ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●タスク管理ツール「Trello」、ユーザー側の設定不備によりデータ公開状態の報告相次ぐ

https://www.itmedia.co.jp/news/articles/2104/06/news080.html
https://www.itmedia.co.jp/news/articles/2104/06/news118.html
https://www.itmedia.co.jp/news/articles/2104/07/news129.html
https://www.atlassian.com/ja/blog/trello-public-board

このニュースをザックリ言うと･･･

- 4月上旬、プロジェクト管理・タスク管理を行うWebサービス「Trello」において機密情報が公開状態になっているという指摘がSNSや匿名掲示板等で相次いで報告されました。

- 指摘があった情報の内容は、企業の内部情報、店舗の採用希望者の個人情報、さらには個人が利用するサービスのアカウント情報等、多岐にわたっています。

- 4月6日(日本時間)、Trello運営元のAtlassian社から声明が出され、Trelloのデフォルトの設定では非公開であるとし、また意図しない情報の漏洩を止めるため、ユーザーのサポートに尽力するとしています。

AUS便りからの所感等

- クラウド上に情報を保存するサービスの設定ミスで外部から閲覧可能となっていたケース自体は珍しいものではなく、特に昨年12月には楽天グループ、今年1月・2月にもイオングループより、営業管理サービス「Salesforce」で管理していた情報に設定の不備で第三者からアクセスされたことが発表され、内閣サイバーセキュリティーセンターから注意喚起が出される事態にもなっています(https://www.nisc.go.jp/active/infra/pdf/salesforce20210129.pdf)。

- Trelloにおいては、いずれもデフォルトで非公開となっている設定をユーザー側が公開状態に変更していたものとみられ、かつそれにより、Google等サーチエンジンからも検索可能な状態となっていた模様ですが、少なからぬユーザーが公開状態への設定変更を行ったことについては、ユーザーインターフェース上の説明がわかりにくかった可能性も指摘する声もあります。

- ともあれユーザー側においては、サービスの公開設定に関して十分に調査するとともに、第三者として外部からアクセス可能でないか、Webブラウザーのプライベートウィンドウ機能を用いて確認する等の自衛策をとることが肝要です。

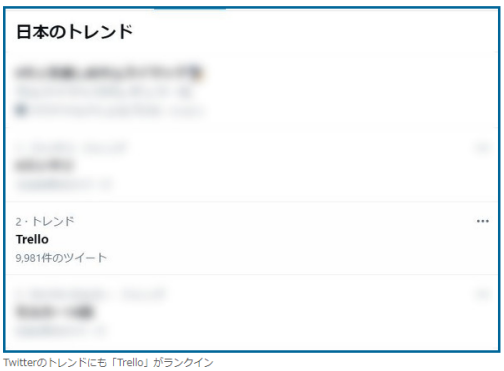
ITmedia NEWS

プロジェクト管理ツール「Trello」で運転免許証など個人情報流出　閲覧範囲の設定ミスが原因か

2021年04月06日 12時10分 公開　[樋口隆元，ITmedia]

印刷　見る　Share　B! 327

プロジェクト管理ツール「Trello」経由で個人情報が流出している――4月5日深夜から6日の朝にかけて、こうした投稿がネット上で注目を集めている。閲覧設定を「公開」としていたことが原因とみられる。Twitterのトレンドにも「Trello」がランクインした他、「公開設定のまま利用」など関連キーワードもランクインした。



Twitterのトレンドにも「Trello」がランクイン

流出騒ぎのTrello、運営元が声明　「初期設定は『非公開』」「意図しない情報漏えいを止めるためサポート」

2021年04月06日 17時18分 公開　[ITmedia]

印刷　見る　Share　B! 167

プロジェクト管理ツール「Trello」経由で個人情報を含むユーザーの書き込んだ情報が一部公開されていた問題で、運営会社の豪Atlassianは4月6日、「ユーザーサポートに尽力する」と公式ブログで発表した。

プロジェクト管理ツール「Trello」

Atlassianは一連の騒動が「閲覧範囲を『公開』と設定していたことに起因」と説明。「初期設定ではボードの閲覧範囲は『非公開』になっており、ユーザーの任意で公開範囲を選択できる」とした。

●Facebookユーザー5.33億人の情報、犯罪フォーラムに…2019年に流出したデータとFB発表

https://internet.watch.impress.co.jp/docs/yajiuma/1316512.html
https://www.itmedia.co.jp/news/articles/2104/04/news016.html

このニュースをザックリ言うと･･･

- 4月3日(現地時間)、米国の複数のメディアより、Facebook(以下FB)の日本を含む世界のユーザー5億3,300万人の個人情報がサイバー犯罪フォーラムにおいて公開されていると相次いで発表されました。

- フォーラムで公開されたデータは、2019年9月に4億1,900万件以上のFacebook IDとそれに紐付いた電話番号のデータの流出が発覚した(AUS便り 2019/9/17号参照)際のものであることがFBより発表されています(その際に悪用された脆弱性も修正済みとしています)。

- 公開されているデータは、ユーザーが「基本データ」において登録したもので、携帯電話番号等について非公開設定にしていたものに関しても含まれているとのことです。

- また、データは国毎にダウンロードが可能とされ、日本人のデータは428,625人分が含まれていたとされています。

AUS便りからの所感

- さらに厳密にいえば、2019年9月のFBからの発表の時点で、そのデータは「2018年4月にFBが携帯電話番号でユーザーを検索する機能を終了した時点のもの」であるとされていました。

- そのような新しくないデータであっても、この時に被害を受けていたユーザーの多くは3年後の現在も同じ電話番号やメールアドレスを利用していると考えられ、スパムメールや営業電話等への悪用は十分有効とみられます。

- 一般論として、ユーザー側においては、各種情報を特に登録する必要がある場面以外ではむやみに登録しない等の自衛策をとることが推奨されるものの、サービスによっては個人の年収から勤務先の社員数とか売り上げ等こと細かな情報の登録を要求するものもあり、サービス提供者側においてもFBの事例を他山の石とせず、センシティブな情報の収集を行わないようにする方向性へ進んでいくことを願いたいものです。


Impress Watch

Facebookから流出した日本人約40万人を含む全世界約5億人の個人情報が「再公開」

tks24　2021年4月5日 13:20

2019年にFacebookから流出した全世界約5億人の個人情報が、自由にダウンロードできる形で再公開されていたことが明らかになった。

これはFacebookの脆弱性によって2019年に流出した個人情報で、日本人約40万人を含む全世界約5億人もの膨大なデータ。Facebookで「基本データ」として登録されている情報が対象であることから、氏名や国名、性別のほか電話番号やメールアドレスなど極めてプライベートな情報が含まれており、リストには創設者であるMark Zuckerbergの個人情報も含まれるという噂も。ハッキング関連のフォーラムで誰でもダウンロード可能な形で公開されているこのデータ、Facebookは2019年の段階で脆弱性は修正したとされており、当時流出したものがあらためてアップロードされたとみられる。ユーザー側としては取れる対策は流出したであろうことを前提に、電話番号やメールアドレスの利用に注意するしかない。

●TEPCO・ゆうちょ・au等を騙るフィッシング、対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/tepco_20210406.html
https://www.antiphishing.jp/news/alert/jp_bank_20210409.html
https://www.antiphishing.jp/news/alert/au_20210409.html

このニュースをザックリ言うと･･･

- 4月上旬、フィッシング対策協議会より、クレジットカード3件、仮想通貨取引所2件、その他サービス2件の計7件のフィッシングに関する注意喚起が出されています。

- 例を挙げると、4月6日(日本時間)、東京電力を騙り、同社運営のサービス「くらしTEPCO」の偽サイトに誘導するフィッシングについての注意喚起を出しています。

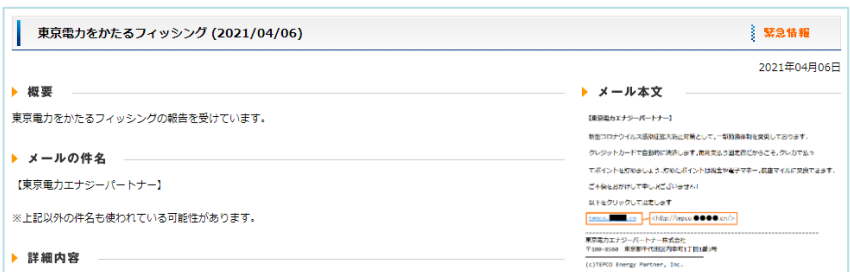
- 4月9日には、ゆうちょ銀行系クレジットカードのJP BANKと、auを騙るフィッシングの2件についての注意喚起が出ています。

AUS便りからの所感

- 同協議会から短期間でこれだけの注意喚起が出るのはここ数年でも珍しく、また4月2日に発表された、3月に寄せられたフィッシング報告件数も4万件を超えており(AUS便り 2021/04/05号参照)、引き続きこれまで以上に多種類のフィッシングメールが送られてくる可能性に警戒するに越したことはありません。

- とは言え、今のところはフィッシングへの防御策として全く新しい策をとらなければならない状況にはないと思われ、利用しているサービスについて公式発表やSNSでの情報に注視する、サイトへのアクセスはブックマークから行う、等を焦ることなく淡々と実施するのが良いでしょう。

フィッシング対策協議会
Council of Anti-Phishing Japan


東京電力をかたるフィッシング (2021/04/06)　緊急情報

2021年04月06日

概要

東京電力をかたるフィッシングの報告を受けています。

メール本文

メールの件名

【東京電力エナジーパートナー】

※上記以外の件名も使われている可能性があります。

詳細内容