

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。

●「あなたはラッキービジターです」不審なポップアップ表示…都教委の採用ページ、改ざんで一時停止

<https://www.itmedia.co.jp/news/articles/1905/14/news091.html>
http://www.kyoiku.metro.tokyo.jp/press/press_release/2019/release20190513_02.html



このニュースをザックリ言うと…

- 5月13日（日本時間）、東京都教育委員会より、教員採用案内のWebサイトが不正アクセスを受け、コンテンツが改ざんされていたと発表されました。
- 改ざんにより、アクセス時に「親愛なIEユーザー様 あなたは、5月12に、2019のラッキービジターです。アンケートに答えていただいた方に『ありがとう』を含めて、Samsung Galaxy S10+を差し上げます」という内容のポップアップが表示され、不審なサイトに誘導されるようになっていたとのことです。
- 12日に利用者からの情報提供を受け、同日夕方にはサイトの公開を停止、調査の結果13日に改ざんが確認されたとのことです。

AUS便りからの所感等

- 当該サイトでは個人情報を保存していなかったためサイトからの流出はないとする一方、**誘導先のサイトにおいて個人情報の流出があったかについてはまだ確認していない**とのことです。
- 攻撃者がWebサイトの改ざんを行うに至る経路は、Webサイトの管理画面から直接不正ログインするもの、サイト管理者のPCに侵入するもの等様々ですので、それぞれについてセキュリティを確保し、加えて万が一の改ざん発生から復旧できるようデータバックアップを随時実施することが重要です。
- 「親愛な(使用しているブラウザ)ユーザー様」「ラッキービジターです」という慣用句、そして**不自然な年月日の表記を含む不審なポップアップ**は、Webサイトに表示する広告として不正な広告コンテンツが配信される形でも2018年頃から発生が報告されており、閲覧する側としては、アンチウイルスやWebブラウザあるいはUTMのアンチフィッシング機能を可能な限り有効にすることにより、防御を固めることを推奨致します。



「あなたはラッキービジターです」不審なポップアップ表示 都教委の採用ページ、改ざんで一時停止

© 2019年05月14日 13時05分 公開

[ITmedia]

印刷 70 Share B! 5

東京都教育委員会は5月13日、教員採用案内のWebページが不正アクセスによって改ざんされ、「アンケートに答えればGalaxy S10+をプレゼントする」とうたうサイトに誘導するポップアップが表示される状態になっていたため、同サイトを停止したと発表した。原因を究明し、安全性を確認次第、再開するとしている。

改ざんされていたのは、教員の採用案内などを掲載していたサイトで、URLは「http://www.kyoinsenko-metro-tokyo.jp」。閲覧したユーザーから12日、「意図しないサイトに誘導される画面が出現する」と情報提供があったという。

このユーザーのPCに表示されていたのは、「親愛なIEユーザー様 あなたは、5月12に、2019のラッキービジターです。アンケートに答えていただいた方に『ありがとう』を含めて、Samsung Galaxy S10+を差し上げます」などと書かれたポップアップ。

都教委のPCでは状況を再現できなかったが、このユーザーとのやりとりから事象を確認し、サイトが改ざんされたと判断して一時停止することにした。担当者は、「ポップアップは、サイトに初めてアクセスした人だけに表示されていたようだ。Webブラウザのユーザー調査を装ってアンケートに答えさせ、個人情報などを詐取る、いわゆるブラウザアンケートのフィッシング詐欺ではないか」とみている。

同サイトは個人情報保存していないため、個人情報の流出はない。閲覧者が意図しないサイトに誘導されたことで個人情報の流出があったかどうかについては確認していないという。



東京都公立学校教員採用案内（東京都教員免許案内を含む）ホームページの一時停止について

公開日：令和元年（2019）5月13日

教育庁

東京都公立学校教員採用案内（東京都教員免許案内を含む）ホームページ（以下、「教員採用案内ホームページ」という。）が外部からの不正アクセスによる改ざんを受け、このホームページは現在公開停止中です。ホームページの公開停止期間中、利用者の皆様には迷惑と御不便をお掛けして申し訳ありませんが、復旧に向けて緊急対応をしておりますので、御理解と御協力をよろしくお願ひいたします。

1 概要

教員採用案内ホームページ（http://www.kyoinsenko-metro-tokyo.jp）が外部からの不正アクセスによる改ざんを受け、当ホームページを閲覧した際、意図しないサイトに誘導するポップアップが組み込まれていた。

2 経緯

- (1) 令和元年5月12日（日曜日）、教員採用案内ホームページを閲覧した方から、「意図しないサイトに誘導される画面が出現する」という情報提供があった。
- (2) 教育庁人事課長室において、当該事象を確認できたことから、同日夕方から教員採用案内ホームページの公開を停止した。
- (3) 令和元年5月13日（月曜日）正午頃、ホームページ運営委託会社の調査により、教員採用案内ホームページの改ざんが判明した。

3 影響

教員採用案内ホームページは個人情報等を閲覧していないため、都保有の個人情報の流出はありません。また、閲覧者が意図しないサイトに誘導されたことにより、個人情報の流出があったかどうかについては確認されていません。

●Instagramインフルエンサーらの個人情報、4,900万件が流出か

<https://japan.cnet.com/article/35137231/>



このニュースをザックリ言うと…

- 5月20日（現地時間）、ITニュースサイトTechCrunchより、写真共有SNS「Instagram」のインフルエンサー（影響力のあるユーザ）アカウント情報約4,900万件が外部サイトで公開されていたと報じられました。
- データはインドのマーケティング会社が所有するデータベースが収集していたものとされ、Instagramで公開されているプロフィール情報の他、電話番号や電子メールアドレスなどの非公開データも含まれていたとのことです。
- あるセキュリティ研究者がデータベースを発見し、前述の会社に問合せた結果、現在はアクセスできない状態になっているとのことです。

AUS便りからの所感等

- 4月にはInstagramの親会社であるFacebookにおいても約5億4,000万件のアカウント情報流出が発覚しており（AUS便り 2019/04/15号参照）、SNS自体への不正アクセスではなく、サードパーティー（外部企業）が収集していた情報のデータベースが公開状態にあった点で共通しています。
- 今回のようなことがあるからという理由でデータベースを社内のサーバに保存する（オンプレミス）にしても、社内ネットワークからのアクセスを適切に制限しなければ、一たび侵入した攻撃者に容易にアクセスされる恐れがありますので、UTM等を用いたネットワークのセグメント分けをはじめ、行うべき対策を洗い出し、実施することが肝要です。



Instagramインフルエンサーらの個人情報、4900万件が流出か

Laura Hoadley | CNET News | 報道元: 産経新聞 | 2019年05月21日 10時54分

UPDATE Instagramのインフルエンサーは、普段から自分たちの生活を人々に公開している。だが、データベースの漏えいにより、彼らについて知ることのできる情報がさらに公開されてしまったようだ。

TechCrunchの報道によると、インフルエンサーやブランドのアカウントを含むInstagramユーザーのアカウント情報4900万件以上がオンライン上で公開されていたという。このデータには、Instagramユーザーのプロフィール情報から集めたと思われる公開データだけでなく、電話番号や電子メールアドレスなどの非公開データも含まれていた。

記事によれば、このデータベースは、自社製品を宣伝したいブランドとインフルエンサーをつなぐ事業を手がけるインドのマーケティング企業Chtrboxのものである。Chtrboxはコメントの依頼に対して回答しなかった。

Instagramの広報担当者は声明の中で次のように述べた。「われわれは現在、電子メールや電話番号を含む問題のデータがInstagramから流出したのか他のソースから流出したのかを知るために、この問題を調査しているところだ。また、このデータがどこから入手し、どのような経緯で公開されたのかを知るために、Chtrboxに問い合わせている」

Instagramは利用規約で、アカウント情報の収集を禁じている。Chtrboxのウェブサイトによれば、同社はクライアントとして18万4000人以上のInstagramインフルエンサーを抱えている。これは、データベースにあったとされる数千万件という記録の数よりもはるかに少ない。

●4月のフィッシング報告状況発表…前月より報告件数増加、AppleやAmazonをかたるフィッシングメールを多数確認

<https://securityblog.jp/news/20190513.html>



このニュースをザックリ言うと…

- 5月2日（日本時間）、フィッシング対策協議会より、4月に同協議会に寄せられたフィッシング報告状況が発表されました。
- 4月の報告件数は2,388件で前月（2,352件）より36件増加、一方フィッシングサイトのURL件数は1,238件で前月（1,207件）より31件減少しています。
- 前月と同様、AppleおよびAmazonをかたるフィッシングメールが大量に配信された他、金融機関・クレジットカード・仮想通貨関連サービスおよびメルカリといったブランドのフィッシングが確認されているとのことです。

AUS便りからの所感等

- 月間のフィッシング報告件数は、2017年8月から2018年2月にかけて1,000件前後を推移していたものが、2018年3月以降は1,500件を超える状況が続いています（同9・10月を除く）。
- また、宅配業者や通信キャリアをかたるフィッシングも少数ながら報告が続いており、例えばセキュリティ強化・アップデート等の名目で、不正なスマホアプリのインストール等を誘導されるケースについても、注意が呼び掛けられています。
- 同協議会でも回避策として挙げていますが、利用しているサービスの正規のサイトへは、不審なメール上のリンクからではなく、正規のアプリや事前に登録したブックマークからアクセスするよう是非とも心掛けてください。



4月も報告件数増加、AppleやAmazonをかたるフィッシングメールを多数確認

2019年5月13日

5月2日、フィッシング対策協議会は、2019年4月の月次報告書を公開した。

これによると、フィッシング報告件数は2,388件となり、前月(2,352件)より36件増加した。また、フィッシングサイトのURL件数は1,207件で、こちらは前月より31件の減少。そして、フィッシングに悪用されたブランド件数は40件で、前月と同じだった。

4月もフィッシング報告件数は引き続き増加しており、AmazonやAppleをかたるフィッシングが大量に配信されている傾向は変わっていない。また、金融機関やクレジットカードのブランド、仮想通貨関連サービスをかたるフィッシングも多く報告された。新たなブランドとして、メルカリをかたるフィッシングも確認されている。