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。

●LINEでの新型コロナ調査を騙りクレジットカード番号を聞く詐欺…厚労省が注意喚起

https://www.itmedia.co.jp/news/articles/2004/01/news082.html
https://www.mhlw.go.jp/stf/newpage_10635.html
https://guide.line.me/ja/coronavirus-survey.html

このニュースをザックリ言うと･･･

- 3月31日(日本時間)、厚生労働省より、同省がLINEとの協力で実施している「新型コロナ対策のための全国調査」を騙る詐欺が確認されたとして注意喚起が出されています。

- LINEでは厚労省と協定締結により、国内ユーザー約8,300万人に対し体調や実施している感染予防策等を質問するアンケート調査を31日に行っていますが、これを装って電話番号やクレジットカード番号等を尋ねる偽の調査の情報が同省に寄せられているとのことです。

- 同省は本物のアンケートでの質問内容を示し、LINEからも緑の公式バッジが付いている公式アカウントか確認するよう注意喚起が出されています。

AUS便りからの所感等

- 4月1日までに実施された第1回調査では約2,454万人の回答を得たと発表され(https://www.itmedia.co.jp/news/articles/2004/03/news147.html)、5日～6日に実施されている第2回調査でも同様に便乗する詐欺、さらにはショートメール(SMS)でも拡散されることは十分に考えられます。

- このようなフィッシング詐欺に共通する回避策は、不審なメール等を受け取ったら安易にリンクをクリックすることなく、公式からの発表・注意喚起やSNS等での報告にあたること、登録している各サービスについて正規のURLを予めブックマークに登録してそこからアクセスすること、PC・モバイルいずれにおいてもアンチウイルスソフトを導入し、ブラウザーおよびUTM含めアンチフィッシング機能を有効にすることです。

厚生労働省
Ministry of Health, Labour and Welfare

【注意喚起】新型コロナウイルス感染症のクラスター対策に資する情報提供に関する取組を装った詐欺にご注意ください～調査を装ってクレジットカード番号等を尋ねるものは詐欺です！～

厚生労働省においては、新型コロナウイルス感染症のクラスター対策に資する情報をご提供いただける民間事業者等と情報提供に関する協定を締結し、新型コロナウイルス感染症のクラスター対策の強化を図るため、3月27日に広く民間事業所等に呼びかけを行い（参考１）、ご趣旨に賛同いただいたLINE株式会社と「新型コロナウイルス感染症のクラスター対策に資する情報提供に関する協定」を締結したところです（参考２）。

現在、LINE株式会社において、サービス登録者に対して健康状態に関するアンケートを実施しているとの情報を得ていますが、このアンケートを装い、クレジットカード番号等を尋ねる等詐欺が疑われる事案が発生しているとの情報が寄せられています。

LINE

【公式アカウントの確認方法】

「LINE」の左に緑の公式バッジがついているものが公式アカウントです。偽物のアカウントにご注意ください。

●ビデオ会議ツール「Zoom」に脆弱性相次いで報告

https://gigazine.net/news/20200402-zoom-should-not-use/
https://gigazine.net/news/20200403-zoom-password-windows-credentials-problems/
https://pc.watch.impress.co.jp/docs/news/1244583.html

このニュースをザックリ言うと・・・

- 3月末以降、オンラインビデオ会議ツール「Zoom」において、脆弱性やプライバシー上の問題が相次いで指摘されています。
- 3月31日(現地時間)、PC情報サイトの米Bleeping Computerより、ZoomのWindows版クライアントに脆弱性が存在し、チャットテキスト中等のUNC(¥¥コンピューター名¥共有名¥パス)がハイパーリンクに変換され、これをクリックすることにより、Windowsアカウントの認証情報が漏洩する可能性があると報じられました(翌4月1日にアップデートがリリースされています)。
- また、会議のIDが9～11桁のランダムな数字で識別されること、かつ当初デフォルトの設定によりパスワードがかかっていないビデオ会議があったことにより、第三者が会議に侵入し、不正なメッセージや画像を送り込む攻撃が昨年以降発生していました(一旦対策は行われたものの、依然これを回避して会議を探索する等の攻撃が行われている模様です)。
- この他にも、「通信の暗号化がエンドツーエンド(クライアント間)ではなくサーバー側で行われていた」「macOS版において不正な方法でアプリケーションをインストールする」等が指摘されており、「最終的にZoomは使うべきではない」と主張するメディアもあるとのことです。

AUS便りからの所感

- ZoomはMicrosoftのSkypeやTeamsと同様のビデオ会議サービスとして、特にテレワークの導入が叫ばれている昨今に注目を集めています。
- 挙げられている問題は利用者側では対応できないものもあり、それらについてのリスクを許容するか否かで利用を判断し、必要に応じサービスを乗り換えられる体制を可能な限り整えた上で、最低でもアプリケーションを最新のバージョンにアップデートし、確実にパスワードを設定する等を心がけることが重要です。
- Zoom側では指摘された問題のいくつかに対し迅速に対応している模様ですが、今後の各種対応を経て、セキュリティ専門家等による安全性の評価がどこまでなされるかに注目したいところです。


GIGAZINE
2020年04月03日 12時06分　セキュリティ
問題続出のオンラインビデオ会議ツール「Zoom」が抱える「パスワード問題」と「OSの資格情報を盗まれる脆弱性」が新たに指摘される
セキュリティおよびプライバシー面で多くの問題が指摘されているオンラインビデオ会議ツールの「Zoom」で、新たに「Zoomを利用している大手企業の多くがパスワードを設定しないままオンラインビデオ会議を行っている」ことが明らかになりました。

●米ホテル大手アプリ利用者520万人の個人情報に従業員が不正アクセスか

https://www.itmedia.co.jp/news/articles/2004/01/news104.html

このニュースをザックリ言うと・・・

- 3月31日(現地時間)、米ホテル大手のMarriott Internationalより、同社宿泊客520万人以上の個人情報が不正アクセスを受けた可能性があると発表されました。
- 被害を受けた個人情報は、同社アプリを利用した宿泊客の住所・氏名・電話番号・メールアドレス・性別・誕生日等となっています。
- 系列ホテルの従業員2名が1月中旬以降に不正アクセスを行っていた可能性があることが2月末に発覚したものとされています。

AUS便りからの所感

- 同ホテルでは2018年にも外部からとみられる不正アクセスにより、最大3億8,300万人分の個人情報が流出したとされています(https://www.itmedia.co.jp/news/articles/1812/04/news070.html)。
- 今回被害を受けた個人情報には、職場あるいはリンクされた航空会社のロイヤリティプログラムのデータ・登録した部屋の好み・使用言語等といったセンシティブなものも含まれていました(入力必須ではない項目含む)。
- 末端のホテル従業員がこれだけ広範囲な宿泊客データにアクセスできる権限を得られた経緯はまだ不明のようですが、こういったデータを一元管理する必要がなければ、データベースを分散管理とし、全てにアクセスできるような強い権限を最初から用意しない等も情報保護のために有用かと思われます。


ITmedia NEWS
Marriott Internationalでまた顧客情報に不正アクセス　520万人に影響の可能性
2020年04月01日 14時37分 公開　[ITmedia]
印刷　見る　Share　B! 6
ホテル大手の米Marriott Internationalは3月31日（現地時間）、同社のアプリを利用した520万人以上の宿泊客の個人情報に影響を与えた可能性のある事件について説明した。
Marriott INTERNATIONAL　News Center
Marriott International Notifies Guests of Property System Incident
MARCH 31, 2020 — BETHESDA, MD