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。

●2月度フィッシング報告件数は48,611件…対策協議会発表、えきねっと騙るフィッシングにも注意喚起

https://www.antiphishing.jp/report/monthly/202202.html
https://www.antiphishing.jp/news/alert/ekinet_20220304.html
https://www.itmedia.co.jp/news/articles/2203/07/news095.html
https://www.eki-net.com/top/oshirase/attention/202201.pdf

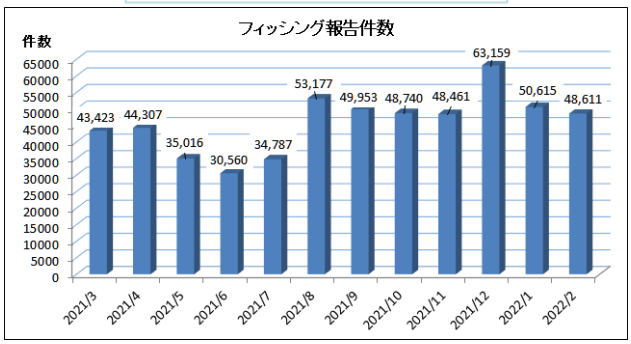
このニュースをザックリ言うと･･･

- 3月3日(日本時間)、フィッシング対策協議会より、2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。
- 2月度の報告件数は48,611件で、1月度(https://www.antiphishing.jp/report/monthly/202201.html)の50,615件からは2,004件減少となっています。
- 一方で翌日の3月4日、同協議会から千葉銀行とえきねっとを騙るフィッシングの注意喚起が出ていますが、特に後者に関するフィッシングメールの報告がTwitter上等でも相次いでおり、決してアカウント情報・個人情報あるいはクレジットカード情報を入力しないよう呼び掛けられています。

AUS便りからの所感等

- 昨年8月度に53,177件を記録してから現在までの7ヶ月間、報告件数が最も少なかった11月度でも48,461件と、48,000件超の水準で推移し続ける状況となっています。
- えきねっとを騙るフィッシングメールは件名「【重要】えきねっとアカウントの自動退会処理について」等が確認されていますが、えきねっとにおいては実際に昨年6月にサービスのリニューアルが行われ、同9月に自動退会に関する文書が掲載されており、フィッシングはこれを模倣した巧妙な手口をとったことが指摘されています。
- えきねっと運営元のJR東日本からは2月22日の時点で同じくフィッシングに関する注意喚起が出ており、3月1日以降に送信する自動退会処理に関するメールにおいてはURLを掲載しない措置をとったとしています。
- なお同社では、正規のサイトのURLは「www.eki-net.com/●●●」のように「eki-net.com」の直後に「/（スラッシュ）」が入るとしていますが、現時点でのフィッシングサイトのドメイン名が「ek1-net-●●●●.live」「eki-net.●●●●.shop」等であるとはいえ、今後「●●●-eki-net.com」(この場合eki-netの直前にハイフンが入っています)というドメイン名が登録される可能性もあることには注意が必要です。
- 対策協議会が推奨する対策については、今回の月例報告より「事業者のみなさまへ」および「利用者のみなさまへ」に分けられて掲載されており、例えば何らかのサービス運営者ではない組織のメールサーバー管理者においても、前者で挙げられているDMARC・SPFさらにはBIMIといった、不審なメールの排除またはその助けとなり得る機構の導入を可能な限り検討、内部で提案すべきでしょう。

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

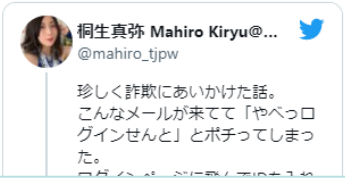


ITmedia NEWS

「これ詐欺だったの？」――「えきねっと」をかたるメール、手口の巧妙さが話題に　“自動退会処理”に注意

2022年03月07日 13時14分 公開　[松浦立樹，ITmedia]

JR東日本が提供する、指定券予約サービス「えきねっと」をかたるフィッシングメールが出回り、その手口の巧妙さが話題になっている。プロレスラーの桐生真弥さん（@mahiro_tjpw）は3月5日、「詐欺にあいかけた話」として、フィッシングメールが届いたことをTwitterに投稿。「このメールはレベルちょっと高かった。近年で一番」と注意を促している。



● Firefoxに致命的な脆弱性…97.0.2等へのアップデートを

https://forest.watch.impress.co.jp/docs/news/1393185.html
https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/

このニュースをザックリ言うと・・・

- 3月5日(現地時間)、米Mozillaより、Firefoxブラウザーの致命的な脆弱性を修正するセキュリティアップデートがリリースされました。
- 脆弱性は致命的なもの2件(CVE-2022-26485, CVE-2022-26486)が報告されており、PC用Firefoxバージョン97.0.2等で修正されています。
- 既に攻撃も確認されているとのことで、早急にアップデートの確認が推奨されています。

AUS便りからの所感

- セキュリティアップデートとして、他にも企業向けFirefox ESRバージョン91.6.1、Android版Firefox(Focus含む)バージョン97.3の他、メーラーThunderbirdについてもバージョン91.6.2がリリースされています。
- 脆弱性を悪用する手段は不明ですが、悪意のあるWebページへのアクセス等で攻撃を受ける恐れが考えられます。
- Firefoxの更新設定については、バージョン90(2021年7月リリース)以降、起動していない場合にも自動更新を行う機能が追加されましたが、場合によってはそれ以前の「更新の確認は行うが、インストールするかを選択する」に設定されている可能性があり、その設定を維持するとしても、「ヘルプ」→「Firefoxについて」を開くことにより、最新バージョンかどうかの確認、あるいは最新でない場合にもアップデートを怠りなく実施するよう心掛けましょう。

- Firefox ESR（v91.6.1で修正）
- Firefox for Android（v97.3で修正）
- Focus（Android版はv97.3で修正）
- Thunderbird（v91.6.2で修正）

● IPA、「情報セキュリティ10大脅威 2022」公開…組織ランキング7位に「ゼロデイ攻撃」初登場

https://www.ipa.go.jp/security/vuln/10threats2022.html

このニュースをザックリ言うと・・・

- 1月27日(日本時間)、IPAより「情報セキュリティ10大脅威 2022」の概要が発表されました。
- 2021年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約150名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。
- 各カテゴリーとも10大脅威はほぼ昨年度と同じ顔ぶれの中で順位が変動していますが、唯一組織側において「修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)」が7位に初登場しています。
- 2月28日には個人側の脅威に関する解説書が公開されており、3月上旬には同じく組織側の驚異の解説書も公開予定となっています。

AUS便りからの所感

- 昨年12月にJNSA社が発表した「2021セキュリティ十大ニュース」(AUS便り 2022/1/5号参照)のように、年末年始等には、大手セキュリティベンダーや関連団体等から、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度における業界の動向予測等がリリースされています。
- タイミング的に組織側の脅威の解説書は公開間近か、既に公開済みとみられますが、その折にでも挙げられている各項目に目を通し、自分自身や自組織に関連するもの以外であっても各種脅威について知識を得る、あるいは以前に得た知識が正しいかの再確認をし、今後の行動に役立てるのが良いでしょう。

■「情報セキュリティ10大脅威 2022」　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位