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。

●大阪万博公式を騙るXアカウント1,137件確認、万博協会が注意喚起

https://www.sankei.com/article/20240724-GXX6YTVMVRLS3PYCVM4QMR3WU4/
https://www.expo2025.or.jp/news/news-20240724-03/
https://jvcea.or.jp/news/main-info/20240716-001/

このニュースをザックリ言うと･･･

- 7月24日(日本時間)、日本国際博覧会協会より、2025年大阪・関西万博の公式を騙る偽のX(旧・Twitter)アカウントが確認されたとして注意喚起が出されています。

- 注意喚起によれば、偽アカウントは給付金の支給をほのめかすものが確認され、不審なサイトに誘導され、個人情報が不正に取得される恐れがあるとしています。

- また一部報道によれば、同22日の時点で計1,137件の偽アカウントが確認され、弁護士を通じてXへの申請を行い、凍結されているとしています。

- 同協会では、今回の万博の公式アカウントは、日本語アカウント(@expo2025_japan)および英語アカウント(@expo2025japan)のみであるとしており、アカウント名を確認するよう警告しています。

AUS便りからの所感等

- 報道で示されていた偽アカウントの例では、bioが暗号資産(仮想通貨)取引所への登録を促す等殆ど万博と関係ない内容、サイトのリンクも日本暗号資産取引業協会(JVCEA)の偽サイトとみられ、JVCEAでは注意喚起が出ています。

- 上記偽アカウントのアカウント名はランダムな文字列でしたが、前述した本物のアカウントと見分けがつきにくいアカウント名を用いる可能性も十分に考えられます。

- パリオリンピックについてもチケットに関連する詐欺が確認される(AUS便り 2024/07/18号)等、大きなイベントに便乗した詐欺やマルウェア感染等を目論むサイバー犯罪は付き物であり、本物の運営団体やセキュリティ関連団体からの注意喚起、実際にメールやSMSが送信される場合のポリシーを確認し、決して無闇にリンクをクリックしないよう慎重に行動してください。

THE SANKEI NEWS

大阪・関西万博のX偽アカ1137確認、個人情報不正取得の可能性も　注意呼びかけ

2024/7/24 16:15

ライフ | くらし　２０２５年大阪・関西万博

日本国際博覧会協会が運用する交流サイト「X」の公式アカウント（左）と成りすましの偽アカウント（右）

２０２５年大阪・関西万博を運営する日本国際博覧会協会（万博協会）は２４日、交流サイト（ＳＮＳ）のX（旧ツイッター）で万博の公式アカウントに見せかけた不正なアカウントが見つかったと発表した。給付金の支給をほのめかすような投稿があり、万博協会は注意を呼びかけている。

●6月度フィッシング報告は144,160件、サイト数は最多更新

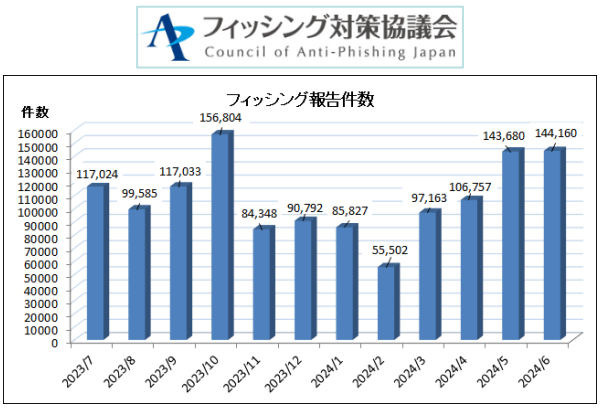
https://www.antiphishing.jp/report/monthly/202406.html

このニュースをザックリ言うと・・・

- 7月18日(日本時間)、フィッシング対策協議会より、6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。
- 6月度の報告件数は144,160件で、5月度(https://www.antiphishing.jp/report/monthly/202405.html)の143,680件から480件増加しています。
- フィッシングサイトのURL件数は54,991件で5月度(38,089件)から16,902件増加、悪用されたブランド件数は71件で5月度(91件)から20件減少となっています。
- 最も多く報告されたのはAmazonを騙るフィッシングですが報告数全体に対する割合は約26.3%と4月度(31.3%)から減少、次いで20,000件以上の報告を受けた三井住友カード、ヤマト運輸、10,000件以上の東京電力、イオンカードと合わせて約82.1%、さらに1,000件以上報告された11ブランドまで含めると約93.9%を占めたとのことです。

AUS便りからの所感

- 報告件数は先月度からの微増で高い水準を維持、サイトURL件数は2022年9月度の53,612件を抜いて最多件数を更新しています。
- フィッシングサイトURLで使用されるTLD(トップレベルドメイン名)の割合は上位から .com(約50.8%)、.cn(約24.0%)、.top(約6.0%)、.xyz(約5.8%)、.net(約4.8%)、.dev(約3.3%)となっており、.cnの増加が目立っています。
- 毎月の発表によれば、フィッシングメールの大量送信を行うIPアドレスにはDNS PTRレコード(IPアドレスからの逆引き)が設定されていないケースが多く(今月度は全体の約85.9%を占めているとのことです)、大手メールサービスでは既にこのようなアクセス元からのメールを受信しない設定となっているものもあるとされ、自組織のメールサーバーにおいても受信しない設定を採用することは、フィッシング・スパムメールの大幅な遮断に有用とみられます(ただし実際の取引先からのメールを誤って遮断しないよう、サーバー管理者において慎重に確認する必要はあるでしょう)。



●大手新聞社のニュースサイトでサポート詐欺広告が報告

https://togetter.com/li/2406746
https://www.yomiuri.co.jp/topics/20240719-SYT8T5591569/
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

このニュースをザックリ言うと・・・

- 7月11日(日本時間)頃より、読売新聞オンラインの閲覧時にサポート詐欺を行う不審な広告が表示されたとする報告がX(旧・Twitter)上で挙がっています。
- 報告されたサポート詐欺は「ファイアウォールの更新が必要」「お使いのシステムがトロジェン(原文ママ)またはスパイウェアに感染していると報告されました」といったポップアップが表示されるもので、「サイトを複数回開いたら表示された」「ページ上でボタン等のクリックを行わなくても表示された」ケースもあるとされています。
- 同19日には同サイトからも注意喚起が出され、マイクロソフトや消費者庁の注意喚起ページへのリンクが貼られています。

AUS便りからの所感

- 同サイトから出された注意喚起に対し、具体的に不審な広告に対応したといった宣言等がないことへの批判、また広告そのものを取り下げるべき等の指摘もなされています。
- ユーザー側においては、OS・Webブラウザー・アンチウイルス・UTMによるアンチフィッシング機能等を有効にして可能な限りサポート詐欺を行う不審なサイトへの誘導を抑制するとともに、それでも遭遇した場合の対策として、上記で挙げられているMS・消費者庁のページや、IPAが公開している特集ページを参考にし、ブラウザーの画面が強制的にフルスクリーン表示にされた場合は「ESCキーを一定時間押す」等の回避策を把握しておくことが有用でしょう。