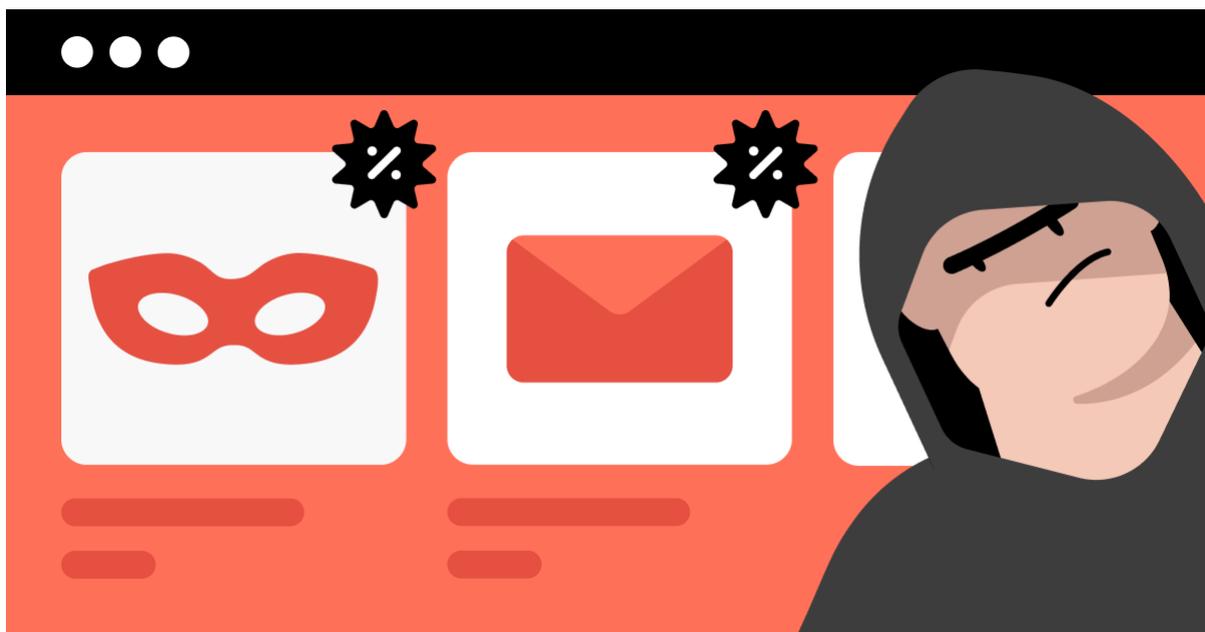


ブラックフライデーで詐欺リスク急増！？ NordVPN、フィッシング詐欺のリスク調査結果を発表！

～オンラインショッピングを安全に楽しむためのセキュリティ対策におけるポイントとは～

個人向けセキュリティサービスを展開する NordVPN(本社: Amsterdam, Netherlands、日本代表: 小原拓郎)は、ホリデーシーズンやブラックフライデーでのショッピングイベントを前に、オンラインの脅威対策機能を持つ同社の Threat Protection Pro™ を用いて、偽ショッピングサイトへのアクセスやフィッシング詐欺のリスクについて調査し、セキュリティ対策を発表しました。

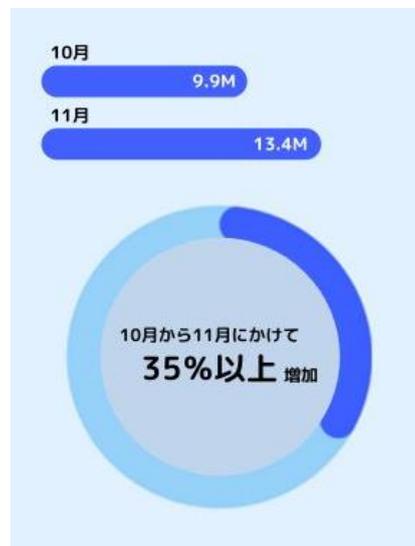


【調査概要】

オンラインの脅威対策機能を持つ Threat Protection Pro™を用いて、偽ショッピングサイトやフィッシング詐欺、悪意のあるダウンロードへのアクセスリスクを調査。2024年9月から10月の期間に収集したデータをもとに、これらの脅威の発生頻度と増加傾向を分析しました。特にホリデーシーズン前の消費行動が活発化する時期に合わせ、各種サイバー脅威が増加する傾向を確認し、1日あたりの平均のアクセスブロック件数や月間のサイトの伸び率を集計しました。

急増する偽ショッピングサイトへのアクセスブロック件数は約4割近く増加

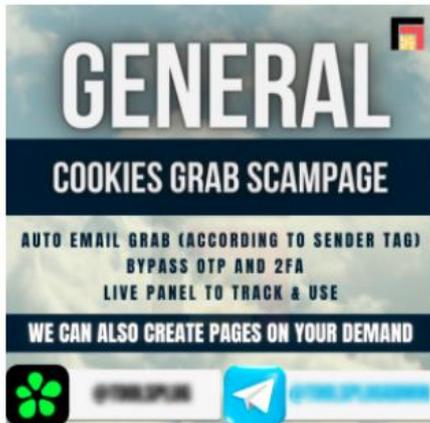
NordVPNの Threat Protection Pro™の統計によると、偽ショッピングサイトへのアクセスブロック件数が直近で35.8%増加し、9月の約990万件から10月には1,340万件に達しました。これは1日あたり平均381,000件がブロックされた計算となり、ブラックフライデーやホリデーシーズンを前に、オンラインショッピング詐欺のリスクが増加していることを示しています。ブラックフライデーなどの大規模ショッピングイベント時には、さらにリスクが高まると予測されます。



Threat Protection Pro™にて
検知された偽ショッピングサイトへの
アクセスブロック件数

ダークウェブでは、月額 100 から 150 ドル程度のサブスクリプションのマルウェア・アズ・ア・サービスが提供されており、フィッシング・キットも無料で入手できることが多いです。その結果、サイバー犯罪者は詐欺がしやすい幅広いツールを手に入れ、簡単にアクセスできるテレグラムチャンネルやフォーラムを通じてサポートを受けることができます。

Cookie 窃取ページは、ダークウェブで見られる最も高価なオンライン詐欺キットの一つです。これらのページは、ユーザーのブラウザや Facebook などのソーシャルメディアから cookie をキャプチャするために特別に作られており、ハッカーはこれを悪意に使用できます。



Cookies Grab Page

All Domains Cookies Grab Script-
General Cookies Grab

☆☆☆☆☆

\$400.00

Add to cart



Cookies Scam Pages

Latest Facebook Cookies
Grab ScamPage

☆☆☆☆☆

~~\$500.00~~ \$350.00

Add to cart



Scam Pages

Chase Bank Scam Page
with OTP CODE

☆☆☆☆☆

\$80.00

Add to cart

「NordVPN の調査により、ダークウェブで 540 億以上の cookie が販売されていることが明らかになりました。ハッカーがあなたのアクティブな Cookie を手に入れた場合、あなたのアカウントにログインし乗っ取るために、ログイン認証情報、パスワード、あるいは多要素認証さえも必要としないことに、気付かないかもしれません。Cookie から最もよく盗まれる個人情報には、名前、電子メールアドレス、都市名、パスワード、住所などがあります」と Nord VPN のサイバーセキュリティ専門家のエイドリアナス・ワルメンホーフェンは話します。

■偽ショッピングサイトでよく使われる手法について

詐欺的なオンラインショップは、さまざまな手法で消費者を騙し、購入後のトラブル解決や返金がほぼ不可能な状況に追い込みます。特にホリデーシーズンやブラックフライデーにはこうした詐欺手法が増加する傾向があり、消費者には一層の注意が求められます。

不自然な割引

著しく割安な商品を提示し、支払い後にサイトを閉鎖する手口です。

低品質や偽造品の配送

購入品が広告と異なり、安価な偽物や低品質な商品であることが多いです。

正規ブランドへのなりすまし

実在するブランドのロゴやデザインを模倣し、消費者の信頼を得ようとする手法です。

偽レビューの掲載

過度に肯定的なレビューのみを掲載し、信頼できるショップに見せかけます。

フィッシングメールや広告

実在のブランドを装ったメールや広告で消費者を誘導し、個人情報を詐取します。

■NordVPN が提案する偽ショッピングサイトの見分け方について

サイバーセキュリティツールを活用するとともに、自らも偽ショッピングサイトを見極めることが重要です。オンラインショッピングを安全に楽しむためのポイントを紹介します。

価格が不自然に安い場合は警戒する

信頼できるサイトで相場を確認し、過度な割引には注意を。

サイトの品質を確認する

文法エラーや低解像度の画像などがある場合は利用を控えましょう。

ドメイン名や SSL 証明書を確認する

不自然なドメイン名や有効な SSL 証明書がない場合は注意が必要です。

連絡先情報の有無

住所や電話番号、メールアドレスが記載されていない場合は利用を慎重にご判断ください。

通常とは異なる支払い方法の要求に注意

暗号通貨やギフトカードなど、追跡が難しい支払い方法の要求には注意してください。

小売業者について調べる

業者名と「レビュー」「詐欺」などのキーワードで検索し、否定的な評価が多い場合は注意しましょう。

セキュリティツールの活用

NordVPN の Threat Protection Pro™ は、不正サイトやフィッシング詐欺を自動的にブロックし、安心してショッピングを楽しむサポートを提供します。

■NordVPN の Threat Protection Pro™について

NordVPN の Threat Protection Pro™は、フィッシング攻撃や偽ショッピングサイトなどのサイバー脅威からユーザーを保護する高度なセキュリティツールです。マルウェアのスキャン、トラッカーや迷惑広告のブロック機能を備え、安全で快適なブラウジングを提供します。また、AIを活用したアンチフィッシング機能により、新たな脅威にも対応が可能なおえ、ワンクリックで複数のブラウザを保護できる点も特徴です。

■NordVPN について

NordVPN は、世界中で何百万人のユーザーをもつ先進的な VPN サービスプロバイダーです。6,400 台以上のサーバーを 111 カ国で提供し、専用 IP や Double VPN、Onion Over VPN サーバーなど、多彩な機能を備え、トラッキングなしでオンラインプライバシーを強化します。主要機能の一つである「脅威対策 Pro」は、悪質なウェブサイトやトラッカー、広告のブロックに加え、マルウェアのスキャンが可能です。さらに、最新製品グローバル eSIM サービス「Saily」を展開しています。

【会社概要】

会社名: NordVPN

本社: Fred. Roeskestraat 115 1076 EE Amsterdam, Netherlands

日本代表: 小原拓郎

NordVPN ウェブサイト: <https://nordvpn.com/ja/>

VPN について: <https://nordvpn.com/ja/what-is-a-vpn/>