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。

●「エリアメール」かたる詐欺メールに注意喚起

https://abematimes.com/posts/5081873
http://news.livedoor.com/article/detail/15497850/

このニュースをザックリ言うと・・・

- 10月25日（日本時間）頃、強い地震や災害が予測される時に送信される「エリアメール」をかたる不審なSMSが確認されたとしてTwitter上で投稿があり、AbemaTVのニュース番組等でも取り上げられています。

- 詐欺メールの一例として挙げられているものは、「緊急地震速報『エリアメール』強い揺れに備えてください。各地の震度はこちらからご覧ください」という文面とともに、アダルトサイトや出会い系サイトへのリンクが貼られているものとなっています。

- ニュース番組では、こういった緊急地震速報がSMSで送られることはないとし、本来の緊急地震速報におけるポイントとして「緊急音が必ず鳴る」「返信できない」「URLが貼り付けられていることはない」の3つを挙げ、注意を呼び掛けています。

AUS便りからの所感等

- SMSを悪用した詐欺は通常の電子メールと同様に枚挙にいとまがありません。

- 例えば、7月には宅配便の不在通知をかたり不正なアプリをインストールさせようとするケースが確認されています。

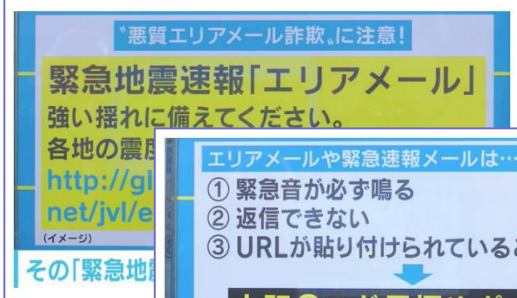
- 一方でエリアメール以外にも、自治体や大手ネットサービスが防災情報等を通常のメールで送信する場合があり、それらをかたる詐欺メールが拡散する可能性も十分に考えられます。

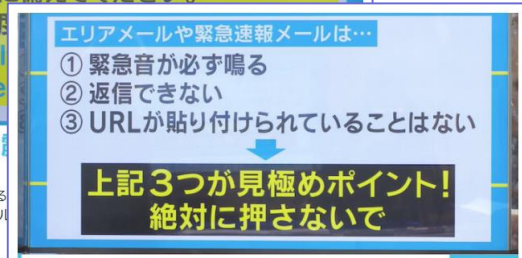
- 利用しているサービスの公式ページにおいて注意喚起が出されていれば事前に確認し、不審な文面の場合はネット上で検索して裏をとる等、可能な限り慎重は行動をとるよう心がけましょう。

AbemaTIMES

「緊急地震速報」謳う詐欺メールに注意、見極める3つのポイント

2018.10.26 19:18





その「緊急地震速報」詐欺かもしれません Abema news/

強い地震が予測される
れを悪用した"詐欺メール

その内容は、「緊急地
の震度はこちらからご覧
メールが送られてきたと
系サイトなどにつながっ

不安感を煽られついURLをタップしてしまいそうだが、そもそもショートメールで緊急地震速報が送られてくることはない。ただ、文章が巧妙に作られていることから注意が必要で、本来の緊急地震速報は「緊急音が必ず鳴る」「返信できない」「URLが貼り付けられていることはない」という3点を頭に入れ、URLを絶対に押さないようにすることが大切だ。

（AbemaTV／『けやきヒルズ』より）

livedoor NEWS

災害のエリアメールを騙った悪質な迷惑メールに注意！

2018年10月25日 17時48分　おたくま経済新聞

強い地震や大規模災害が予測される時に発信される、「エリアメール/緊急速報メール」。このメールは気象庁や各省庁、地方公共団体などの発表にもとづき被災の恐れのあるエリアに一斉配信
た詐欺が発生しており、

【さらに詳しい元の記事

このメールを受信し、
208"さん。

「迷惑メールもここま
受信画面をツイッター
タイトルは【緊急地震速
ださい。各地の震度はこ
字の羅列が入ったURLが

■ エリアメールは緊急音が必ず鳴る

どの携帯キャリアでも、緊急地震速報などが発令されたら、その該当地域に在住の人が持つ携帯やスマホに、共通の専用緊急音と共に画面上にポップアップで情報が表示されます。しかし、エリアメールを騙った詐欺ではその緊急音まで鳴らす事はできません。したがって、この手のショートメールが届いた場合にはまず詐欺だと思って間違いはないかと思います。

●鋼板加工機器がウイルスに感染、2年間不審なDNSクエリ…開発中に感染か

https://japan.zdnet.com/article/35127649/

このニュースをザックリ言うと・・・

- 10月26日（日本時間）、IPA等を中心にサイバー攻撃に関する情報共有の実運用を行っているサイバー情報共有イニシアティブ（J-CSIP）より、2018年7～9月期の活動状況が発表されました。

- 上記四半期におけるサイバー攻撃等の情報提供は519件で、うち75%は8月上旬に発生した「.iqyファイル」が添付された日本語のばらまきメールによるものとされています。

- またレポートにおけるトピックとして、鋼板加工機器でのウイルス感染事例等が挙げられており、制御用コンピューターのOSに使用されていたWindows Embeddedにマルウェアが感染し、機器が設置された2016年以降2年近く外部に不審なDNSクエリを送信していたとされています。

AUS便りからの所感等


ZDNet Japan

鋼板加工機器がウイルスに感染、2年間不審なDNSクエリ--開発中に感染か

ZDNet Japan Staff 2018年10月26日 15時40分

いいね！ 81 G+ B! 16 Pocket 46

印刷 メール ダウンロード クリップ

情報処理推進機構（IPA）や国内企業、業界団体らで構成するサイバー情報共有イニシアティブ（J-CSIP）は10月26日、2018年7～9月期の活動状況を発表した。鋼板加工機器でのウイルス感染事例などを紹介している。

それによると、期間中にはサイバー攻撃など519件の情報提供があり、うち30件が標的型攻撃メールを見られるものだった。全体の約75%は、「IQY」形式のファイルを添付する不特定多数を狙った日本語の攻撃メールだったが、IPAでは初めて日本語による「ビジネスメール詐欺（BEC）」を確認している。また、参加組織から産業用機器へのウイルス感染事例の情報提供もあった。

- 今年8月に導入したIDSで不審なDNSクエリの送信が検知され、その後機器のメーカーから、機器の開発期間中にマルウェアが混入した可能性が高いと報告があったとのことです。

- こういった開発環境でのマルウェア感染の結果、ソフトウェアのインストーラーにもマルウェアが混入したという事件も以前発生しています。

- マルウェアは制御システムや産業用機器を狙ったものではなかったとされ、また当該機器から社外ホストの名前解決およびサーバへのアクセスを不可とする運用にしていたため、実質的な被害は発生していなかったとしていますが、万が一、機器がマルウェアに感染したとしても、そこからの感染拡大を食い止めるための「出口対策」が行えるようなネットワークをIDSやIPSを駆使して構成することが重要と言えます。

●3,294件のメールアドレス流出…兵庫県立図書館が誤送信

https://cybersecurity-jp.com/news/27919

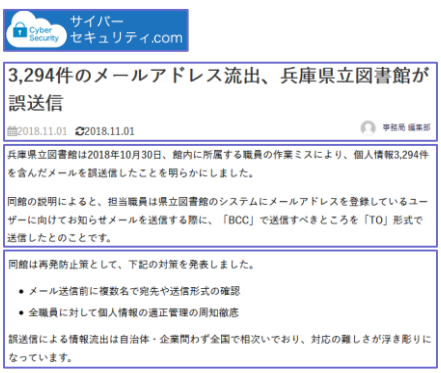
このニュースをザックリ言うと・・・

- 10月30日（日本時間）、兵庫県立図書館より、お知らせメールの送信時に誤ってメールアドレス3,294件が外部に流出したと発表されました。

- 発表によれば、メールアドレスを登録したユーザに対し同26日にお知らせメールを送信した際、送信先をBcc:（送信されたメールには表示されない）に入力すべきところを、誤ってTo: に入力して送信したことが原因としています。

- メールアドレス以外に個人情報が特定し得る情報は含んでいないとしており、同26日にはお詫びとメール削除のお願いを送信したとのことです。

AUS便りからの所感等


サイバーセキュリティ.com

3,294件のメールアドレス流出、兵庫県立図書館が誤送信

2018.11.01 2018.11.01 事務局 編集部

兵庫県立図書館は2018年10月30日、館内に所属する職員の作業ミスにより、個人情報3,294件を含んだメールを誤送信したことを明らかにしました。

同館の説明によると、担当職員は県立図書館のシステムにメールアドレスを登録しているユーザーに向けてお知らせメールを送信する際に、「BCC」で送信すべきところを「TO」形式で送信したとのことです。

同館は再発防止策として、下記の対策を発表しました。

- メール送信前に複数名で宛先や送信形式の確認
- 全職員に対して個人情報の適正管理の周知徹底

誤送信による情報流出は自治体・企業問わず全国で相次いでおり、対応の難しさが浮き彫りになっています。

- 3,000件以上という大量のメールアドレスをメーラーに手動で入力するという方法は、今回のようにミスが発生する可能性が少なからず存在し、かつその場合の被害も大きいものとなります。

- 発表では、今後このようなメール送信の際は複数名で入力内容のチェックを行う等の対策をとるとしていますが、それだけでは再発を根本的に防止するのは簡単ではないでしょう。

- このように単純な方法で潜在的リスクの高い運用を行うよりは、メーリングリスト等、同報メール送信のためのシステムの導入を強く推奨致します。

- また、To: やCc: に不自然に大量のメールアドレスが含まれているメールは同様の失敗をしている可能性があるため、メールサーバやUTMにおいてメールチェックによる送信を拒否する機能があるならば、それを有効にすることも検討に値するでしょう。