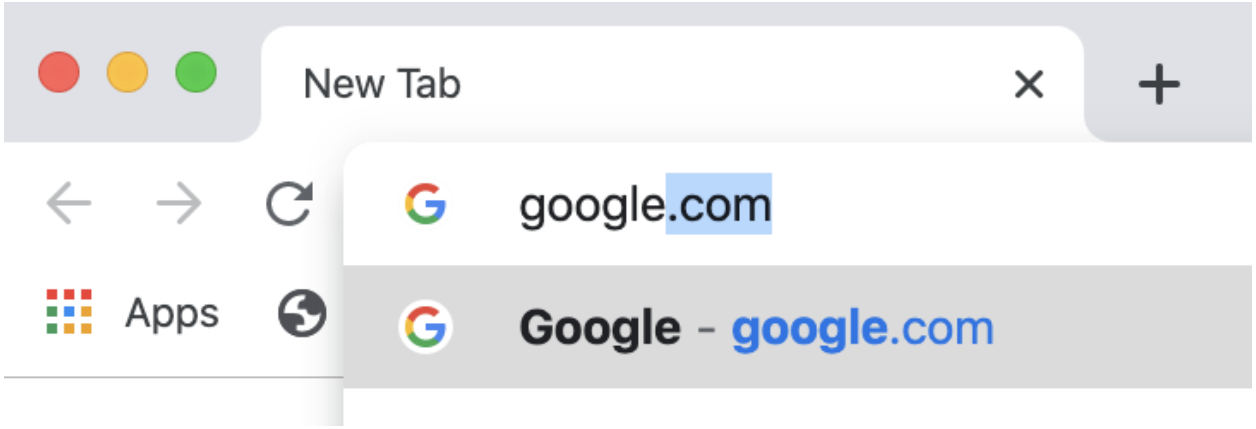
どう調べても本物から送られてくる詐欺もあります。
例えば、社員のアカウントを盗んで正規のアカウントから詐欺メールを送るという手法があります。
実際に日本でもこの被害にあった航空会社があり、ビジネスメール詐欺として報道されました。

Googleではこのような詐欺に関連した報告はないようですが、今後ある可能性はゼロではありません。

お金やアカウントに関する怪しいメールは全て疑ってかかるのも悪い判断ではないです。

基本的なアカウントの保護方法

オレオレ詐欺では銀行員を名乗る人に暗証番号を教えないように呼びかけていますが、これと同じようにGoogleアカウントのパスワードはGoogleやYouTubeの社員を名乗る人含め、誰にも教えないでください。

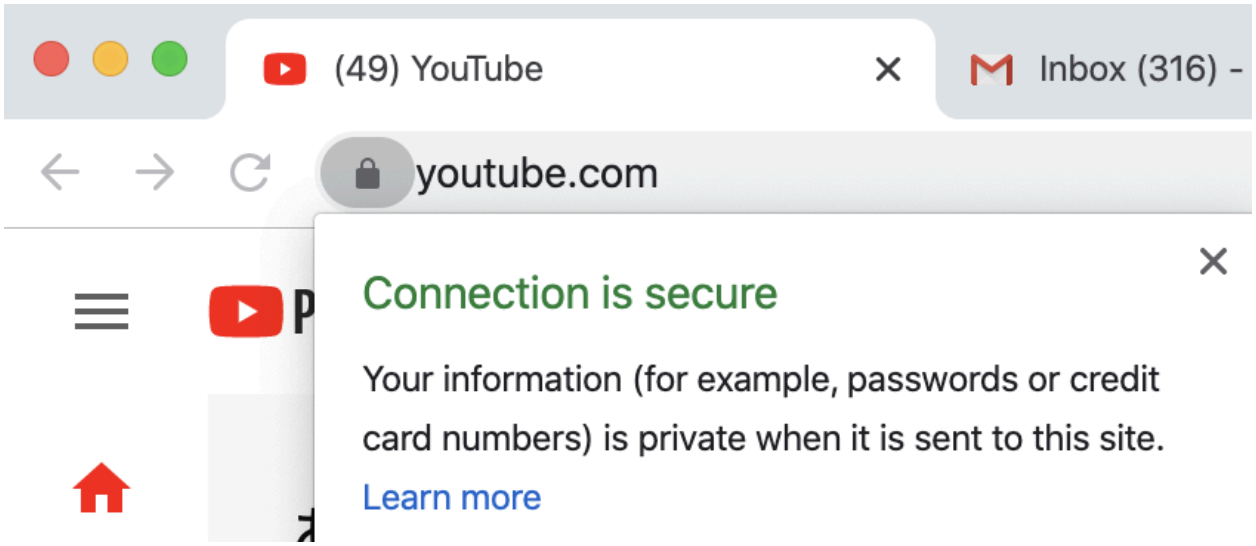


偽のログイン画面を見分けるのは難しいですが、ログインする際は、どこかのリンクをクリックするのではなく、ブラウザに google.com や youtube.com などのアドレス直接入力して直接アクセスしてログインしてください。
パスワードはアカウント毎に設定して、どこかで漏れたパスワードを使ってもログインできないようにしてください。

メールが本物かどうかを確認する場合は、この文章の最後にある[YouTubeからメールが届いた際に確認すべき事]を読んでください。

> 注意:
> スマートフォンの場合、これから説明する確認方法の操作は難しいので、もしもログイン画面などが出た場合はログインしないというのが最も安全です。

接続したサイトが本当にYouTubeなどかを確認する場合、Chromeブラウザの場合は横にある鍵マークから様々な情報が確認できます。
youtube.comに見た目そっくりなドメイン、youtube.com以外に他の文字がついているドメイン等の場合もありますので注意してください。



Chromeブラウザの場合のサイトの接続が安全か確認する方法
https://support.google.com/chrome/answer/95617

さらにアカウントを守る基本的な方法

2段階認証にする。
ログイン時に携帯電話のSMSに送られるコードを入力するように設定しておけば、パスワードが漏れたとしてもログインできません。
もちろん、パスワードを教えるような人はこの2段階認証のコードも教えるかも知れませんので、これが完璧なわけではありません。
根本的にセキュリティ意識を持つことが必要になります。

二段階認証の設定方法
https://support.google.com/accounts/answer/185839

チャンネルが盗まれるとどうなるか

多くの盗難されたYouTubeチャンネルには著作権違反など、YouTubeで禁止されている動画がアップロードされています。

その結果、チャンネルが停止になる事が多いです。

盗まれたチャンネルであっても、チャンネルが停止した場合、他のGoogleアカウントやYouTubeチャンネルにもそのペナルティが加わる可能性があります。

そのため、盗まれたからあきらめて新しくチャンネルを作り直しても、作り直したチャンネル自体が問題なくても停止になることもありえます。

このため、盗まれたチャンネルは取り戻すための手続きをすることが推奨されます。

盗まれないように、普段のアカウント管理、セキュリティスキルの向上が最も重要です。

以上

その他のリソース
https://sites.google.com/view/teampe