

月次報告書（2008年11月分）

フィッシング情報届出状況

2008年12月20日

目次

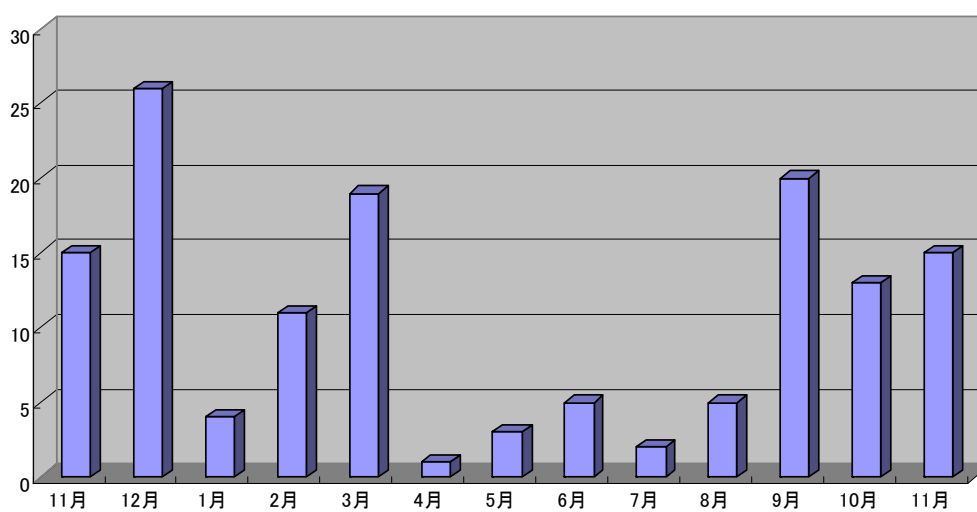
1. フィッシング情報届出状況	2
1.1. フィッシング情報届出状況	2
1.2. 業種別の状況	5
1.3. フィッシングサイトのホスト国	6
1.4. フィッシングメールの動向	7
1.5. フィッシングサイトの動向	14
1.6. フィッシング関連の不正プログラム情報	19
1.7. その他の動向	19
1.8. 総括	19

1. フィッシング情報届出状況

1.1. フィッシング情報届出状況

- ・ フィッシングメール届出件数： 15 件

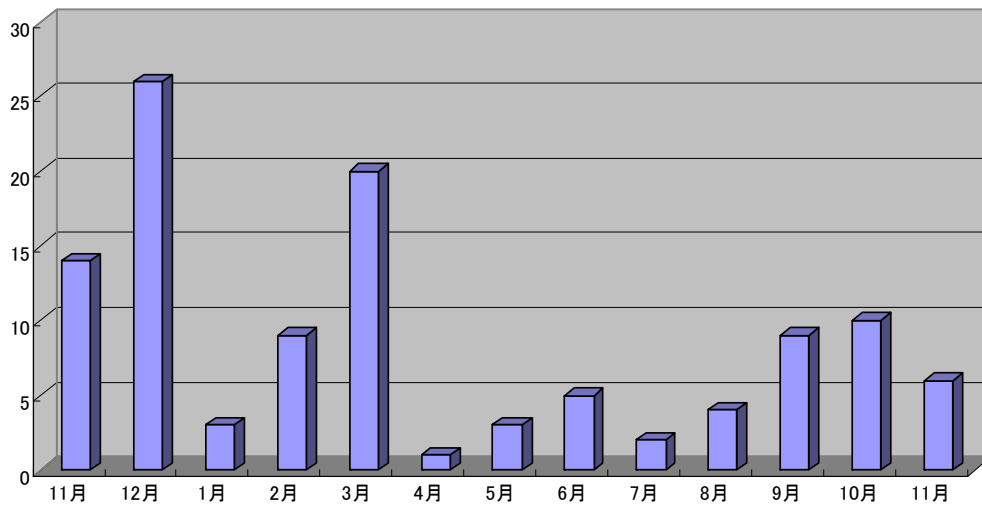
2008年11月度におけるフィッシング情報の届出件数は、前月度より2件増加し15件となりました。過去1年間の平均を上回っています。



フィッシング届出情報の件数(2007年11月～2008年11月)

・ **フィッシングメールの件数**： 6件

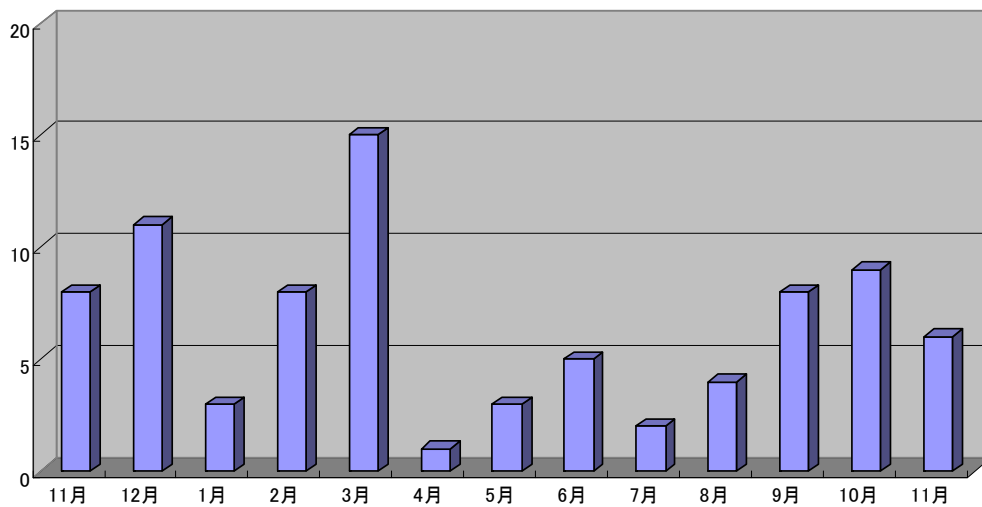
2008年11月度に報告されたフィッシングメールの件数は、前月度より4件減少し6件となりました。過去1年間の平均を若干下回っています。



フィッシングメールの件数(2007年11月～2008年11月)

・ **フィッシングサイトの件数**： 6件

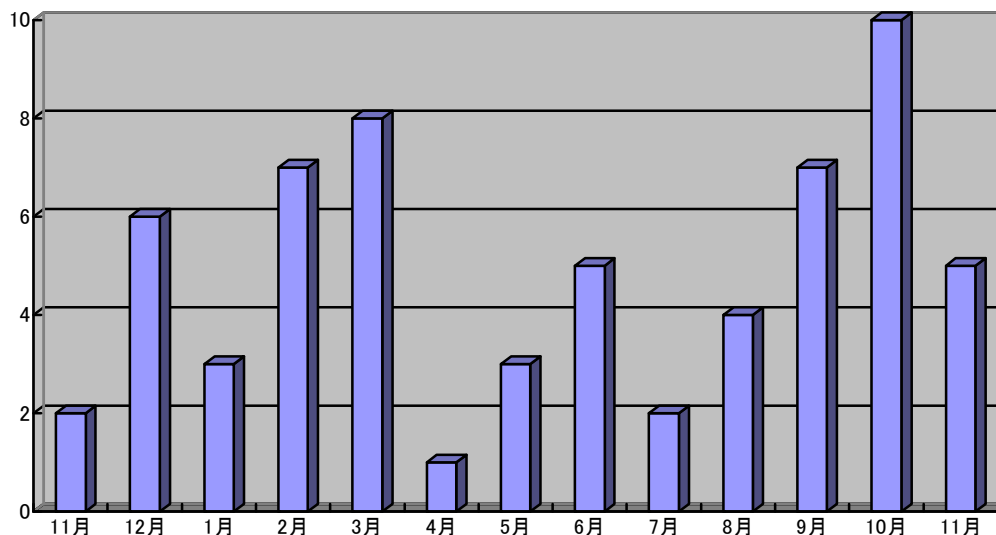
2008年11月度に報告されたフィッシングサイトの件数は、前月度より3件減少し6件となりました。過去1年間の平均とほぼ同じです。



フィッシングサイトの件数(2007年11月～2008年11月)

・ フィッシングによりブランド名を悪用された企業の件数 : 5 件

2008 年 11 月度にブランド名を悪用された企業の件数は、前月度より 5 件減少し 5 件となりました。

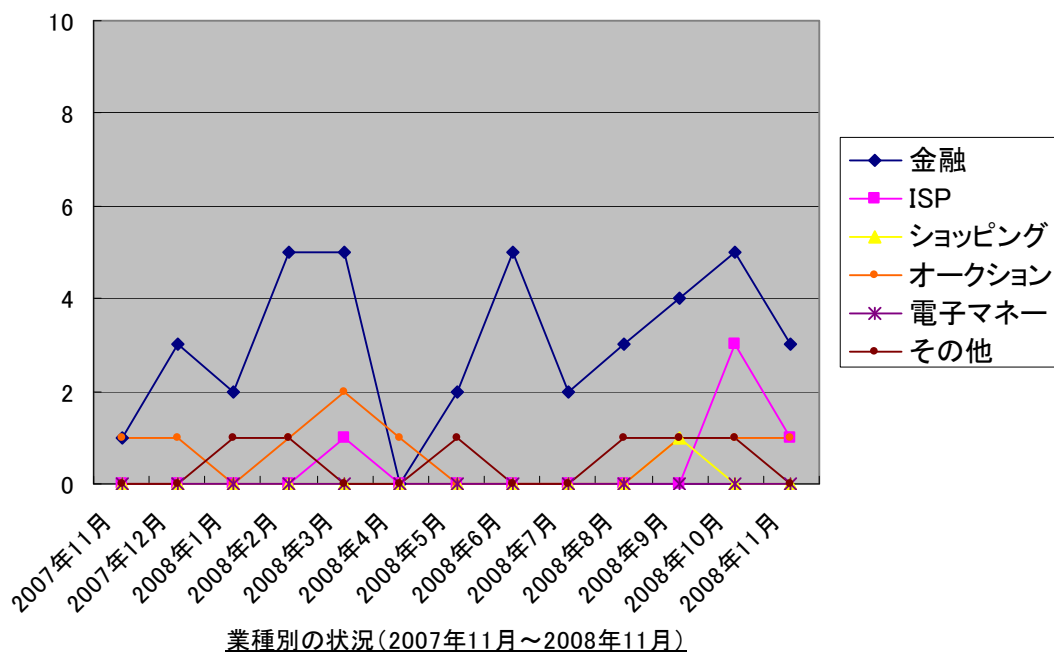


フィッシングによりブランド名を悪用された企業の件数(2007年11月～2008年11月)

- ・ もっともフィッシングに利用される WEB サイトが多かった国 : アメリカ (2 件)、日本 (2 件)、ロシア (1 件)

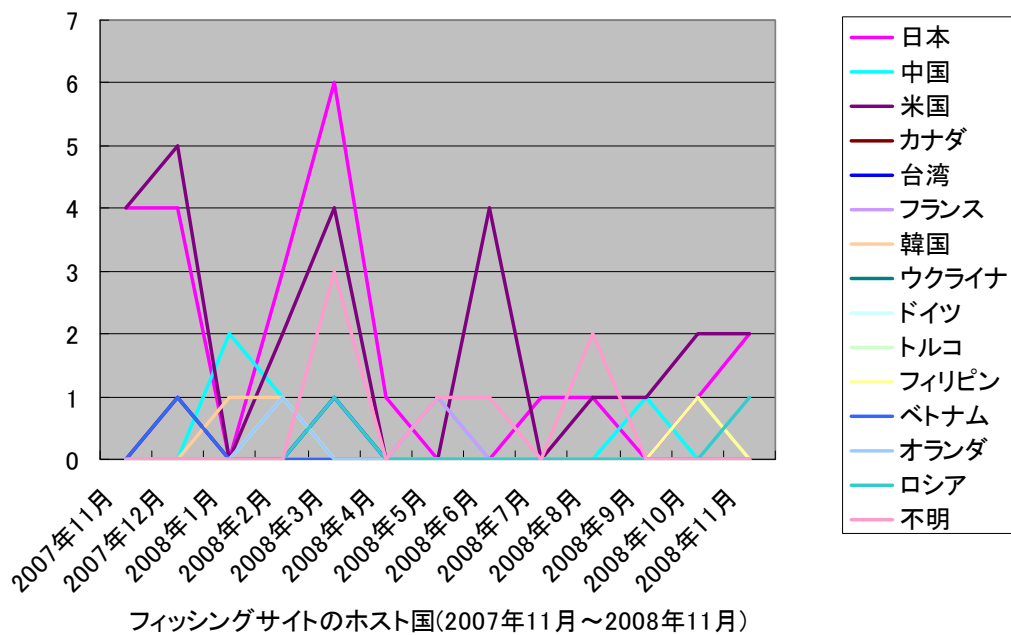
1.2. 業種別の状況

2008年11月度に標的となった業種は、金融が3件、ISPが1件、オークションが1件でした。



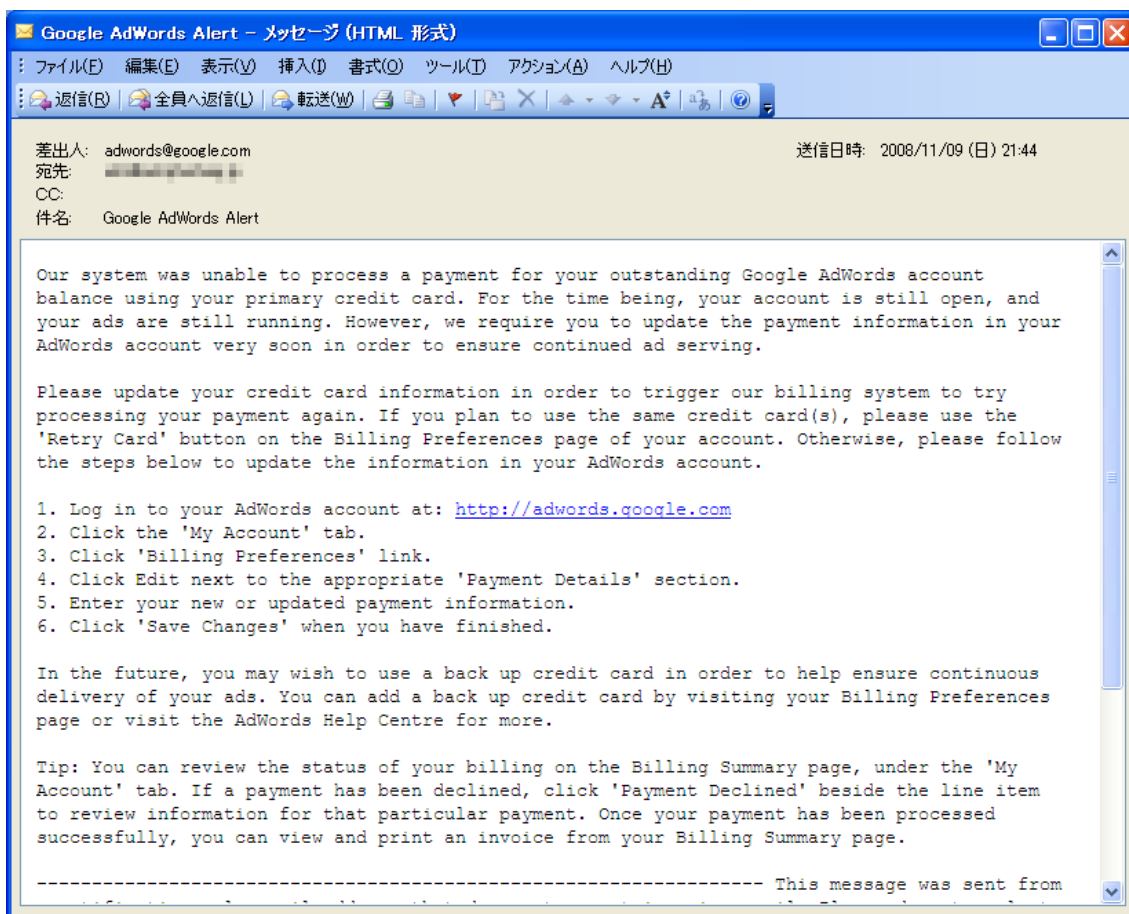
1.3. フィッシングサイトのホスト国

2008年11月度に報告されたフィッシングサイトは、アメリカで2件、日本で2件、ロシアで1件ホスティングされていました。

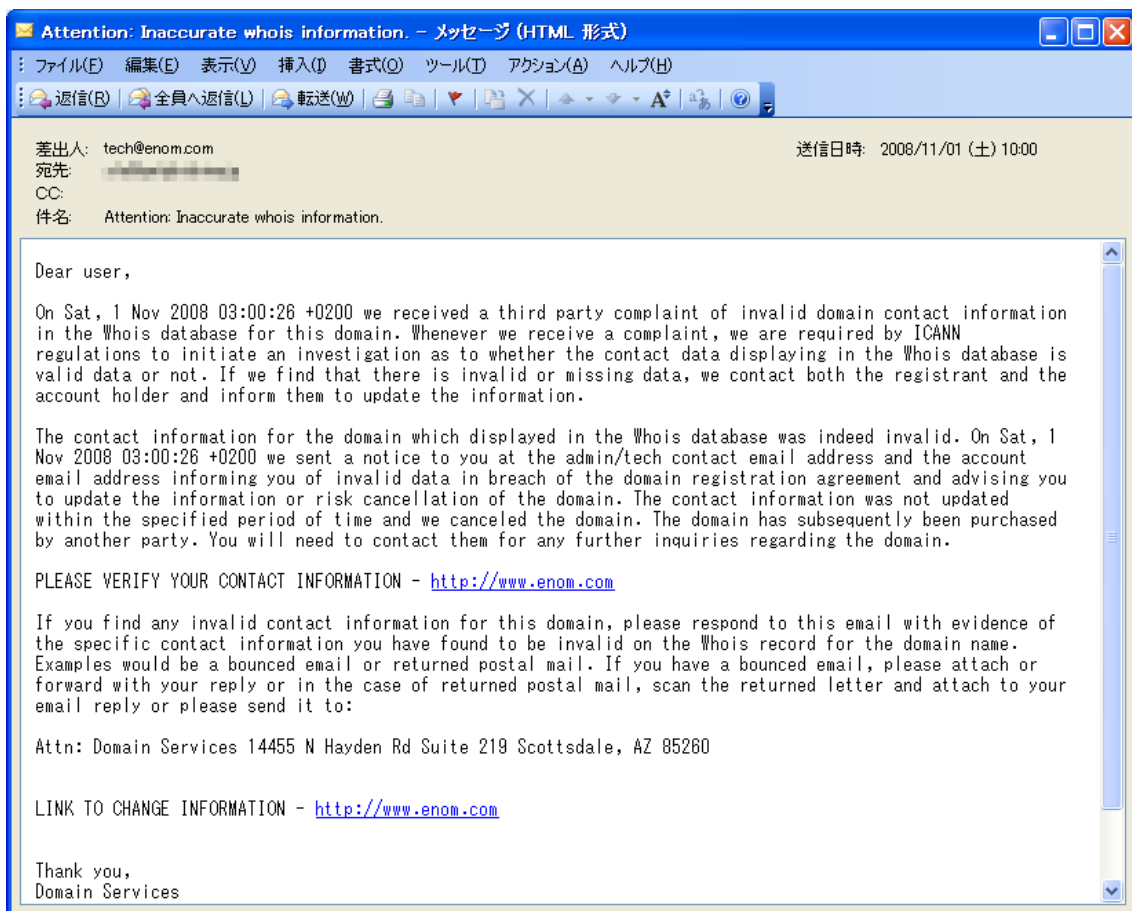


1.4. フィッシングメールの動向

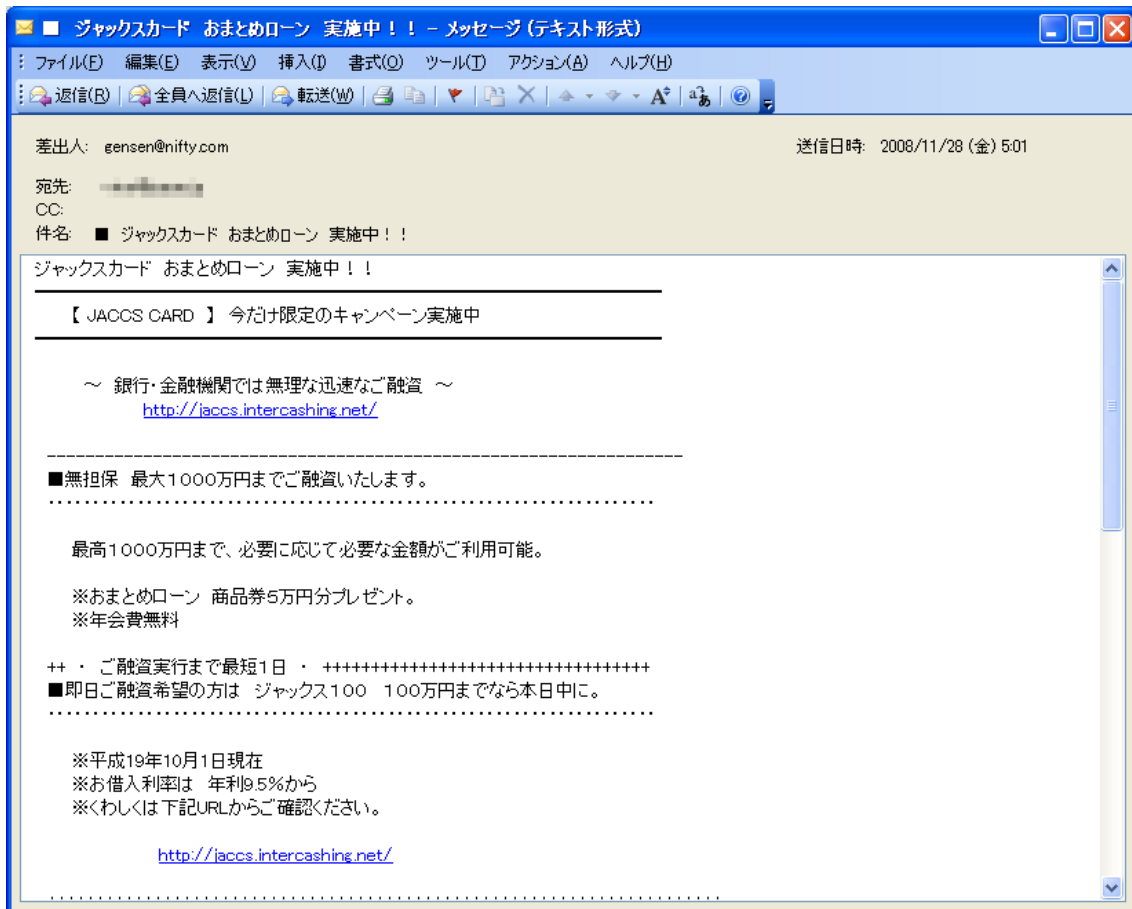
「Google AdWords」をかたるフィッシングメールが確認されました。差出人は「adwords@google.com」、件名は「Google AdWords Alert」で、英語で書かれたHTML形式のメールになっています。メールは、「Google Adwords」の支払いプロセスが実行できないなどとして、クレジットカード情報入力の偽サイトへ誘導しようとしています。



先月に引き続き、「Enom.com」をかたるフィッシングメールが確認されました。差出人は「tech@enom.com」、件名は「Attention Inaccurate whois information.」で、英語で書かれたHTML形式のメールになっています。メールは、ドメインの連絡先情報が無効であるという苦情を受けたため、ICANNの規則によって調査を開始しなければならないとし、登録情報の更新のためとして偽サイトへ誘導しようとしています。



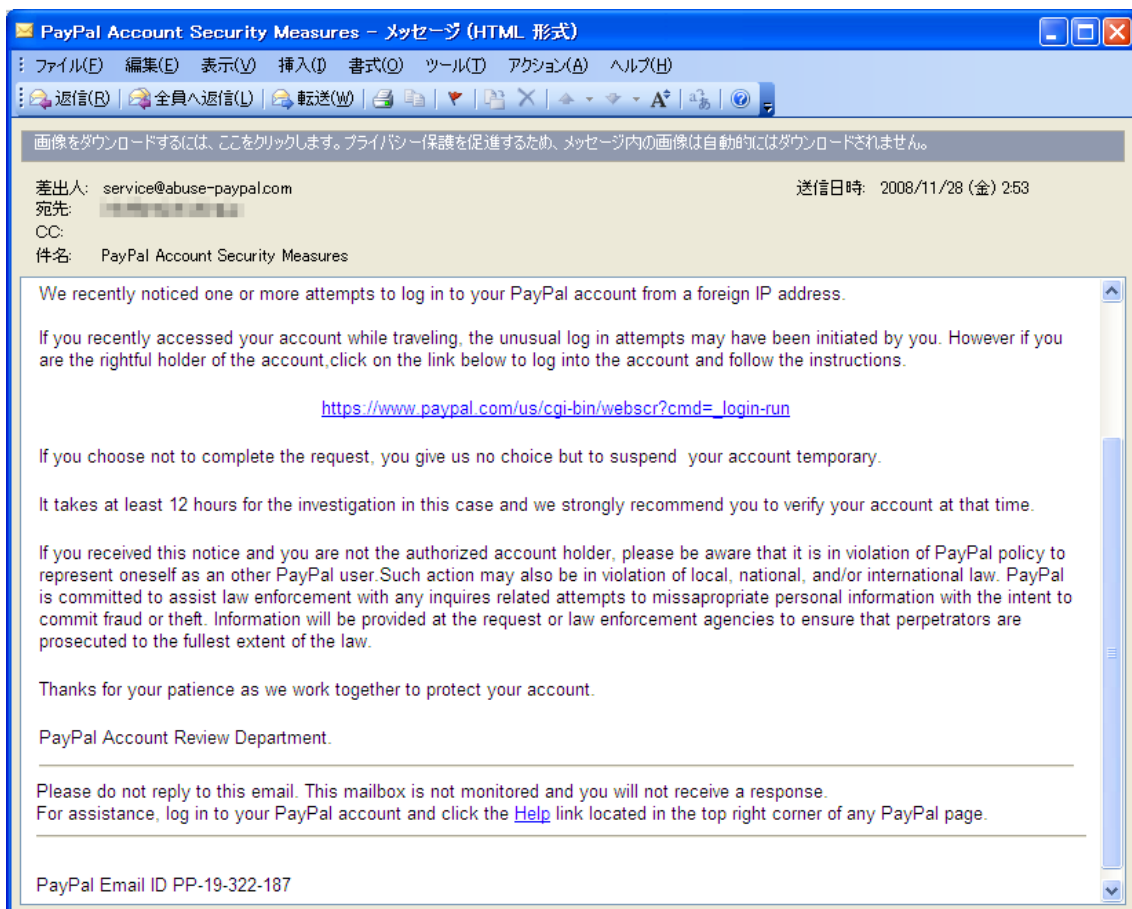
今月新たに、「ジャックス」をかたるフィッシングメールが確認されました。差出人は「gensen@nifty.com」、件名は「■ ジャックスカード おまとめローン 実施中！！」で、日本語で書かれたテキスト形式のメールになっています。メールは、キャッシング詐欺サイトを宣伝し、個人情報を入力させる偽サイトへ誘導しようとしています。



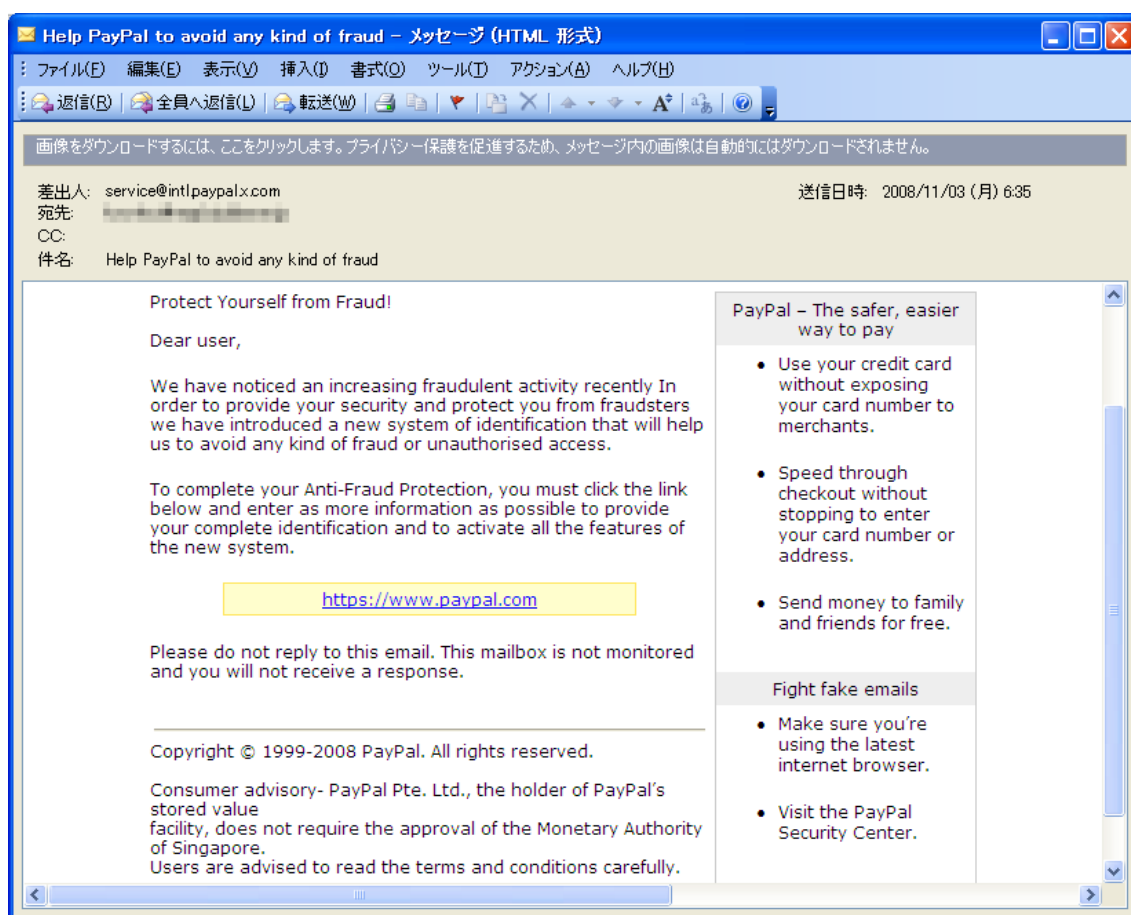
「オリコ」をかたるフィッシングメールが確認されました。差出人は「gen5454@nifty.com」、件名は「■ オリコグループのネット専用キャッシング」で、日本語で書かれたテキスト形式のメールになっています。メールは、キャッシング詐欺サイトを宣伝し、個人情報を入力させる偽サイトへ誘導しようとしています。



先月に引き続き、「PayPal」をかたるフィッシングメールが確認されました。差出人は「service@abuse-paypal.com」、件名は「PayPal Account Security Measures」で、英語で書かれた HTML 形式のメールになっています。メールは、ユーザの「PayPal」口座に外国からログインがあり、ユーザが正規の利用者か確認するためとして口座情報の入力偽サイトへ誘導しようとしています。



先月に引き続き、「Paypal」をかたるフィッシングメールが確認されました。差出人は「service@intl.paypal.x.com」、件名は「Help PayPal to avoid any kind of fraud」で、英語で書かれた HTML 形式のメールになっています。メールは、近年のフィッシング詐欺の増加に伴い、「PayPal」に新規のセキュリティシステム導入が予定されており、システムの有効化のため登録作業が必要だとして偽サイトへ誘導しようとしています。



先月に引き続き、「Yahoo! オークション」をかたるフィッシングメールが確認されました。先月出回っていたフィッシングメールと文面、書式が似ており差出人は「cly35860@pop26.odn.ne.jp」、件名は「Yahoo!オークションのご利用に関するお知らせです。※重要！！」で、日本語で書かれたテキスト形式のメールになっています。メールは、Yahoo! オークションを引き続き利用するために Yahoo! JAPAN ID ユーザーアカウント更新手続きが必要だとして偽サイトに誘導しようとしています。



1.5. フィッシングサイトの動向

「Google Adwords」をかたるフィッシングサイトは、正規のログインサイトを装い Google アカウントの登録メールアドレス、パスワードを盗み出そうとします。サイトはアメリカのサーバでホスティングされていました。



English (US)

Increase website traffic with Google

No matter what your budget, you can display your ads on Google and our advertising network. Pay only if people click your ads.

Try AdWords now

Your ads appear beside related search results...

People click your ads...

...And connect to your business



Sign in to Google AdWords with your Google Account

Email:

Password:

Sign in

[I cannot access my account](#)

Learn about AdWords

How it works

[Reach more customers](#)

[Costs and payment](#)

[For local businesses](#)

[Success stories](#)

You create your ads

You create ads and choose keywords, which are words or phrases related to your business.

[Get keyword ideas](#)

Your ads appear on Google

When people search on Google using one of your keywords, your ad may appear next to the search results. Now you're advertising to an audience that's already interested in you.

You attract customers

People can simply click your ad to make a purchase or learn more about you. You don't even need a webpage to get started - Google will help you create one for free. It's that easy!

[Sign up now](#) | [Next topic](#)>>



Keywords are what people search for on Google.



Your *ad* appears beside relevant search results.

「Enom.com」をかたるフィッシングサイトは、正規の Enom.com サイトを装いアカウントの登録 ID、パスワードを盗み出そうとします。サイトはアメリカのサーバにホスティングされていました。

The image shows a screenshot of a phishing website designed to look like the Enom.com domain registration page. The layout includes a dark blue header with the Enom logo, navigation links like 'Get Started', 'Log-in', and 'Help', and buttons for 'Register', 'Transfer', and 'Whois'. A search bar for 'Register A Domain' with a 'GO' button is present. Below the header is a navigation menu with categories: 'Domains', 'Hosting', 'Email', 'SSL Certificates', 'More Products', 'Resellers', and 'Get Started'. The main content area is split into two columns. The left column, titled 'New to eNom?', contains text about applying for a reseller account and lists features: 'Account Manager', 'Versatile Product Suite', and 'FREE Services'. It also features an 'ICANN ACCREDITED' logo and a 'Learn more' button. The right column, titled 'Log-in to your Account', prompts users to enter their 'Log-in ID' and 'Password', with checkboxes for 'Remember my Log-in ID' and 'Keep me logged-in on this computer', and a 'log-in' button. A disclaimer at the bottom of this section states that logging in implies agreement to terms and conditions, with links for 'log-in help' and 'lost password?'. The footer contains a navigation menu with links like 'About Us', 'Help', 'Careers', etc., and sections for 'Awards & Achievements' (listing logos for ICANN, BBB, and others) and 'Payment Options' (listing logos for PayPal, VISA, MasterCard, American Express, and Discover). The footer also includes copyright information for 1998-2008 eNom Inc. and a 'demand MEDIA Services' logo.

「ジャックス」をかたるフィッシングサイトは、融資の自動診断としてメールアドレス、名前、携帯電話番号などを盗み出そうとします。サイトは日本のサーバにホスティングされていました。

参考情報)

【ご注意】弊社名および弊社と紛らわしい名を名乗る団体について（ジャックス）

http://www.jaccs.co.jp/information/attent_ruiji.html

The screenshot shows the JACCS Corporation website interface. At the top left is the JACCS CORPORATION logo. A navigation bar contains links for HOME, ご利用方法, 商品のご案内, and 会員様ログイン. On the left side, there are menu buttons for お申し込み, Q & A, プライバシーポリシー, and 会社概要. The main content area features a banner with the text "毎日の暮らしの中に、いつもジャックス" and an image of a man in a suit. To the right of the banner is a "キャンペーン情報" (Campaign Information) section with three bullet points: 1. Real interest rate for JACCS Free-100 is 9.5%, and for JACCS Business 1000 it is 5.4%, a significant reduction. 2. For JACCS Free-100, the transfer time from application to the designated account is as short as 25 minutes, or within 30 minutes. 3. For JACCS Business 1000, a new contract is a gift to all members, including a 50,000 yen gift certificate. Below the banner is an "自動診断" (Automatic Diagnosis) section with a warning: "ご融資の可否をスピード簡易審査!! 簡単な項目の選択だけで、ご融資が可能かすぐに連絡します。お申し込み前のチェックにご利用下さい。" The form includes input fields for 希望金額, メールアドレス, お名前, 携帯電話番号, 生年月日 (with year, month, and day dropdowns), お住まいの地域, and ご連絡可能な時間帯. A note states: "* 全て入力しないと、自動返信できません". At the bottom of the form are buttons for "診断" and "取消". On the right side of the page, there is a warning box titled "こんな手口に注意!" (Pay attention to this method!) with the text: "※ 悪質な振込め詐欺の被害が急増しています。090金融などにご注意下さい。"

「オリコ」をかたるフィッシングサイトは、融資のお試し診断としてメールアドレス、名前、携帯電話番号などを盗み出そうとします。サイトは日本のサーバにホスティングされていました。

参考情報)

当社名称及び当社の類似名称を名乗る金融業者（オリコ）

http://www.orico.co.jp/school/security/info_01.html

Orico
オリコ信販株式会社

オリコグループ ネット専用キャッシング

HOME
ご利用方法
商品のご案内
シュミレーション
お申し込み
会員様ログイン
Q&A
プライバシーポリシー
会社概要

所在地:
〒106-0013
東京都港区浜松町2-9
電話番号:
03-5907-4624
貸金業登録番号:
東京都知事(2)第15682号

新規ご契約のお客様には、
もれなく5万円分の商品券をプレゼント!!

お試し診断
ご融資の可否をスピード簡易審査!!
簡単な項目の選択だけで、ご融資が可能がすぐに連絡します。
お申し込み前のチェックにご利用下さい。

希望金額
メールアドレス
お名前
携帯電話番号
生年月日 昭和 年 月 日
お住まいの地域
ご連絡可能な時間帯

* 全て入力しないと、自動返信できません

キャンペーン情報
実質年率をオリコフリー100は9.5%に、オリコビジネス1000は5.4%へと大幅に引き下げいたしました。
この機会にぜひお申し込み下さい。

オリコフリー100なら、お申し込みからお客様の指定口座に振込みまで最短25分、30分以内に確実に振込みいたします。

オリコビジネス1000を新規にご契約いただいたお客様には、全員に商品券5万円分をプレゼント。

ご注意
悪質な振込の詐欺の被害が増えています。
090金融などにご注意下さい。

Copyright(c)2008 ORICO SHINPAN All Rights Reserved.

「PayPal」をかたるフィッシングサイトは、正規のPayPal ログインサイトを装い、アカウントの登録メールアドレス、パスワードを盗み出そうとします。サイトはロシアのサーバにホスティングされていました。



1.6. フィッシング関連の不正プログラム情報

特にありません。

1.7. その他の動向

US-CERT（米政府系組織のコンピュータ緊急事態対策チーム）は、米国の連邦準備制度をかたるフィッシングメールについて警告を行いました。メールには、フィッシング詐欺の発生が報告されており、詳細情報として、PDFの脆弱性を悪用する不正なWebサイトのURLが記載されています。

関連 URL :

U.S. Federal Reserve Fraudulent Email Scam 2008/11/13 (US-CERT)

http://www.us-cert.gov/current/archive/2008/11/18/archive.html#u_s_federal_reserve_phishing

Bogus Federal Reserve Sites Deliver PDF Exploit 2008/11/13 (TrendLabs)

<http://blog.trendmicro.com/bogus-federal-reserve-sites-deliver-pdf-exploit/>

1.8. 総括

今月度は、新たに「ジャックス」をかたるフィッシングメールおよびサイトを確認しました。同様にクレジットカード会社をかたるものとして「オリコ」のフィッシングも確認されており、両方ともメール、サイトが非常に良く出来ているため、ログイン、パスワード等の入力を行わないよう引き続き十分な注意が必要です。

その他のフィッシングは以前から出回っている「Google Adwords」、「Enom.com」、「PayPal」、「Yahoo! オークション」などでメールの内容、サイトも同じものでした。但し、サイトのホスティング場所は変わっており、今後もホスティング場所を変えながら同様のブランドをかたるフィッシング詐欺が繰り返されることが予想されます。