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。

●ドメイン管理サービスへの不正ログインか…企業のドメイン名乗っ取られる

https://www.itmedia.co.jp/news/articles/2406/04/news120.html
https://www.nikkei.com/nkd/disclosure/tdnr/20240603519251/

このニュースをザックリ言うと･･･

- 6月3日、ファッション系ネット通販業の夢展望社より、子会社トレセンテ社の公式サイトのドメイン名(trecenti.com)が第三者に奪取されたと発表されました。
- ドメイン管理サービスへの不正ログインにより、5月29日に海外の別の管理サービスに当該ドメイン名を移管されたとしています。
- 当該ドメイン名の移管以外で、サーバーへの不正アクセスや個人情報等流出等の被害は確認されておらず、別のドメイン名で運営されているトレセンテ社のECサイトについても影響はないとのことです。

AUS便りからの所感等

- ドメイン名が第三者に入手される事例としては、失効したドメイン名が正規に登録されるものが知られ、特に終了からさほど時間が経っていないサービスで使われていたドメイン名を乗っ取り、不審なサイトへの誘導に利用する「ドメインスクワッティング(サイバースクワッティング)」という攻撃手法が知られています。
- 今回のように利用中のドメイン名が第三者に乗っ取られる事例では、レジストリロック(トランスファーロック)がかかっていなかったためにアカウントへの不正ログイントを経ずとも移管手続きが実行されるケース、またJPドメインではレジストリロックがない上に申請から10日以内に拒否しなかった場合に成立してしまうルールが悪用されたケースもあります。
- 外部に移管する作業を行っているのでない限り、レジストリロックが提供されていればそれを有効にすることが大前提となりますが、ドメイン管理サービスのアカウントに不正ログインされた場合にこれを解除される等して不正移管に繋がる恐れがあり、アカウントに対し強固かつ他のサービスで使っていないパスワードを設定すること、加えてサービスが提供する多要素認証を利用することにより、確実に保護することも決して忘れてはいけません。

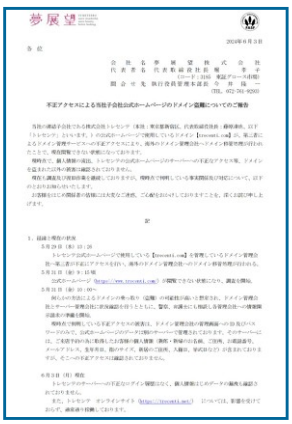
ITmedia NEWS

公式サイトのドメイン盗まれアクセス不能に　ドメイン管理会社への不正アクセスが原因　夢展望子会社

2024年06月04日 12時42分 公開　［岡田有花，ITmedia］

ファッション通販サイト運営の夢展望は6月3日、子会社で結婚指輪販売などを手掛けるトレセンテの公式サイトのドメイン「trecenti.com」が乗っ取られ、サイトにアクセスできなくなったと発表した。ドメイン管理会社が不正アクセスを受け、海外のドメイン管理会社に移管処理が行われたという。

失ったドメインを取り戻すことは難しいと判断し、別途新たなドメインを入手して公式サイトを移管する予定だ。


夢展望 2024年6月3日

不正アクセスによる当社子会社公式ホームページのドメイン盗難についてのご報告

夢展望の開示より

●小学校教師のPC「サポート詐欺」で遠隔操作…児童約200人分の個人情報流出か

https://www.ktv.jp/news/articles/?id=12760
https://www.asahi.co.jp/webnews/pages/abc_25969.html
https://www.town.kumatori.lg.jp/material/files/group/1/20240603-houdouteikyou2.pdf

このニュースをザックリ言うと･･･

- 6月3日(日本時間)、大阪府熊取町教育委員会より、同町の小学校児童の個人情報がいわゆる「サポート詐欺」によって流出した可能性があると発表されました。
- 関西地方のテレビ局での報道によれば、被害を受けたのは、同町立小学校の教師が受け持っている児童約30人の集合写真・個人名等(学級通信に掲載)と、以前受け持っていた別の市の小学校の児童約170人分の活動記録・成績所見とされています。
- 5月29日、同教師が資料作成を行っていたPCで突如「ウイルスにかかっています」等といった警告が表示され、記載された電話先からの指示に従ったところ、PCを遠隔操作され、児童の情報が入ったフォルダーが削除されていたとしています。
- 同日中に校内の他のPCやサーバーを含めウイルスチェックを行いましたが、感染は確認されなかったとのことです。

AUS便りからの所感

- サポート詐欺でよく使用される「偽のセキュリティ警告画面」については、IPAが体験サイトを公開(https://www.ipa.go.jp/security/anshin/measures/fakealert.html 、AUS便り 2023/12/20号参照)しており、例えば偽の警告画面のフルスクリーン表示を解除する方法として「ESCキーを一定時間押す」ことが挙げられています。
- 一方で今回サポート先を騙る相手からもこの操作が指示されたと報じられており、被害者を安心させ、詐欺を成功させやすくする意図があったと考えられ、様々な攻撃の手口についてユーザーが学習、および組織内で周知し、慎重な行動をとってもらうことが肝要です。

8 日テレ

【速報】児童200人分の個人情報『教師のPC』から漏洩『片言の日本語』指示に教師が従ってしまう

06月05日 10:39

■PC画面フリーズ「ウイルスにかかっています」とメッセージ
大阪府熊取町教育委員会は、町立の小学校教師がパソコンに保存していたおよそ200人分の児童の個人情報が漏洩したと発表しました。

熊取町教委によると先月29日、熊取町立中央小学校で30代の女性教師が資料作成中にネットで検索したフリーのイラストを資料に挿入しようとしたところ、パソコンの画面が突然フリーズし「ウイルスにかかっています」と書かれたメッセージが表示されました。

■メッセージに従い電話　指示通り操作「遠隔操作」開始さらにウイルス感染からパソコンをサポートする旨のメッセージが届き、「505」から始まる10桁の電話番号が表示されたことから、教師はメッセージに従い電話をかけ、通話相手の指示通りパソコンの操作を行ないました。そして、教師が通話相手の「初めにescapeキーを10秒押す」「その次にWindowsキーとRキーを同時に押す」という指示通りにパソコンを操作したところ、通話相手による遠隔操作が始まったということです。

●gmailではなくgm「e」ilへ…高校生徒個人情報等第三者へメール送信か

https://www.yomiuri.co.jp/national/20240601-OYT1T50016/

このニュースをザックリ言うと･･･

- 5月31日、滋賀県教育委員会より、同県立高校からインターンシップに参加した生徒140人分の個人情報(氏名・生年月日・住所・保護者名)等が学外に流出した可能性があると発表されました。
- 同高校教諭が私用のGMailアドレスにデータを送信しようとして、「***@gmail.com」となっていたメールアドレスを「***@gmeil.com」と誤入力して送信していたことが原因としています。
- 上長からメール送信の許可を得ていたものの、パスワードによるデータの保護やアドレスの確認を怠っていたとしています。

AUS便りからの所感

- gmail.comに似たドメインへの入力ミスによる送信の事例は過去たびたび発生しており、2022年には埼玉県の大学から「@gmai.com」へ、2023年には大阪府の大学から「@gmeil.com」へ、それぞれメール転送設定を誤り、長期間情報が流出していたことが明らかになっています。
- ユーザー側で入力ミスを完全に防止するには限界があり、メーラー自身やアドオンあるいはメールサーバー等に対するソリューションとして提供される誤送信防止機能の導入による対策を強く推奨致しますが、一方で前述したような実害が度々発生しているドメイン名については、メールサーバーの設定で遮断するよう設定するのも検討に値するでしょうし、製品であれば有害なドメイン名としてデフォルトで設定されるようになることも期待したいものです。

YOL 讀賣新聞オンライン

滋賀県立高教諭、「ｇｍａｉｌ」でなく「ｇｍｅｉｌ」に誤送信…生徒１４０人分の個人情報流出

2024/06/01 12:21　この記事をスクラップする

滋賀県教育委員会は３１日、県立湖南農業高校（草津市）の教諭が、私用アドレスにデータを送信する際、メールアドレスのドメイン（インターネット上の住所）の入力を誤り、生徒１４０人分と、４９事業所の情報などが含まれるメールを誤送信したと発表した。悪用は確認されていない。

滋賀県の地図

発表によると、２５日午後、同校の教諭が、今年度行う生徒のインターンシップ（就業体験）のデータを私用アドレスに送る際、「ｇｍａｉｌ」を「ｇｍｅｉｌ」と誤って入力した。誤送信先は送信者のミスを狙った「ドッペルゲンガー・ドメイン」と呼ばれている。