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。

●練馬区の中学校、誤って生徒にSNSのパスワード提出を要求…区教委が謝罪

https://www.tokyo-np.co.jp/article/147263
https://mainichi.jp/articles/20211203/k00/00m/040/497000c
https://togetter.com/li/1812166

このニュースをザックリ言うと･･･

- 12月3日(日本時間)、東京都練馬区教育委員会より、同区の中学校において生徒のSNSのパスワードを提出するよう要求する事態が発生していたことが発表されました。

- 11月30日、家庭でのSNSルール等と一緒にパスワードの記入・提出が求められたとする、Twitterでの保護者からの報告が発端とされています。

- その後の各報道において、これが同区による安全なSNS利用啓発のための「SNS練馬区ルール」のリーフレットを用いたものであった一方、パスワードを記入させての提出は当該中学校での手違いによるものだったことが明らかになり、同教委は個人情報の取り扱いが不適切だったとして謝罪しています。

AUS便りからの所感等

- 「SNS練馬区ルール」の取り組みは2020年6月に開始、区内の小中学校にリーフレットが配布され、スマホ・SNSの一日の利用時間等を家庭内で話し合って記入することが想定されていましたが、一方で「SNSのパスワードは　　です」という記入欄があることについては、学校がパスワードを知り得ることへの懸念が指摘されていました。

- これを受け、同年8月に区教委から各学校へ、リーフレットの提出を依頼する際には当該項目を「未記載」か「消した状態」で提出してもらうよう通知が出ていましたが、今回当該中学校においてはこの説明を行うことを失念していたとされています。

- 学校・会社含め、組織で管理していない外部サービスのアカウント情報を要求(あるいは提出)することはプライバシーの侵害や不正アクセス禁止法への抵触に繋がり得るものであり、今回について言えば、通知をもとに学校から生徒に周知してもらうだけに留まらず、リーフレット(PDFはもちろん印刷済のものも含め)について修正を行う等の措置を可能な限りとるべきであったと考えます。

練馬区教育委員会は区内の中学校一校が、生徒が使っているＳＮＳのパスワードを紙に記入させ、学校に提出させていたと発表した。個人情報の不適切な取り扱いがあったとして三日、堀和夫教育長が謝罪するコメントを出した。情報漏えいはないという。

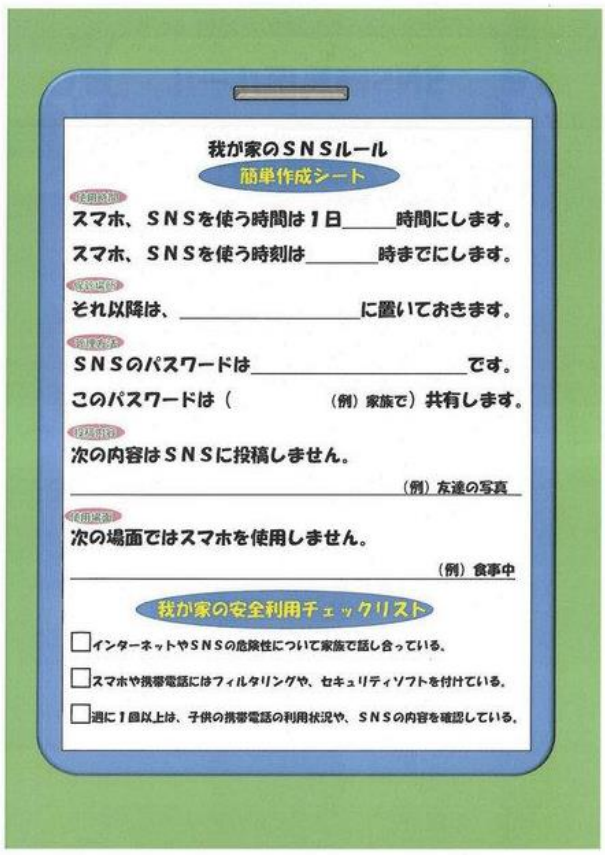
区教委によると、家庭内でのＳＮＳの使い方を啓発するため、区が児童生徒に配ったリーフレットの中で「我が家のＳＮＳルール」として、一日に使う時間や時刻と共にパスワード記入欄があった。家庭内でルールを共有してもらい、安全につなげる狙いだったが、作成当初に区教委の会議では「学校がパスワードを知るのは不適切」と指摘。

東京新聞

東京

安全なSNS利用の啓発のはずが…練馬区の中学校で生徒のパスワード提出させる　教育長が謝罪

2021年12月7日 07時12分



▲パスワードの記入欄がある「ＳＮＳ練馬区ルール・リーフレット」（区提供）

●人気アニメ公式ECサイトに不正アクセス…カード情報17,828名分流出か

https://www.itmedia.co.jp/news/articles/2112/01/news107.html
https://www.evangelion.co.jp/news/2021_1130/
https://www.evastore.jp/

このニュースをザックリ言うと･･･

- 11月30日(日本時間)、グラウンドワークス社より、同社運営による、人気アニメ作品のグッズを扱うECサイト「EVANGELION STORE(オンライン)」が不正アクセスを受け、クレジットカード情報が流出した可能性があると発表されました。

- 被害を受けたとされるのは、2020年6月8日～2021年6月30日に同サイトでカード決済を行った17,828名分のクレジットカード情報(名義・番号・有効期限・セキュリティコード)および同サイトへのログイン情報(メールアドレス・パスワード)とされています。

- 7月12日に流出の懸念について連絡を受けて決済を停止しており、第三者機関による調査の結果、不正アクセスによるペイメントアプリケーションの改ざんが行われたことが原因とされています。

AUS便りからの所感

- 発表によれば、EVANGELION STOREグループの他のサイトとは完全に分離したシステムであるため、実店舗および「Yahoo! ショッピング」上の別店舗には影響はないとのことです。

- ECサイトからのカード情報漏洩は、以前取り上げたコマキ楽器WEBサイト(AUS便り 2021/08/31号参照)やTANAXオンラインショップ(同2021/11/09号参照)の例のように、Webサイトの注文ページ周り等を改ざんし、偽の決済ページへの誘導や、フォームに入力された内容の攻撃者への送信を行うよう改変する等により、セキュリティコードも含めたカード情報の奪取を行う手口が主流となっています。

- 独自にECサイトを立ち上げる場合には、Webアプリケーションやサーバーの脆弱性について確実に修正・対策を行い、攻撃者による侵入や改ざんの余地をなくすよう努めるとことが肝要であり、加えて攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置、および情報の流出を食い止める出口対策についても検討することを強く推奨致します。


ITmedia NEWS

「エヴァ」公式ECでクレカ情報流出か　セキュリティコード含む1万7828件

2021年12月01日 13時02分 公開　[松浦立樹，ITmedia]

アニメ「エヴァンゲリオン」シリーズなどの著作権管理を手掛けるグラウンドワークス：は11月30日、同社が運営するECサイト「EVANGELION STORE（オンライン）」が第三者の不正アクセスを受け、顧客のクレジットカード情報1万7828件が漏えいした可能性があると発表した。一部の顧客のカード情報は、不正利用された可能性もあるという。

EVANGELION STORE

EVANGELION STORE オンライン（休店中）

2021年11月30日

お客様各位

株式会社グラウンドワークス

弊社株式会社グラウンドワークスが運営する「EVANGELION STORE(オンライン)」への
不正アクセスによる個人情報漏えいに関するお詫びとお知らせ

このたび、弊社株式会社グラウンドワークスが運営する「EVANGELION STORE(オンライン)」(https://www.evastore.jp/)におきまして、

●11月度フィッシング報告数は48,461件…8月度以降の高水準続く

https://www.antiphishing.jp/report/monthly/202111.html

このニュースをザックリ言うと･･･

- 12月3日(日本時間)、フィッシング対策協議会より、11月に寄せられたフィッシング報告状況が発表されました。

- 11月度の報告件数は48,461件で、10月度(https://www.antiphishing.jp/report/monthly/202110.html)の48,740件からは279件減少となっている一方、フィッシングサイトのURL件数は7,575件(10月度7,418件)、悪用されたブランド件数は82件(10月度77件)とそれぞれ増加しています。

- 報告全体に対するブランドの割合については、最も多いAmazonは28.5%と10月度(28.2%)より微増、これにメルカリ・三井住友カード・楽天・ETC利用照会サービスを合わせた5ブランドで約67.7%(10月度 66.6%)、また1,000件以上の報告があったブランドが9あり、これらで全体の約79.2%を占めたとしています。

- この他にも同協議会からは、11月に8ブランドのフィッシングについて、また12月にも既に東京都水道局を騙りクレジットカード情報を詐取しようとするフィッシングについて注意喚起が出されています(https://www.antiphishing.jp/news/alert/waterworks_metro_tokyo_20211202.html)。

AUS便りからの所感

- 報告件数は減少が続いているとはいえその幅は小さく、初めて5万件を超えた8月度より前に比べ、非常に高い水準を維持している状況です。

- 調査用メールアドレス宛に届いているフィッシングメールの傾向として、送信元として正規のメールアドレス(ドメイン)を使用した「なりすまし」メールの割合が8月度以降90%前後を維持(11月度は約89.0%)、他にも中国のIPアドレスからの送信についても8～10月度は90%台に上っていた(11月度は約81.7%、また国内IPアドレスからも約5.5%)とされています。

- 一方で、DMARCによる送信元メールアドレスの検証と迷惑メールフィルターにより、多くの「なりすまし」メールが排除できているともされ、自社ユーザーのみならず取引先ユーザーについてもフィッシングメールからの保護を行う意味でも、可能な限りDMARC(およびSPF)といった検証機構を自社メールサーバーおよびドメイン名に関して設定することが有用となるでしょう。

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