— AUS（アルテミス・ユーザ・サポート）便り 2016/11/14号 —
http://www.artemis-jp.com

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。

●amazon.co.jpをかたるフィッシングメールに注意･･･「アカウント検証」を装う

http://www.itmedia.co.jp/enterprise/articles/1611/08/news093.html
http://www.antiphishing.jp/news/alert/amazon_20161108.html

このニュースをザックリ言うと･･･

- 11月8日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、amazon.co.jpをかたる新たなフィッシングメールが確認されたとして、警告が出されています。

- メールは「アカウント検証」という件名で、本文に偽のログイン画面へのリンクが示されており、メールアドレス・パスワードを入力すると、さらに住所とクレジットカード情報（セキュリティコードまでを含む）の入力を要求するフォームが表示されるとのことです。

AUS便りからの所感等

- 今回のフィッシングメールおよび偽サイトには、現在のところ不自然な日本語のメッセージが書かれていますが、本物のサイトを参考にする等により、より自然な日本語のメッセージに修正されたフィッシングが発生することは当然考えられます。

- 大手サイトや金融機関をかたるフィッシングはもはや珍しいものではなく、amazon.co.jpでは受け取ったメールが本物か確認するためのポイントをまとめています（https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201304810）。

- この他の自衛策として当便りでは、メールに記載されたリンクを安易にクリックしないことはもちろん、ブラウザのブックマークから正規のサイトへアクセスすることや、ブラウザ・アンチウイルスソフトあるいはUTM等のアンチスパムやアンチフィッシング機能を活用することを度々推奨しております。

ITmedia エンタープライズ

2016年11月08日 12時44分 更新

Amazonの偽メールに注意、「アカウント検証」を装う

メールから誘導されるフィッシングサイトではクレジットカード情報の入力も求めてくる。

[ITmedia]

印刷／PDF　215 ツイート　324 いいね！　324 シェア　12 Bookmark　29 Pocket　8 G+1　共有する　通知

フィッシング対策協議会は11月8日、Amazonを名乗る偽メールへの注意を呼び掛けた。件名には「アカウント検証」とあり、フィッシングサイトに誘導される恐れがある。

偽メールは不自然な日本語文書が記載され、「下記のホームページアドレスをクリックするだけ」という文言と、「今すぐ確認します」と書かれたボタンが表示される。このボタンをクリックしてしまうと、フィッシングサイトに接続してしまう。

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

amazon　アカウント 検証

親愛な【受信者のメールアドレス】，

あなたのアカウントにいくつかの情報がなかったり、間違っていたり、アマゾン アカウントのすべての利点を享受し続けることができますので、あなたのアカウント情報を速やかに更新してください。。

24 時間以内にあなたの情報を更新しない場合、アマゾン アカウントで何ができるか約を終ってください。。

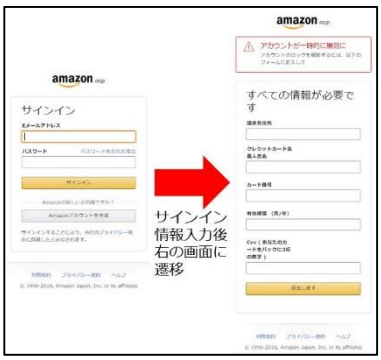
下記のホームページ アドレスをクリックするだけ：

今すぐ確認します。

あなたの関心事をありがとう。

心から、

Amazon.co.jp
https://www.amazon.co.jp/



amazon.co.jp プライム

セキュリティ&プライバシー › 規約 ›

Amazon.co.jp からのEメールかどうかの識別について

Amazon.co.jp を装った詐欺メール（フィッシングメール）を受け取った際、Eメールが本当にAmazon.co.jp から送られたものかどうかを識別するための方法がいくつかあります。

重要:
偽装の疑いのあるEメール内の添付ファイルやリンクを開かないでください。もし添付ファイルやリンクを開いてしまった場合は、コンピューターを保護するをご覧ください。

フィッシングメールである場合、Eメール内に以下のものが含まれている傾向があります。

- 注文していない商品の注文確認をする内容

  注: アカウントサービスの注文履歴で、Eメールに記載されている注文の情報がサイト上に表示される注文詳細と合致しているかを確認してください。合致していない場合、そのEメールはAmazon.co.jp から送られたものではありません。

- Amazon.co.jp のアカウントにご登録のお名前やパスワード、その他個人情報を求める内容
- お支払い情報の更新を求める内容

  注: アカウントサービスの**クレジットカード情報の編集・削除**内にある**支払い方法欄**にアクセスしても、支払い方法の更新の指示が出ていない場合、そのEメールはAmazon.co.jp から送られたものではありません。

- Amazon.co.jp のWebサイトではないサイトへのリンク。「http://××.amazon.co.jp」または「https://××.amazon.co.jp」で始まらないWebサイト
- 添付ファイルやソフトウェアのインストールを求める内容
- 誤字や文法の間違い
- 送信元が、Amazon.co.jp やAmazon.com を装ったEメールアドレス

  注: ‘送信元’ のEメールアドレスに、以下のドメインリストに掲載されていないインターネットサービスプロバイダが含まれている場合は、偽装メールです。

Amazon.co.jp で使用しているドメイン

Amazon.co.jp は以下のドメインを使用してEメールをお送りしています。

- amazon.co.jp
- amazon.jp
- amazon.com
- marketplace.amazon.co.jp
- m.marketplace.amazon.co.jp
- gc.email.amazon.co.jp
- gc.amazon.co.jp
- payments.amazon.co.jp

●Wi-Fiストレージに脆弱性、メーカー一時販売停止

http://itpro.nikkeibp.co.jp/atcl/news/16/110203247/

このニュースをザックリ言うと・・・

- 11月2日（日本時間）、パソコン周辺機器大手のアイ・オー・データ機器より、同社製品の一部機能に脆弱性が存在し、DDoS攻撃等に悪用される可能性があると発表されました。

- 対象となる製品は、スマホ等からのデータ保存・SDメモリカードリーダー・Wi-Fiルータ等の機能を持つ小型Wi-Fiストレージ「ポケドラ(WFS-SR01)」で、ルータ機能に存在する脆弱性を外部から悪用することにより、機器上で任意のコマンドを実行されたり、挿入されたSDカード等にアクセスされる可能性があるとされています。

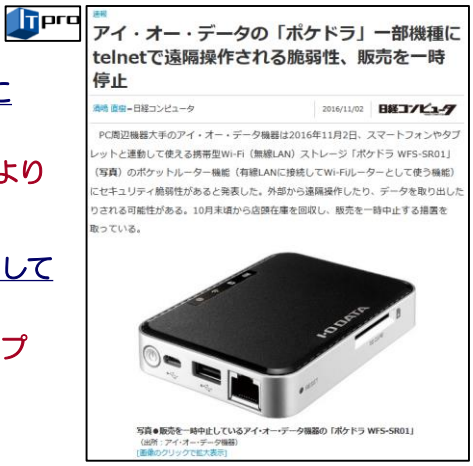
- 同社では、10月末頃から当該機器の一時販売停止・店頭在庫回収等の処置をとっており、ファームウェアのアップデートが行われるまで、回避策としてルータ機能を無効にするよう呼び掛けています。

AUS便りからの所感等

- 同社の説明によれば、当該機器のtelnetサービス（TCPポート23番）に簡単なパスワードでアクセス可能な状態であるとのことです。

- 先月にも、このようなtelnetサービスから機器に侵入するマルウェアによりDDoS攻撃が発生したばかりであることを踏まえ（「AUS便り 2016/10/31号」参照）、PCやスマホだけではない、ネットワークにつながる様々な機器が不正アクセスやマルウェア感染、そして攻撃の踏み台にされる可能性があるものと注意する必要があります。

- WindowsのOSやアプリと異なり、このような機器のセキュリティアップデートはなかなか意識されない傾向にありますが、自分が利用しているあらゆる機器の存在を把握したうえで、随時メーカーサイトやニュースを確認し、速やかに適切な対策をとれる体制を整えるのが良いでしょう。



●レンタルサーバ業者が不正アクセス被害、約5万人の個人情報流出

http://www.itmedia.co.jp/news/articles/1611/10/news096.html

このニュースをザックリ言うと・・・

- 11月9日（日本時間）、レンタルサーバサービスを提供するカゴヤ・ジャパン社より、同社サーバが不正アクセスを受け、同社ユーザの個人情報が流出した可能性があると発表されました。

- 対象となるのは9月21日まで同社サービスを利用していた全ユーザ（解約済みユーザも含む）48,685人分の氏名・住所・電話番号・メールアドレス・アカウントIDとパスワードの他、クレジットカード情報20,809件が含まれていたとのことです。

- 9月16日に同社の複数の顧客サーバに不正プログラムがインストールされていたことが発覚しており、そこからデータベースサーバに存在した「OSコマンドインジェクション」の脆弱性を突いて侵入した形跡が確認された模様で、同社では対象ユーザのパスワードを変更する等の対策をとっています。

AUS便りからの所感等

- 攻撃者はユーザが利用する外部に公開されたサーバを踏み台にしてデータベースサーバにアクセスしたとみられており、ネットワーク構成の詳細は不明ですが、このような事態を防ぐ策としては、個人情報を収納しているサーバ等のある会社のネットワークについて、レンタルサーバのネットワークや、サーバの保守を行う管理者がサーバにアクセスする際のネットワークからアクセスできないよう、UTM等を活用して隔離することが考えられます。

- 事件を受けて、同社では不正アクセスされたカード情報を削除し、決済業務をPCIDSSに準拠する決済代行会社に委託しているとのことです。

- クレジットカードを取り扱う事業者は2018年3月末までに自社でPCIDSSに準拠するか、カード情報を自前で保持しないシステムにすることが要求されており（「AUS便り 2016/10/11号」参照）、カード情報に限らず、余分な情報を持たないことは万が一の流出時のリスクを抑えるためにも重要なことです。