— AUS（アルテミス・ユーザ・サポート）便り 2021/06/22号 —
https://www.artemis-jp.com

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。

●エムアイカード、りそな、NTTグループ…クレジットカードを騙るフィッシングの注意喚起相次ぐ

https://www.antiphishing.jp/news/alert/micard_20210615.html
https://www.antiphishing.jp/news/alert/resonacard_20210616.html
https://www.antiphishing.jp/news/alert/mylink_20210617.html

このニュースをザックリ言うと･･･

- 6月15日から17日(日本時間)にかけて、フィッシング対策協議会より、クレジットカード各社を騙るフィッシングへの注意喚起が相次いで出されています。

- 同15日に注意喚起が出されたのはエムアイカードを騙るフィッシングメールで、件名は「Webエムアイカード利用確認」その他、文面は「このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので…」とするものが例に挙がっています。

- 同16日のりそなカードを騙るフィッシングの注意喚起では、「【重要なお知らせ】【りそなVISAカードVpass】ご利用確認のお願い」等という件名で、文面は一部が前述のエムアイカードのもの共通している模様です。

- また、同17日のNTTグループカードを騙るフィッシングの注意喚起で挙げられているメールの例は、「【NTT】お取引のご確認」等の件名、「このたび、お客さまのお取引につきまして、第三者による不正利用の可能性を検知したため、一時的にお取引をお止めしました」等という文面からなっています。

AUS便りからの所感等

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

- いずれのフィッシングも、クレジットカードのWebサービスのアカウントと、各種カード情報を詐取する偽サイトへ誘導するものとなっていますが、特にりそなカードのフィッシングサイトはVJAグループ発行のクレジットカード向けサービス「Vpass」の偽サイトとなっており、今後フィッシングのターゲットが同グループの各カード利用者に広がることも考えられます。

- 同協議会からの各注意喚起には本物のカード業者からの注意喚起へのリンクも貼られていますので、常日頃から、あるいはフィッシングメールを受け取った際に、こういった各社・団体からの啓発情報およびTwitter等における報告がないか検索等で確認するとともに、利用しているサービスへは予めブラウザーのブックマークに登録してアクセスする等の自衛策をとるよう心掛けてください。

【りそな銀行】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。
つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

りそなカード株式会社

■発行者■
りそなカード株式会社
東京　〒135-0042　東京都江東区木場1-5-25
大阪　〒541-0051　大阪市中央区備後町2-1-8

□部分のリンク (URL)
<https://www3.vpass-ne.●●●●/>

メール文面例

●インターン学生40名分の個人情報流出…Excelファイル上でマスクしたのみ、PDF化してもコピー可

https://scan.netsecurity.ne.jp/article/2021/06/14/45809.html

このニュースをザックリ言うと・・・

- 5月26日(日本時間)、鳥取県中小企業団体中央会より、同会が実施している「とっとりインターンシップ推進事業」に関連する個人情報の流出が発生していたことが発表されました。
- 被害を受けたとされるのは、インターンシップ参加学生40名分の個人情報(氏名・学校名・学部・学年・携帯電話番号・メールアドレス・エントリー先企業名等)とのことです。
- インターンシップ関連Webサイト開発委託業務のプロポーザル募集の際、資料として4月30日にアップロードされたPDFファイルに前述の個人情報が含まれていることが指摘され、5月25日に当該資料を削除しています。
- また、サーチエンジンにおいて該当する学生の氏名で検索することにより、関連する情報が表示される状態にもなっていたとしています(現在は削除依頼により、表示されない)とのことです)。

AUS便りからの所感

- PDFファイル上でコピー&ペーストによる個人情報の閲覧が可能であったことが流出(およびサーチエンジン掲載)の原因とされていますが、PDFの変換元となったExcelファイルにおいて、個人情報部分にはマスキングを施されたのみの状態であり、「PDFデータに変換すれば、マスキング前の個人情報にはたどり着かない」という誤った認識にあったとのことです。
- マスキングされるデータ自体をテキストレベルから修正・削除すること、その状態でできるかぎりExcelファイルないし変換後のPDFファイルで機密データの検索・コピー等が可能でないか確認することが対策として肝要です。
- 注意すべきはテキストに留まらず、貼り付けられた画像データ上に機密情報が含まれていて、それを単にマスクしたという場合でも、画像データのみを抜き出される恐れがありますので、やはりその画像データ自体を修正する必要があることに注意しましょう。

●ECサイト構築ツール「EC-CUBE」バージョン3向けプラグインにXSSの脆弱性

https://scan.netsecurity.ne.jp/article/2021/06/17/45831.html
https://www.jpcert.or.jp/at/2021/at210028.html

このニュースをザックリ言うと・・・

- 6月11日および14日(日本時間)、イーシーキューブ社より、同社開発のECサイト構築ツール「EC-CUBE」バージョン3系のプラグインにクロスサイトスクリプティング(XSS)の脆弱性が確認されたとして、注意喚起が出されています。
- 11日の発表では、サードパーティー開発の「配送伝票番号プラグイン」「配送伝票番号csv一括登録プラグイン」「配送伝票番号メールプラグイン」について、管理画面上でXSSが発生する可能性があるとし、修正バージョンへのアップデートが呼び掛けられています。
- 14日にはイーシーキューブ社開発の「帳票出力プラグイン」「メルマガ管理プラグイン」「カテゴリコンテンツプラグイン」についても、同様にXSSの脆弱性が存在するとしており、やはり修正バージョンへのアップデートが推奨されています。
- 同15日にはIPA・JPCERT/CCからも同様に注意喚起が出され、既に脆弱性を悪用した攻撃も確認されているとしています。

AUS便りからの所感

- EC-CUBEは現在バージョン2・3・4系がサポート中で、今年5月にはバージョン4系にのみ存在するXSSの脆弱性が報告(AUS便り2021/05/17号参照)されていましたが、今回はバージョン3系にのみ影響する、また別の脆弱性となります。
- イーシーキューブ社では、2019年以降、EC-CUBEの脆弱性を悪用した攻撃によりサイトの改ざん等が行われ、クレジットカード情報の流出にまでつながる事案が発生していることを鑑み、度々対策の実施を呼び掛けていますので、EC-CUBEで構築されたサイトを運営している場合には随時同社からの情報を確認し、根本的対策としてのアップデートを速やかに実施できる体制を整えるとともに、サーバー自体の防御をも強固にすることが重要です。
- また、攻撃者が管理者のPCを踏み台にしてサイトの管理画面にアクセスする等の可能性も考慮し、そちらもアンチウイルスやUTM等による防御を固めることを怠らないようにしましょう。