2022 年 12 月 19 日

Press Release

アカマイ・テクノロジーズ合同会社

【メディアアラート】
ホリデーシーズンに見られる 5 つの買い物客のタイプと
タイプ別で用心すべきサイバー詐欺について解説

いよいよホリデーシーズンの到来。クリスマスや新年の贈り物選びに買い物客でにわかに活気づく季節です。加えて、中国「独身の日」や、ブラックフライデー、サイバーマンデー、初売りやウィンターセールなど、国内外でセールや特売が続くこの季節は、買い物客にとってお得なショッピングのチャンスでしょう。
ここでは、オンラインライフの力となり、守るクラウド企業の Akamai Technologies, Inc. がオンラインショッピングサイトの年末年始の商戦でよく見られる 5 つの買い物客のタイプ別の特徴を紹介します。さらに、それぞれのケースで用心すべきサイバー詐欺も併せて解説します。消費者と企業、それぞれの立場から潜在的なセキュリティの盲点を認識して、このホリデーシーズンに自らを守る方法を再確認してみませんか？

「サイバー攻撃の数は増加の一途をたどり、絶えず変化しています。2022 年最大の懸念として、悪性ボットによる攻撃が急増し、その数は 3 倍に達しています。小売業界では、パスワードリスト型攻撃 (Credential Stuffing 攻撃)が増加しています。この攻撃では、不正に入手したユーザー認証情報のリストを使用してユーザーアカウントに侵入し、個人情報などのデータを抜き出す攻撃を仕掛けます」と、Akamai の APJ 担当 Director of Security Technology and Strategy の Dean Houari は述べています。

「この時期、ギフトやお得な商品を手に入れようと、多くの消費者で活性化するオンラインショップを、攻撃者が標的とするのは当然と言えます。特にアジアは、全世界の e コマース売上の約 60% を占めており、攻撃によって膨大な収益を得られるからです。買い物客と小売企業がともに詐欺行為に備え、自らを守る方法を学ぶことが重要です」と Houari は続けます。

5 つの買い物客のタイプ

1. **THE PLANNER（計画的な買い物客）**
   計画的な買い物客は、ホリデーシーズンの数か月前から情報収集し、確実にプレゼントを購入、ラッピングして準備を整える人々です。事前にしっかり計画して購入するこうした買い物客は、クレジットカード情報、ログイン情報、個人情報をショッピングサイトに保存しがちです。

   最も用心すべきサイバー攻撃：パスワードリスト型攻撃 (Credential Stuffing)
   サイトに情報を保存するのは便利ですが、そのアカウントに不正にログインされると、データが危険にさらされます。

攻撃者は不正に入手したユーザー認証情報のリストを使用し、多くのユーザーが複数のサービスで使いまわしているユーザー名とパスワードを悪性のボットを使って、標的にしたサイトでログインを試みます。

Credential Stuffing を阻止するために

- 特に決済に関わる情報をショッピング Web サイトに保存する場合は注意しましょう。 サイトごとに異なるパスワードを設定し、パスワードの安全性を高めましょう。さらに、パスワードマネージャーを使用して、推測しづらい強固なパスワードを生成することをお勧めします。

2. THE LAST-MINUTE SCRAMBLER（直前に慌てて購入する買い物客）

計画的な買い物客とは対照的に、直前に慌てて購入する買い物客は、セール日当日の深夜になって初めて、残り時間僅かで買い物をしなければならないことに気付きます。買いそびれないよう、常にぎりぎりの状態で慌てて購入しがちです。

最も用心すべきサイバー詐欺：フィッシング

直前に慌てて購入する買い物客は、急ぐあまり、メールやショートメッセージで届いた疑わしいハイパーリンクを、確認する間もなくついクリックしてしまい、フィッシング詐欺の犠牲になります。信頼できる小売企業からのメールになりすまして、偽の割引情報を案内するなど、多くの手口は見え透いていますが、こうした買い物客には細部を確認する余裕がありません。

オンラインマーケットプレイスの増加により、こうした詐欺行為が常態化しています。今年初め、シンガポールで最も人気の消費者間取り引きを仲介するマーケットプレイスで、攻撃者が出品された商品の購入者になりすまし、被害者を偽の銀行 Web サイトに導いて、支払いを受け取るための銀行情報を入力させました。その結果、72 人以上が被害に遭い、10 万 9,000 ドル (約 1,500 万円相当) 以上を騙し取られました。

フィッシングを阻止するために

- リンクをクリックしたり、個人情報を入力する前に、リンク先のサイトの信頼性を確認しましょう。メッセージに表示されている URL だけでなく、設定されているハイパーリンクが正規のドメインかも確認するようにしてください。
- 身に覚えのないメールであれば、何かおかしなところがないか確認します。誤った情報が記載されていたり、マクロの有効化、セキュリティ設定の調整、アプリのインストールが要求された場合は、そうした指示に一切従わないようにします。

3. THE BARGAIN HUNTER（バーゲンハンター）

バーゲンハンターは、価格が最も重要な購入判断の基準になります。さまざまなサイトで価格比較し、少しでもお得な商品を探します。

最も用心すべきサイバー詐欺：Web スキミング、オーディエンスハイジャック

バーゲンハンターは、なりすましのメールをクリックしたり、価格比較ツールと称する悪性のブラウザ拡張機能をそうと気付かずに有効化してしまう傾向があります。

攻撃者は、少しでもお得に購入したいという購買者の欲求につけ込みます。偽のセールス情報やクーポンを送ったり、ブラウザ表示させたりすることで、個人データをフォームに入力するように誘導します。さらに Google Analytics や Google Tag Manager などの正規ツールになりすまして、コードを不正に改ざんして盗聴用のスクリプトを仕込み有益な情報を盗み出して、ショッピングサイトと利用者に被害をもたらします。

Web スキミングやオーディエンスハイジャック攻撃を阻止するために

- 割引クーポンのオファーやメッセージの送信者の正当性を常に確認しましょう。
- 疑わしいファイルやリンクを阻止する第一防御ラインとして、スパムフィルターを活用してメールをスキャンするのも有効です。

4. THE IMPULSE BUYER（衝動買いの購入者）

衝動買いの購入者は、買い物前に何を買おうか具体的に考えていません。こうした買い物客は、時間制限のあるオファーやコストパフォーマンスに釣られて商品にアクセスし、時間に追われて購入しがちです。

最も用心すべきサイバー詐欺：なりすまし攻撃

サイバー犯罪者は、不正なリンクを介して人気のブランドになりすまし、被害者を騙して偽の Web サイトに誘導し、非正規製品の販売したり、マルウェアのダウンロードなどを仕掛けます。こうした傾向を助長しているのがソーシャルメディアです。ソーシャルメディアを利用することで、攻撃者は容易にブランドになりすまし、商品購入を希望する顧客とつながり、個人情報を要求します。

なりすまし攻撃を阻止するために

- メールに記載されたリンクが、正規のサイトに接続しない場合や、ブランドとは無関係の第三者のサイトに導いている場合は特に用心しましょう。
- 疑わしい場合は、リンクをクリックして決済を行う前に、ソーシャルメディアの公式チャネルなどからブランドに問い合わせて、そのオファーが正当かどうかを確認します。その場合も、表示された公式と思われるアカウントが認証済みかどうかを確認してください。

5. THE RESEARCHER（リサーチ重視の買い物客）

リサーチ重視の買い物客は、購入前に製品やオファーを徹底的に比較します。商品をすばやく比較できるように、さまざまなブラウザー拡張機能を有効にしがちです。

最も用心すべきサイバー詐欺：拡張機能マルウェア攻撃

サイバー犯罪者は、アドオンに隠ぺいしたウイルスで広告をインストールし、ユーザーの閲覧履歴を収集したり、有名なアプリや拡張機能になりすましてログイン認証情報を獲得します。セキュリティソフトウェアが、既知の拡張機能を信頼できるアプリケーションとして一旦扱ってしまうと、アップデートや改ざんなどで悪性のふるまいを追加された場合に、検知ができません。

最近話題になっているのは、FB Stealer などの情報窃盗マルウェアを使用した攻撃です。このマルウェアは、標準的で認知度の高い Chrome の拡張機能である Google Translate になりすまし、ユーザーを騙します。金銭を目的とした攻撃者は、ユーザーの Facebook アカウントをロックし、被害者になりすまして友人にお金を無心する行為に及んでいます。

拡張機能マルウェア攻撃を予防するために

- ブラウザの公式ストアにリストされている拡張機能のみをインストールするようにしましょう。
- 拡張機能のインストール前に疑わしい許可を求められた場合は、インストールするべきではありません。

小売企業は自社の責任で対策を

消費者に安全なショッピング体験を提供するために、小売企業は自らの責任で対策を取る必要があります。

ここ数年の小売大手に対する攻撃は、小売企業にとって重要な教訓になります。予防策は事後の救済策より有効です。小売体験全体で買い物客の安全を守るために、潜在的な脅威を監視し、不正アクセスをブロックする事前対策を講じるべきです。

「Web トラフィックの増加とともに、攻撃者の攻撃も増加しています。たとえば、昨年の「独身の日」には、悪性ボット攻撃が 3 倍に増加しています。こうした攻撃は、顧客アカウントの流出、サイト機能への損害、暗号化されたデータに対する身代金要求などを直ちに、あるいは将来的に引き起こします。いずれの場合も企業は莫大な費用を被ることになります」と Houari は説明します。

「長期にわたってロイヤルティを維持するために、小売企業には、買い物客のデータの安全性を確保するためにあらゆる努力が求められます。たとえば、ボット管理対策を展開して パスワードリスト型攻撃 (Credential Stuffing)を未然に阻止したり、多要素認証を使用してユーザーのセキュリティを確保するといった対策を推奨します」と Houari はまとめています。

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。クラウドからエッジまで、世界で最も分散されたコンピューティングプラットフォームにより、Akamai は、アプリケーションの開発や実行を容易にし、同時に、体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。