— AUS（アルテミス・ユーザ・サポート）便り 2016/03/14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。

●ビックカメラドットコムで不正アクセス、他サイトのアカウント情報流用か

http://www.sankei.com/affairs/news/160304/afr1603040037-n1.html
http://news.mynavi.jp/news/2016/03/04/614/

このニュースをザックリ言うと･･･

- 3月3日（日本時間）、大手量販店のビックカメラは、同社のショッピングサイト「ビックカメラドットコム」が不正アクセスを受け、利用者数十人のポイント約100万円分が利用される被害が発生したと発表しました。

- 発表によると、同サイトからアカウント情報が流出したものではなく、他のサイトで奪取されたアカウント情報が利用されたものとしており、ポイントの不正利用については、ポイントカードのほか、スマートフォンアプリでログインしたユーザ用のバーコードを表示することも可能であることから、不正ログインしたアカウントのものとなるバーコードを提示した可能性もあるとしています。

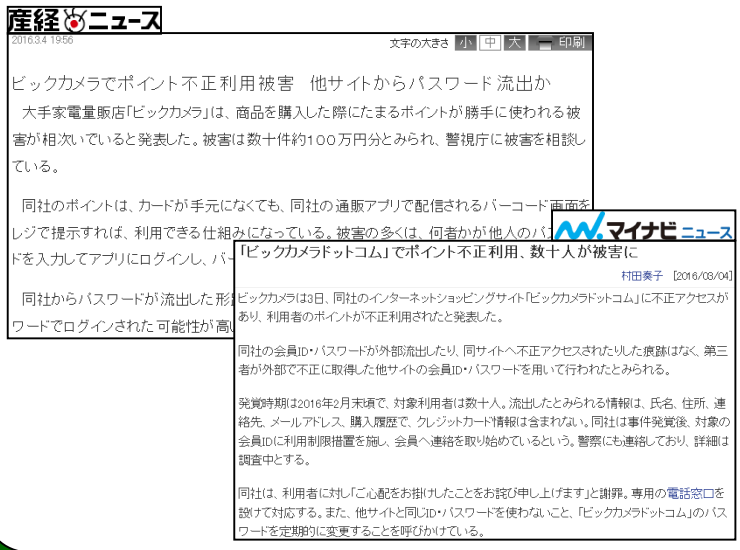
- ビックカメラでは、不正ログインされたユーザの一部の個人情報（氏名、住所、連絡先、メールアドレス、購入履歴）が閲覧された可能性はあるものの、クレジットカード情報は含まれていないとしており、ユーザに対し「他のWebサイト等と同一の会員ID・パスワードを使用しないこと」「ビックカメラドットコムのパスワードを定期的に変更すること」を呼びかけています。

AUS便りからの所感等

- あるサイトで奪取されたアカウント情報が他のサイトでも悪用され、同じID・パスワードを使用しているアカウントが芋づる式に不正ログインの被害を受けるケースは、2014年以降著名なサイトも巻き込んでしばしば大きく取り上げられています。

- パスワードの扱いにあたっては、攻撃者が既に取得したパスワードあるいはよく利用される簡単なパスワードではない、破られにくいものであることも重要ですので、当便り2015/12/28発行号での「セキュアなパスワードの作り方とは？」を参考に、複雑なパスワードの設定、時にはツールを用いることも含めた適切な管理の検討を推奨します。

- 自組織のメールサーバ等への不正ログインにより、アカウント情報が奪取されて悪用される可能性もありますので、攻撃者の不正ログイン試行を遮断できるよう、可能であればUTMを活用することも重要です。


産経ニュース
2016.3.4 19:56
文字の大きさ 小 中 大 印刷
ビックカメラでポイント不正利用被害　他サイトからパスワード流出か
大手家電量販店「ビックカメラ」は、商品を購入した際にたまるポイントが勝手に使われる被害が相次いでいると発表した。被害は数十件約100万円分とみられ、警視庁に被害を相談している。
同社のポイントは、カードが手元になくても、同社の通販アプリで配信されるバーコード画面をレジで提示すれば、利用できる仕組みになっている。被害の多くは、何者かが他人のパ
ドを入力してアプリにログインし、パ
同社からパスワードが流出した形
ワードでログインされた可能性が高

マイナビニュース
「ビックカメラドットコム」でポイント不正利用、数十人が被害に
村田奏子　[2016/03/04]
ビックカメラは3日、同社のインターネットショッピングサイト「ビックカメラドットコム」に不正アクセスがあり、利用者のポイントが不正利用されたと発表した。
同社の会員ID・パスワードが外部流出したり、同サイトへ不正アクセスされたりした痕跡はなく、第三者が外部で不正に取得した他サイトの会員ID・パスワードを用いて行われたとみられる。
発覚時期は2016年2月末頃で、対象利用者は数十人。流出したとみられる情報は、氏名、住所、連絡先、メールアドレス、購入履歴で、クレジットカード情報は含まれない。同社は事件発覚後、対象の会員IDに利用制限措置を施し、会員へ連絡を取り始めているという。警察にも連絡しており、詳細は調査中とする。
同社は、利用者に対し「ご心配をお掛けしたことをお詫び申し上げます」と謝罪。専用の電話窓口を設けて対応する。また、他サイトと同じID・パスワードを使わないこと、「ビックカメラドットコム」のパスワードを定期的に変更することを呼びかけている。

ビックカメラによる告知文


ビックカメラ.COM
平成28年3月3日
各位
株式会社ビックカメラ
当社インターネットショッピングサイトでの会員ＩＤ，パスワード不正使用被害について
この度、第三者によって外部で不正に取得されたと思われる他サイトの会員ＩＤ・パスワードを用いて、何者かが当社インターネットショッピングサイト「ビックカメラドットコム」に不正アクセスし、ポイントを不正に利用された事実が発覚いたしました。
不正アクセスされたと思われるお客様の会員ＩＤは、事実発覚後に利用制限措置を講じております。対象のお客様には、すでに連絡を取り始めております。
本件の詳しい事実関係は現在調査中です。既に警察等の関係行政機関には届出をし、捜査に全面的に協力をしております。
お客様にはご心配をおかけすることになりましたことをお詫び申し上げます。
お客様におかれましては、会員ＩＤ・パスワードの管理の重要性をご理解頂り、次のことを実施して下さいますようお願い申し上げます。
①他のＷｅｂサイト等と同一の会員ＩＤ・パスワードを使用しない事。
②ビックカメラドットコムのパスワードを定期的に変更する事。
※今回の不正アクセス時に用いられたＩＤ・パスワードは、第三者によって外部で不正に取得されたと思われるものであり、当社内からの外部流出や、ビックカメラドットコムへの不正アクセスによって取得された痕跡は発見されておりません。
※本件の対象となる一部のお客様の情報（氏名、住所、連絡先、メールアドレス、購入履歴）が第三者に閲覧された可能性がございますが、当該情報にクレジットカード情報は含まれておりません。
以　上
【本件のお問い合わせ先　ビックカメラドットコム】
専用フリーダイヤル　０１２０－３７２－６６６（９：３０～１９：００）

●2015年のネット不正送金被害は過去最悪の30億7300万円・・・被害口座の7割が対策未実施

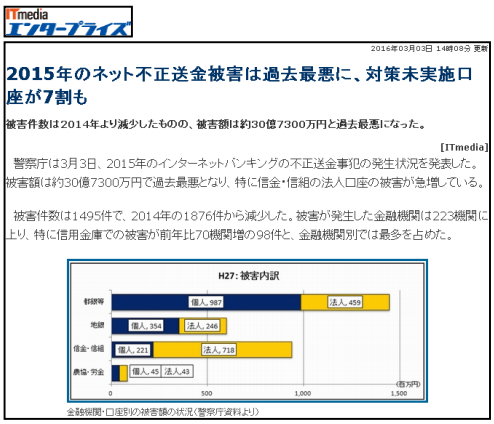
http://www.itmedia.co.jp/enterprise/articles/1603/03/news097.html

このニュースをザックリ言うと・・・

- 3月3日（日本時間）、警察庁より、2015年中のインターネットバンキングに係る不正送金事犯の発生状況等について発表がありました。

- 発生件数は1,495件と2014年の1,876件より381件減少していますが、被害総額は約30億7,300万円で昨年より1億6,300万円上昇しており、また、被害が発生した金融機関は223機関ですが、うち最も多かったのが信用金庫の98機関となり、前年の18機関から一気に80機関増加しています。

- 被害口座におけるセキュリティ対策状況は、個人口座でのワンタイムパスワードの利用率が9.7%、法人口座での電子証明書の利用率が17.2%にすぎず、個人・法人ともこうした対策を利用していない割合が7割前後にも上っています。


ITmedia エンタープライズ

2016年03月03日 14時09分 更新

2015年のネット不正送金被害は過去最悪に、対策未実施口座が7割も

被害件数は2014年より減少したものの、被害額は約30億7300万円と過去最悪になった。

[ITmedia]

警察庁は3月3日、2015年のインターネットバンキングの不正送金事犯の発生状況を発表した。被害額は約30億7300万円で過去最悪となり、特に信金・信組の法人口座の被害が急増している。

被害件数は1495件で、2014年の1876件から減少した。被害が発生した金融機関は223機関に上り、特に信用金庫での被害が前年比70機関増の98件と、金融機関別では最多を占めた。

金融機関・口座別の被害額の状況（警察庁資料より）

AUS便りからの所感等

- 振込み等の際の認証について、従来の番号表から、ハードウェアトークンあるいはスマホアプリによるワンタイムパスワードへ移行するケースが増えており、特に三菱東京UFJ銀行が今年6月からワンタイムパスワードの利用を必須とすることを発表していることから、他の金融機関が続く可能性も考えられます。

- 一方で、PCに感染し、パスワードや番号表の数字等あらゆる情報を搾取しようとする不正送金ウイルスの中には、ワンタイムパスワードをも奪取して不正送金を行おうとするものもあるとされており、アンチウイルスやUTMによりマルウェアが感染しないよう防御することも決して怠ってはいけない対策となります。

●CEOを語るメールで個人情報を外部に送信する事例相次ぐ

http://www.itmedia.co.jp/enterprise/articles/1603/01/news081.html

このニュースをザックリ言うと・・・

- 2月28日（米国時間）、写真共有アプリを提供する米Snapchat社より、フィッシング詐欺により同社従業員の給与情報が流出したと発表がありました。

- 発表によると、26日に給与課に対し、同社CEOのEvan Spiegel氏をかたり給与情報の送信を依頼するメールが送られており、従業員がフィッシングと気付かずに給与情報を返信したとのことで、同社ではこの4時間後に詐欺だったことを確認、FBIに通報しており、社内システムへの不正アクセスやアプリ利用者の情報の流出は発生していないとしています。

- 米国のセキュリティ情報サイト「Krebs on Security」によると、3月1日にハードディスクメーカーの米Seagate社でも、同様の手口により従業員の給与情報が流出していたとのことです。

- 今回の事件を受け、セキュリティベンダーのカスペルスキー社は「差出人が本人かどうか必ず確認し、できない限りはリンクをクリックしたり、要求された情報を送ったりしないこと」「適切なアンチウイルス製品を使うこと(悪意のあるリンクの検出等も行う)」を挙げている他、一般的なフィッシングの手口と対策に関するポイントを改めて紹介しています。


ITmedia エンタープライズ

2016年03月01日 07時54分 更新

米Snapchat、CEOかたる詐欺メールにだまされ従業員が情報流出

シュピーゲルCEOになりすました詐欺メールに従業員がだまされ、多数の従業員の給与に関する情報を流出させてしまった。

[鈴木聖子, ITmedia]

消えるメッセージングアプリを展開する米Snapchatは2月28日、ある従業員がフィッシング詐欺メールにだまされ、多数の従業員の給与に関する情報を流出させてしまったことが分かったと発表した。

発端はSnapchatの給与部門に2月26日に届いた1通のメールだった。何者かが最高経営責任者（CEO）のエバン・シュピーゲル氏になりすまし、従業員の給与に関する情報を要求。このメールを受け取った従業員は、詐欺だと気付かないまま、同社従業員と元従業員の給与情報を外部に流出させてしまったという。

Snapchat

AUS便りからの所感等

- これらのケースでとられた手法は、「ソーシャル・エンジニアリング」と呼ばれる古典的な手法ですが、今日においても依然として有効であるということを改めて裏付ける出来事と言えます。

- 前述した差出人の確認については、例えばメールヘッダによる送信元の確認も有効となるでしょうが、各ユーザにそれを求めるよりは、UTM等でそのチェックを行う機能があれば活用する方が現実的でしょう。