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。

●8月のフィッシング報告状況発表…不在通知を装うSMSを用いたフィッシングが多数確認される

https://securityblog.jp/news/20180910.html
http://www.antiphishing.jp/report/monthly/201808.html

このニュースをザックリ言うと・・・

- 9月3日（日本時間）、フィッシング対策協議会より、8月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 8月の報告件数は1874件で前月（1977件）より103件減少、フィッシングサイトのURL件数は954件で、こちらも前月（996件）より42件減少しています。

- この時期のトピックとして、7月末から8月初めにかけて、「不在通知を装いフィッシングや不正アプリのインストールを促すサイトへ誘導するSMS」の報告や相談が多数寄せられたこと等が挙げられています。

AUS便りからの所感等

- 月間報告件数は今年3月に1908件と倍近くに急増（前月836件）し、以降も概ね約1900件前後を維持しており、警戒するに越したことはないでしょう。

- 前述した以外のトピックとして、Softbank等のキャリア決済の不正利用を目的としたフィッシング、あるいはMUFGやセゾンといったクレジットカードやLINEをかたるフィッシング等が挙げられています。

- 出回っているフィッシングメール等の情報をフィッシング対策協議会のサイト等で収集すること、アンチウイルス・ブラウザあるいはUTMのセキュリティ機能でメール自体やフィッシングサイトへのアクセスを遮断すること、また利用しているサイトについてはブックマークからアクセスする等の各種防御策をとるようにしましょう。

日立ソリューションズ Information security blog 情報セキュリティブログ

8月は報告件数減少も、不在通知を装うSMSを用いたフィッシングが多数確認される

2018年9月10日

9月1日、フィッシング対策協議会は、2018年8月の月次報告書を公開した。

これによると、フィッシング報告件数は1,874件となり、前月(1,977件)より103件減少した。また、フィッシングサイトのURL件数は954件で、こちらも前月より42件減少している。そして、フィッシングに悪用されたブランド件数は32件で、前月から9件減少した。

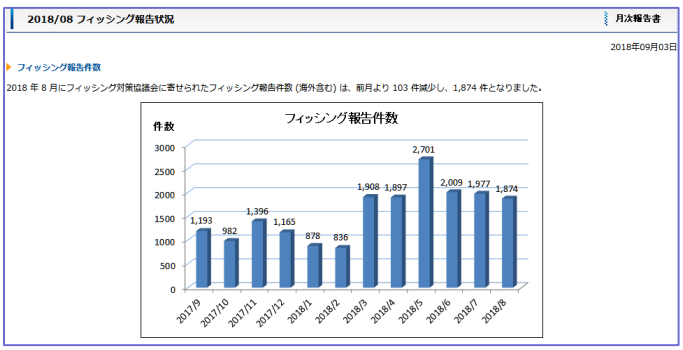
8月のフィッシング報告件数は7月と比較して103件の減少となったものの、7月末から8月はじめにかけてSMS(ショートメッセージサービス)を用い、不在通知を装ってフィッシングや不正アプリのインストールを促す手口に関する報
イルキャリア
ブランドをか
信されている

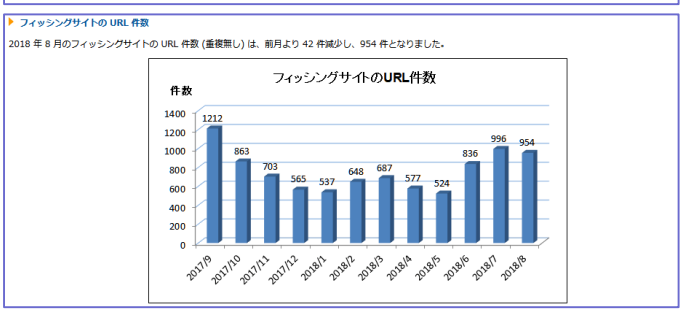
LINEをかたるフィッシングについては、8月中旬より、これまで稼働していた「cn ドメイン」以外のドメインでフィッシングサイトが確認され、引き続き注意が必要だという。

このほかにも、AppleやAmazonなど、多くの利用者を抱えるブランドをかたるフィッシングメールも非常に多くの種類が確認されており、同協議会では、フィッシングかどうかの判断に迷うメールや、不審なメールを受け取った場合は、各サービス事業者の問合せ窓口や同協議会まで連絡するよう呼びかけている。

・2018/08 フィッシング報告状況(フィッシング対策協議会)
・あなたのパスワードが狙われている！フィッシングの被害を防ぐための4つのポイント(今すぐ見直したいセキュリティ対策)
・「人の脆弱性」が悪用される！　メール等の安全な取扱いのポイントについて聞いてみた(辻 伸弘のセキュリティ防衛隊)

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





●Microsoft、Windows 7の法人向け有償延長サポートを2023年1月まで提供

https://japan.zdnet.com/article/35125227/

このニュースをザックリ言うと･･･

- 9月6日（米国時間）、Microsoftより、2020年1月14日に一般のサポート終了が予定されているWindows7について、法人向けに有償の延長サポート「Windows 7 Extended Security Updates(ESU)」を2023年1月まで提供することが発表されました。

- 対象はボリュームライセンス契約のWindows 7 ProfessionalとEnterpriseとなり、リテール版やDSP版は対象となりません。

- また課金はデバイス単位で行われ、料金は毎年引き上げられる予定とのことです。

AUS便りからの所感等

- ネット上では、安易に「お金を払えば2020年以降もWindows 7を使い続けられる」と取る声も多くありましたが、ボリュームライセンス契約に限定されること等から、中小企業においては7の延命とはならないと指摘する声もあります。

- また大企業であっても、台数が多いほど不利になる課金体系となっており、もし利用可能であったとしても、2020年までにWindows 10への移行を完了する場合の方を前提としつつ、それぞれのコスト等の比較検討を十分に行うべきでしょう。

- 全てのサポートが切れ、有償延長サポートも受けられない状態のOSは基本的に稼働させるべきではなく、どうしても必要であれば、せめてOS以外のアプリケーションを全て最新に保ち、アンチウイルスやUTMにより未修正の脆弱性を突かれる可能性を少しでも抑止することを心がけましょう。


ZDNet Japan

マイクロソフトが「Windows 7」の延長サポートを有償で提供へ

Mary Jo Foley（ZDNet.com） 翻訳校正：編集部 2018年09月07日 12時43分

米Microsoftは米国時間9月6日、「Windows 7」のサポートを有償で延長すると発表した。Windows 7のサポートは2020年1月14日に終了するが、この延長サービス「Windows 7 Extended Security Updates （ESU）」により、セキュリティアップデートを2023年1月まで受け取ることができる。

Windows市場全体で、Windows 7が占める割合は依然として高く、特に企業ユーザーが多い。事前に計画を立てていても、何千台ものデスクトップでWindowsを利用している企業にとって、旧版からの移行は時間のかかるプロセスだ。

有償のESUはデバイス単位で課金され、料金は毎年引き上げられる。ボリュームライセンス契約をする「Windows 7 Professional」と「Windows 7 Enterprise」の全ユーザーが対象で、「Windows Software Assurance」もしくは「Windows 10 Enterprise」、「Windows 10 Education」の利用者には割引が適用される。ESUを利用しているデバイスなら、「Office 365 ProPlus」は2023年1月までサポートされる。

●ドコモの「dポイント」で不正利用…約35,000件を利用停止

https://www.nikkei.com/article/DGXMZO35304710T10C18A9000000/

このニュースをザックリ言うと･･･

- 9月12日（日本時間）、NTTドコモより、同社が提供する「dポイント」の不正利用の被害が大量に発覚したことを受け、同10日に約35,000件のdポイントカード番号を利用停止したことが発表されました。

- 不正利用は8月25日以降に相次いで発生しており、あるdポイント加盟店のWebサイトが不正アクセスを受けて「dポイントカード番号」が流出したことが原因とされ、これまでに約300件の申告があったとのことです。

- 利用停止したユーザに対してはdポイントカードの再発行等、利用再開時に必要な手続きを案内しているとのことです。

AUS便りからの所感等

- 前述のとおり、加盟店サイトの不正アクセスで流出したのは「dポイントカード番号」のみであり、それだけで不正利用が可能であったこと、またカードに記載されているバーコードについても、番号から生成しカードを偽造することも可能であったという指摘もなされています。

- 現状での防衛策としては「dポイント番号を他人に知られないようにする」ぐらいかといったところのようです。

- 今後、dポイントおよびdポイントカードの不正利用を防止するためにどういった対策がなされるかが注目されます。


日本経済新聞

ドコモ「dポイント」で不正利用　悪用の容易さ指摘

科学&新技術 ＢＰ速報

2018/9/13 18:00

日経 XTECH

NTTドコモは2018年9月12日、共通ポイントサービス「dポイント」で不正利用が発生していたことを明らかにした。8月25日以降、相次ぎ発生し、これまで約300件の申告があった。被害の拡大を防ぐため、9月10日に約3万5000件のdポイントカード番号の利用停止措置を実施した。

同社によると、あるdポイント加盟店のウェブサイトが不正アクセスを受け、dポイントカード番号とポイント残高を盗み見られたという。ここで漏れたdポイントカード番号で被害が発生しており、同サイトに登録があったアカウントカード番号（約3万5000件）の利用停止措置を実施した。

NTTドコモはこの点について、「バーコード方式のリスクについては理解している。ただ、バーコード方式が直ちに不正利用を起こすかと言えば別と考えている。dアカウントのアプリでもdポイントカード番号を非表示にしており、今回の件は多くのdポイントカード番号が簡単に盗み見られたことが原因と考えている。セキュリティー対策を日々強化していくのはもちろんで、将来にわたってどうしていくかまで一概に言えないが、今回の件については既に対策した」（広報部）としている。

とはいえ、dポイントカード番号が悪意のある第三者に渡れば簡単に悪用される危険性は残り、ユーザーは自衛が必要と言えそうだ。NTTドコモによると、dポイントを加盟店で使うと、デフォルトでその旨が「メッセージR」で本人に通知されるという。今回の不正利用も、同機能で身に覚えのない「メッセージR」を受信したユーザーからの申告で判明した。ポイントの定期的なチェックはもちろん、受信した「メッセージR」は必ず確認するようにしたい。