令和3年1月12日

サイバーセキュリティ関連情報（1月号）

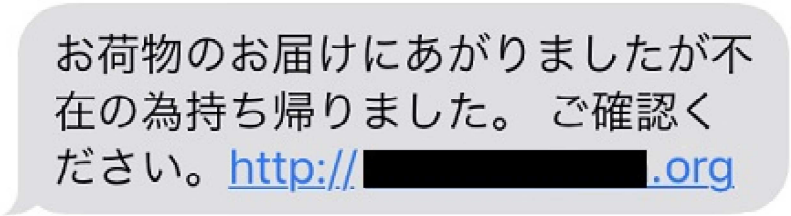
鳥取県警察本部サイバー犯罪対策課

○ ネットバンキング不正送金事案が県内で連続発生！

宅配便の不在通知を装い、金融機関のフィッシングサイトへ誘導するショートメッセージ（SMS）によるものと思われるネットバンキングの不正送金事案が年末年始にかけて、鳥取県内で2件連続発生しています。被害の金融機関は、いずれも「auじぶん銀行」であることから、サイバーセキュリティ関連情報（令和2年8月号）でご提供した手口と同一のものと認められます。フィッシングサイトは、「auじぶん銀行」以外にも「セブン銀行」「住信SBIネット銀行」「ジャパンネット銀行」などへ誘導される例も確認されていますが、次々と金融機関ブランドを変えて立ち上がっているため、今後も引き続き注意が必要です。また、誘導先で同様の不在通知を大量に送信させる不正アプリをダウンロードさせられるケースなども確認されており、こちらも注意が必要です。

不在通知を装うフィッシングによる被害は、コロナ禍におけるネット通販の利用増加に伴って全国で拡大しています。

フィッシング対策協議会のホームページには、フィッシングに関する緊急情報がいち早く掲載されることから、最新手口の動向を把握するためにも、ブックマーク登録の上、日々、ご確認をお願いします。



絶対にクリックしないで！ ↗　　参考：フィッシング対策協議会　https://www.antiphishing.jp/

○ 鳥取市のサイトに対するサイバー攻撃事案の発生！

鳥取市は、1月2日、市が運営する6次産業化マッチングサイト「ロクジカとっとり」が外部からサイバー攻撃を受けたと発表しました。鳥取市に対し、ロクジカとっとりのリンク先をクリックすると不審なサイトにつながるとの情報提供があり、確認したところ、外部からのハッキングによりサイトが書き換えられていることが判明しました。

情報漏えいはないとしているものの、現在、原因究明のためサイトを休止しており、今後、保守業者と協議の上、システム改修などの対応策を決めるとしています。

新型コロナウイルスの影響によるテレワークの普及に伴い、ウェブサイトの脆弱性や運用管理の不備を悪用した情報漏えいやウェブサイトの改ざん、企業情報を盗み出し、身代金を要求するランサムウェアによる被害など、セキュリティの隙を突いたサイバー攻撃は、全世界的に激化しており、今後も増える可能性があります。

ウェブサイトを安全に運営管理するためには、まず、セキュリティ対策の基本となるOSやサーバソフトウェア、ミドルウェアのバージョンを最新のものに更新して下さい。また、ウェブアプリケーションを構成している様々なソフトウェアやフレームワーク等も脆弱性が発見された場合、適宜バージョンアップ等の対策が必要となります。なかには、旧バージョンで作成されたウェブアプリケーションが最新バージョンでは動かなくなる互換性の問題から移行ができないというケースもあると思いますが、万が一脆弱性が悪用された場合の事業継続への影響や利用者に対する賠償責任など事後の対応に計り知れないコストが生じてしまうことを考慮した上、管理方法の検討をお願いします。

IPAでは、脆弱性対策として、「安全なウェブサイトの作り方」を公開しています。

詳細な資料のダウンロードができますので、ウェブサイトを運営されておられる方は、ご確認をお願いします。　　参考：IPA https://www.ipa.go.jp/security/vuln/websecurity.html