月次報告書（2009年2月分）

フィッシング情報届出状況

2009 年 3 月 20 日

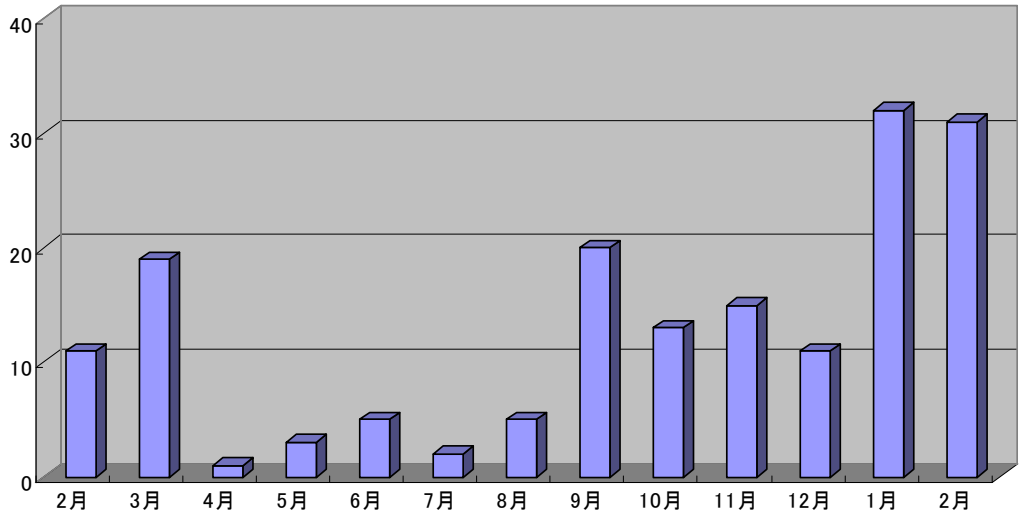
目次

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**： 31 件

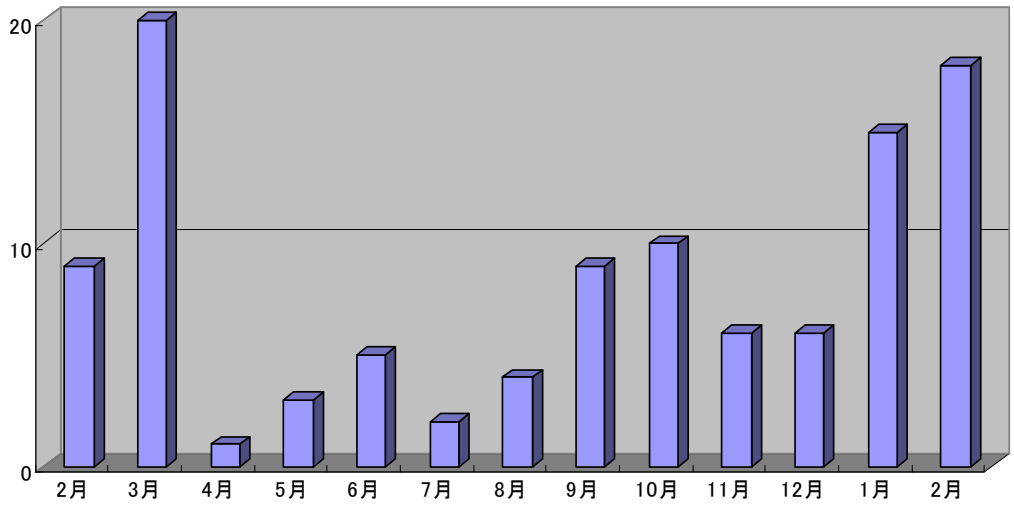
2009 年 2 月度におけるフィッシング情報の届出件数は、前月度より 1 件減少し 31 件となりました。過去 1 年間の平均を大きく上回っています。



フィッシング情報の届出件数（2008年2月～2009年2月）

・ **フィッシングメールの件数**： 18 件

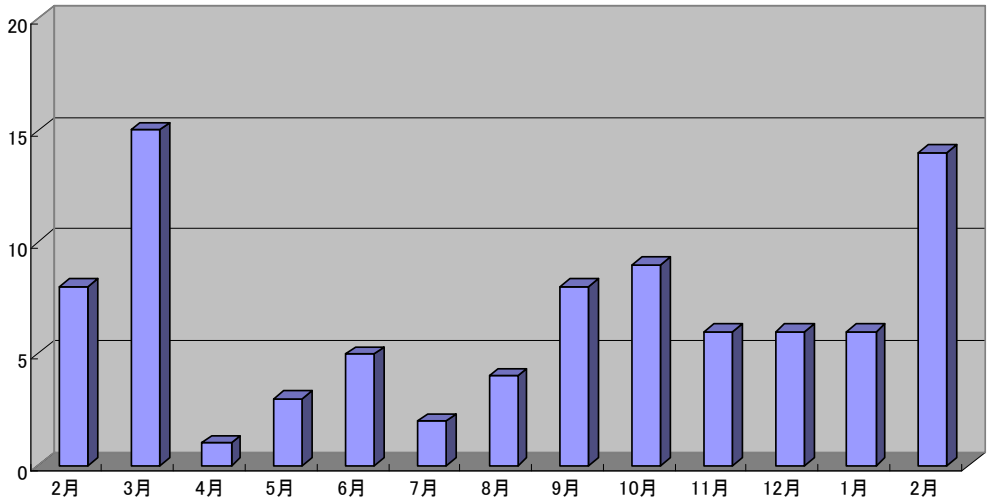
2009 年 2 月度に報告されたフィッシングメールの件数は、前月度を上回り、18 件となりました。過去 1 年間の平均を 2 倍以上で上回っています。



フィッシングメールの件数（2008年2月～2009年2月）

・ **フィッシングサイトの件数**： 14 件

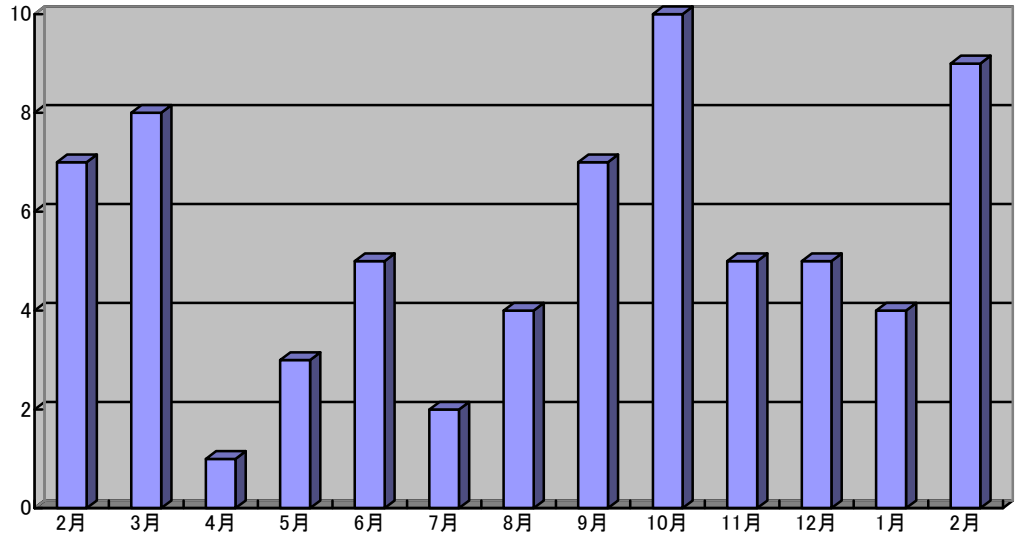
2009 年 2 月度に報告されたフィッシングサイトの件数は、前月度を上回り 14 件となりました。過去 1 年間の平均に対し、2 倍の数値を示しています。



フィッシングサイトの件数（2008年2月～2009年2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： 9 件

2009 年 2 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 件増加し、9 件となりました。



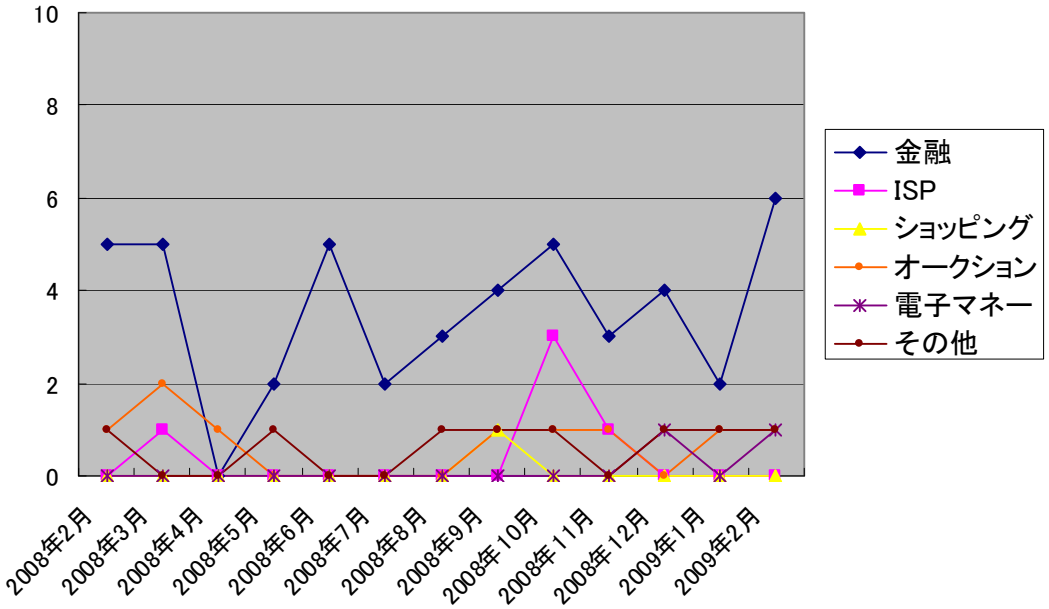
フィッシングによりブランド名を悪用された企業の件数（2008年2月～2009年2月）

・ **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**：

日本（3 件）アメリカ（2 件）

1.2. 業種別の状況

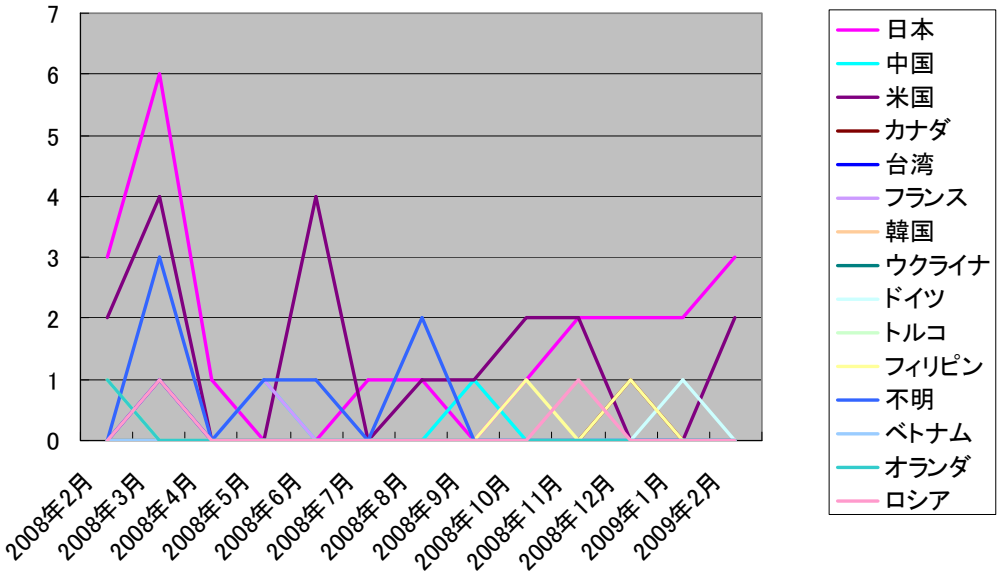
2009 年 2 月度に標的となった業種は、金融が 6 件、オークションが 1 件、電子マネーが 1 件、その他が 1 件でした。



業種別の状況（2008年2月～2009年2月）

1.3. フィッシングサイトのホスト国

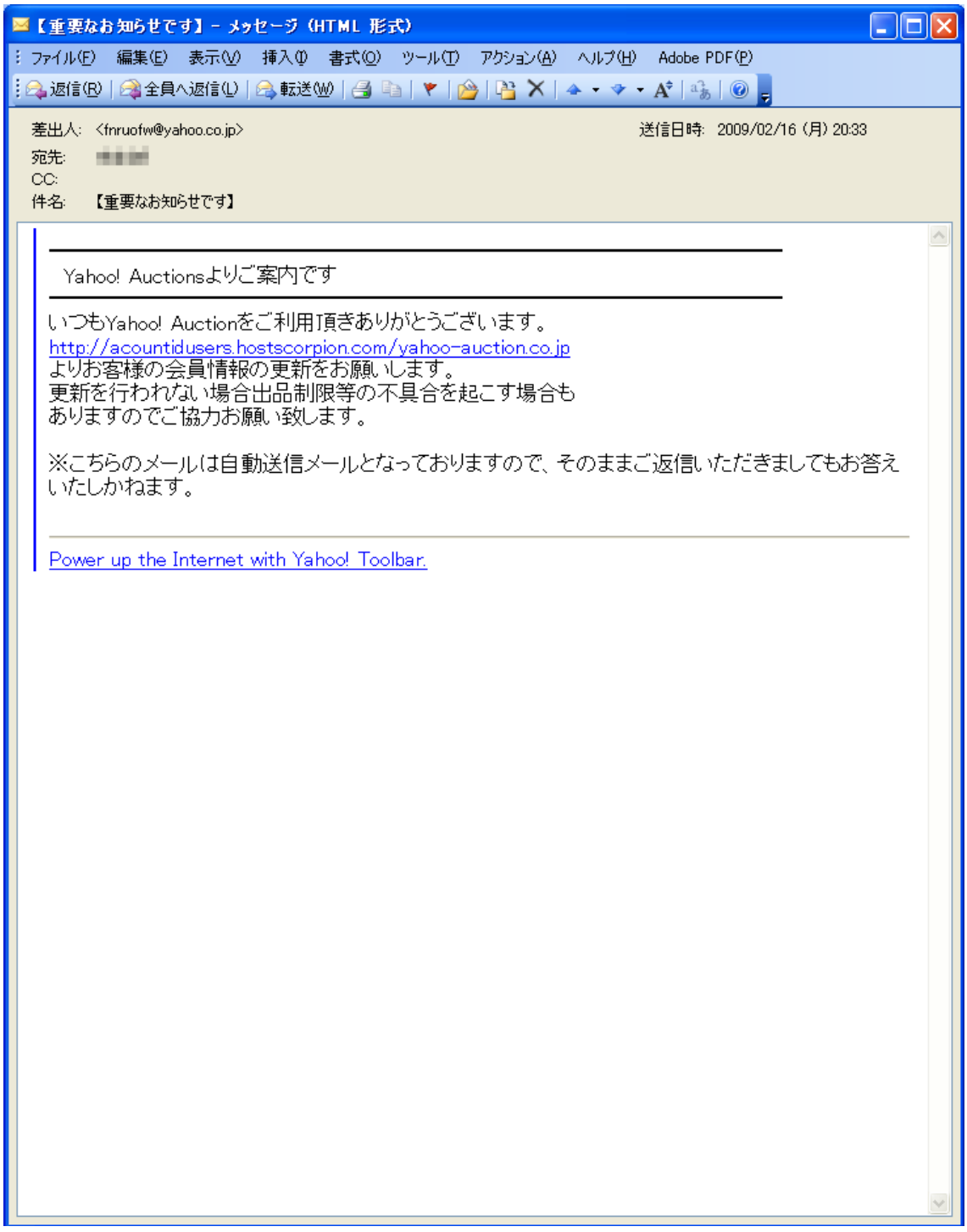
2009 年 2 月度に報告されたフィッシングサイトは、日本で 3 件、アメリカで 2 件ホスティングされていました。



フィッシングサイトのホスト国(2008年2月～2009年2月)

1.4. フィッシングメールの動向

先月に引き続き「Yahoo!」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「<fnruofw@yahoo.co.jp>」、件名は「【重要なお知らせです】」で、日本語で書かれた HTML 形式のメールになっています。メールは、会員情報の更新が必要とし、偽サイトへ誘導します。



差出人および件名、偽サイト URL の一覧を、下表に纏めます。

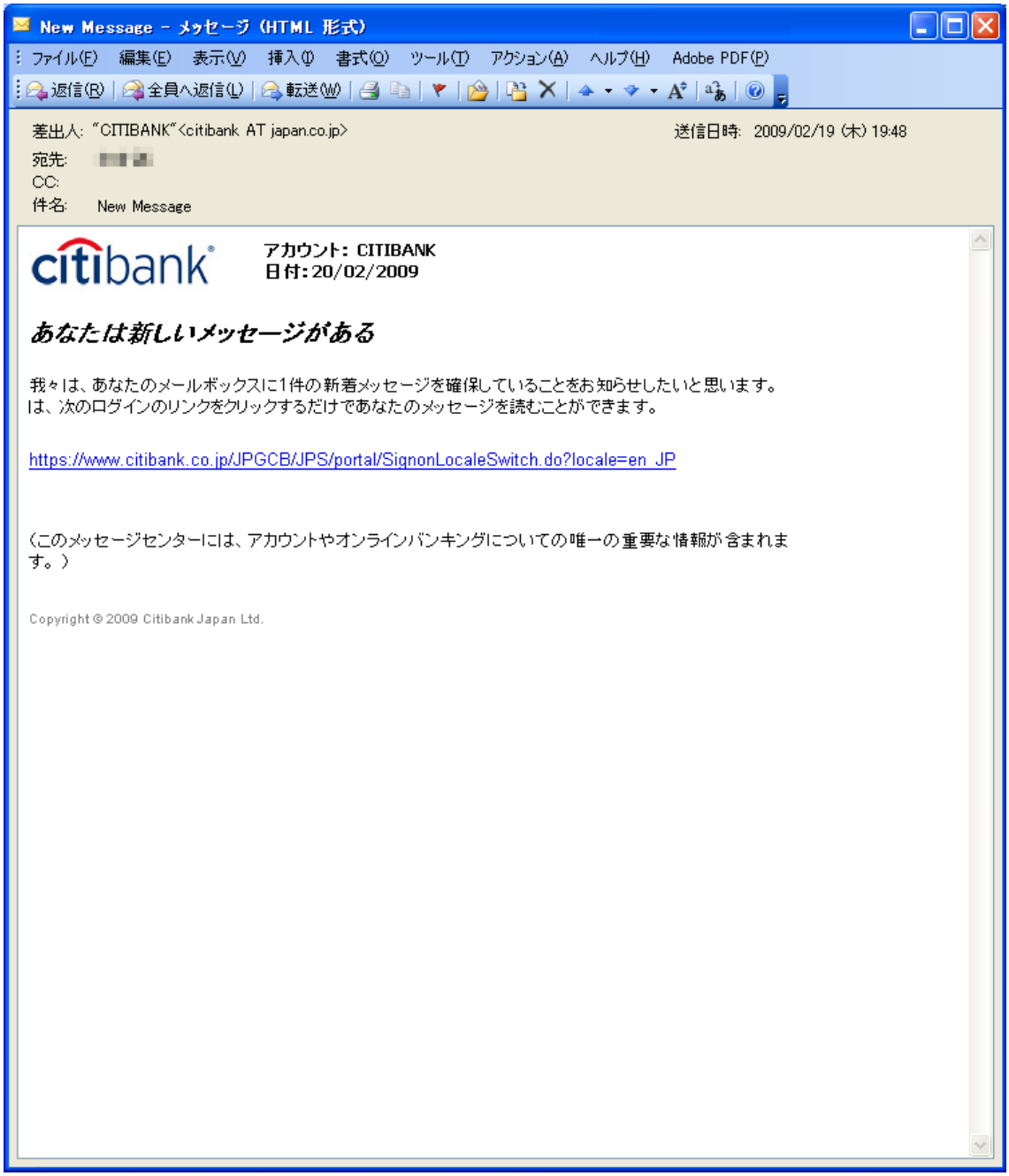
今月確認された「Yahoo!」をかたるフィッシングメールの一覧

1	差出人	<lkhjgdf3@yahoo.co.jp>
	件名	【重要なお知らせです】
	偽サイト URL	auctioniduser.vergilhost.info/yahoo.co.jp
2	差出人	Dfjeojls@yahoo.co.jp <dfjeojls@yahoo.co.jp>
	件名	【重要なお知らせです】
	偽サイト URL	acountidusers.hostscorpion.com/yahoo-auction.co.jp
3	差出人	<fnruofw@yahoo.co.jp>
	件名	【重要なお知らせです】
	偽サイト URL	useracountsin.50webs.com/yahoo.co.jp

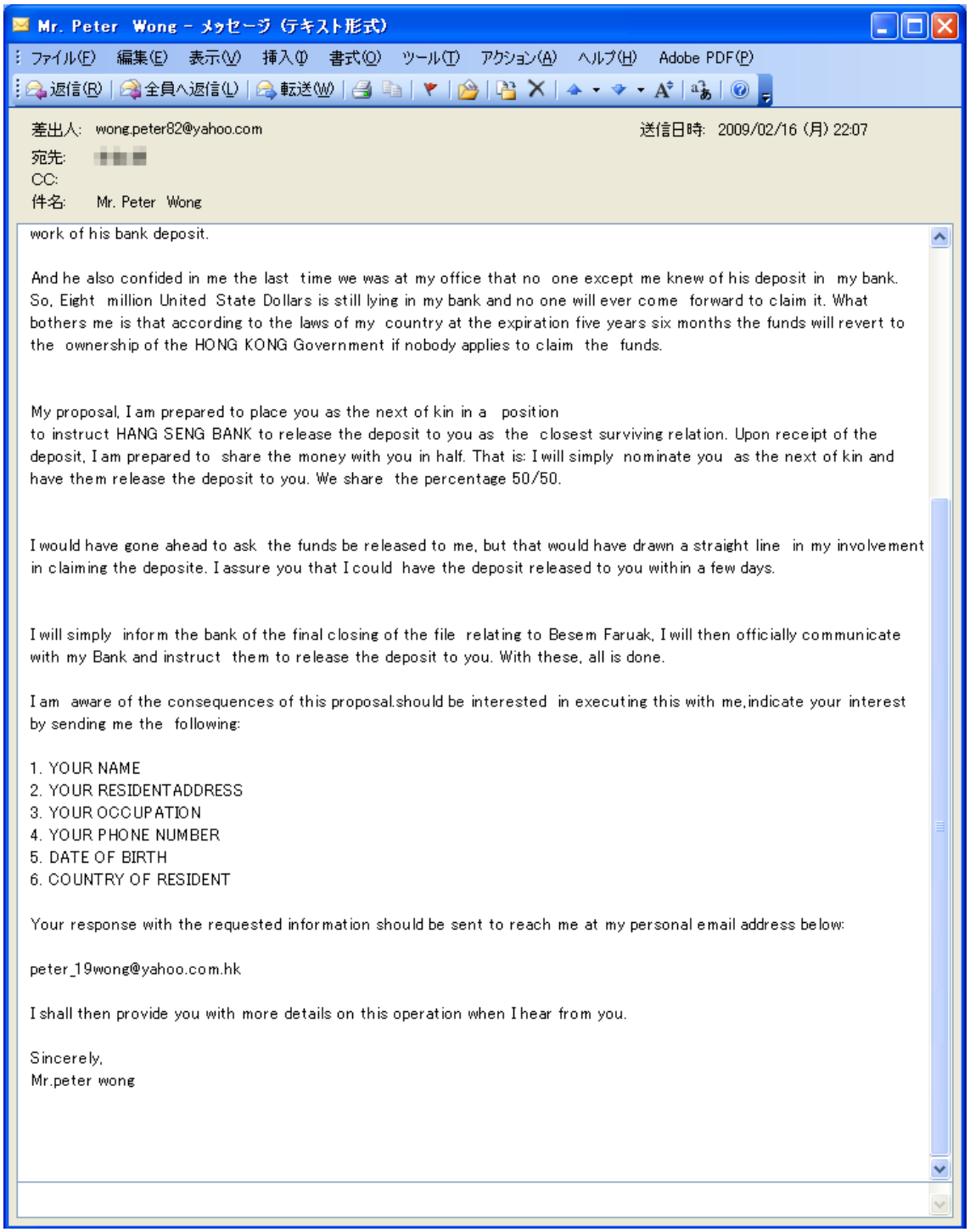
※メール本文の内容は、上記メール画像の内容と酷似しているため省略します。

※偽サイトには、悪意のあるソフトウェアが仕込まれている場合がありますので、不用意にアクセスしないようにしてください。

今月新たに「citibank」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「"CITIBANK"<citibank AT japan.co.jp>」、件名は「New Message」で、日本語で書かれた HTML 形式のメールになっています。メールは、ユーザに対し新着メッセージがあるとし、偽サイトへ誘導します。



今月新たに「Hang Seng Bank」の社員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「wong.peter82@yahoo.com」、件名は「Mr. Peter　Wong」で、英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、400 万ドルが入手可能とし、個人情報を送信させようとします。



Mr. Peter Wong - メッセージ (テキスト形式)

ファイル(F)　編集(E)　表示(V)　挿入(I)　書式(O)　ツール(T)　アクション(A)　ヘルプ(H)　Adobe PDF(P)

返信(R)　全員へ返信(L)　転送(W)

差出人: wong.peter82@yahoo.com　　送信日時: 2009/02/16 (月) 22:07

宛先: [redacted]

CC:

件名: Mr. Peter Wong

work of his bank deposit.

And he also confided in me the last time we was at my office that no one except me knew of his deposit in my bank. So, Eight million United State Dollars is still lying in my bank and no one will ever come forward to claim it. What bothers me is that according to the laws of my country at the expiration five years six months the funds will revert to the ownership of the HONG KONG Government if nobody applies to claim the funds.

My proposal, I am prepared to place you as the next of kin in a position
to instruct HANG SENG BANK to release the deposit to you as the closest surviving relation. Upon receipt of the deposit, I am prepared to share the money with you in half. That is: I will simply nominate you as the next of kin and have them release the deposit to you. We share the percentage 50/50.

I would have gone ahead to ask the funds be released to me, but that would have drawn a straight line in my involvement in claiming the deposite. I assure you that I could have the deposit released to you within a few days.

I will simply inform the bank of the final closing of the file relating to Besem Faruak, I will then officially communicate with my Bank and instruct them to release the deposit to you. With these, all is done.

I am aware of the consequences of this proposal.should be interested in executing this with me,indicate your interest by sending me the following:

1. YOUR NAME
2. YOUR RESIDENTADDRESS
3. YOUR OCCUPATION
4. YOUR PHONE NUMBER
5. DATE OF BIRTH
6. COUNTRY OF RESIDENT

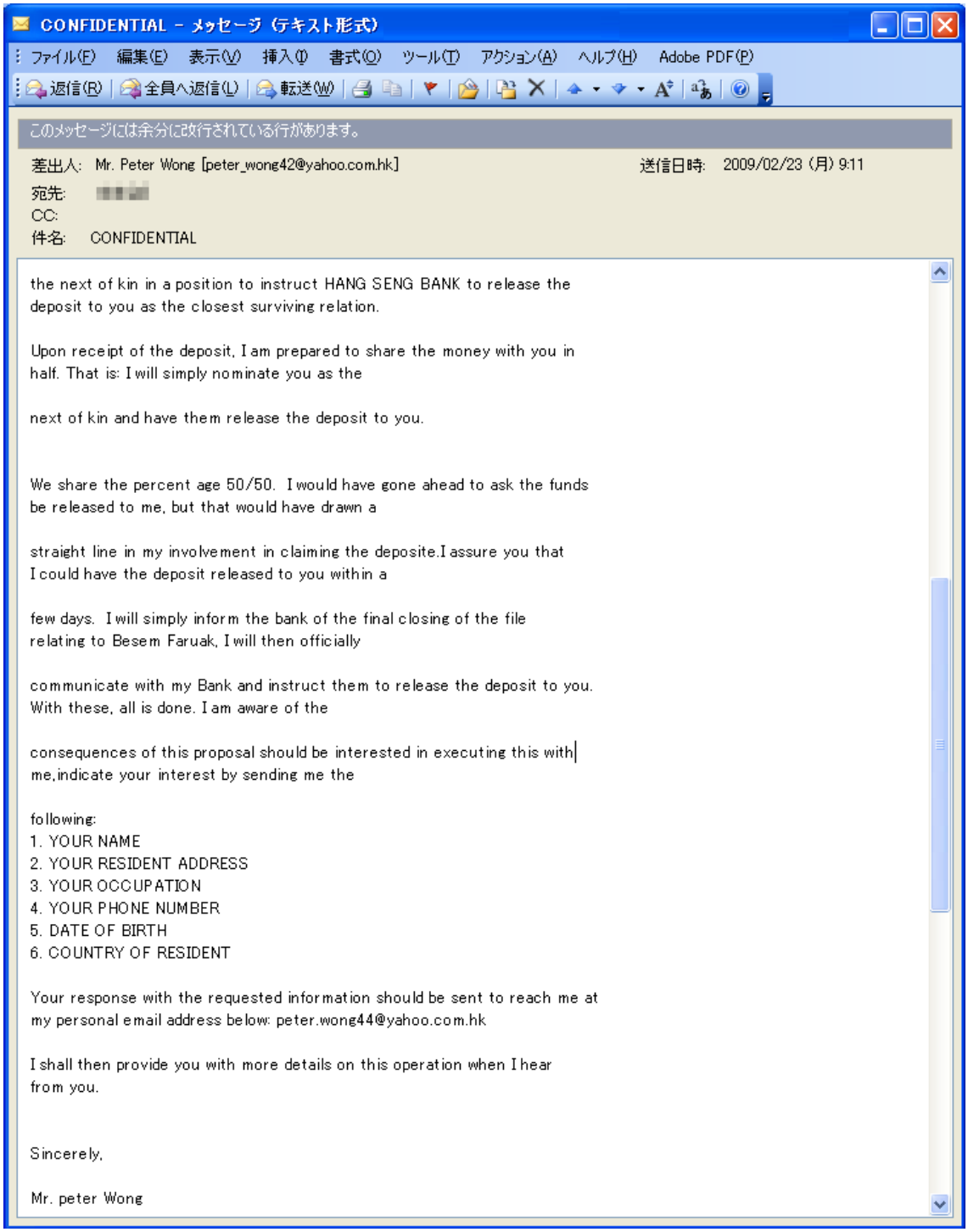
Your response with the requested information should be sent to reach me at my personal email address below:

peter_19wong@yahoo.com.hk

I shall then provide you with more details on this operation when I hear from you.

Sincerely,
Mr.peter wong

同じく「Hang Seng Bank」の社員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「Mr. Peter Wong [peter_wong42@yahoo.com.hk]」、件名は「CONFIDENTIAL」で、英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、400 万ドルが入手可能とし、個人情報を送信させようとします。



CONFIDENTIAL - メッセージ (テキスト形式)

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) アクション(A) ヘルプ(H) Adobe PDF(P)

返信(R) 全員へ返信(L) 転送(W)

このメッセージには余分に改行されている行があります。

差出人: Mr. Peter Wong [peter_wong42@yahoo.com.hk] 送信日時: 2009/02/23 (月) 9:11

宛先: [redacted]

CC:

件名: CONFIDENTIAL

the next of kin in a position to instruct HANG SENG BANK to release the deposit to you as the closest surviving relation.

Upon receipt of the deposit, I am prepared to share the money with you in half. That is: I will simply nominate you as the

next of kin and have them release the deposit to you.

We share the percent age 50/50. I would have gone ahead to ask the funds be released to me, but that would have drawn a

straight line in my involvement in claiming the deposite.I assure you that I could have the deposit released to you within a

few days. I will simply inform the bank of the final closing of the file relating to Besem Faruak, I will then officially

communicate with my Bank and instruct them to release the deposit to you. With these, all is done. I am aware of the

consequences of this proposal should be interested in executing this with me,indicate your interest by sending me the

following:

1. YOUR NAME
2. YOUR RESIDENT ADDRESS
3. YOUR OCCUPATION
4. YOUR PHONE NUMBER
5. DATE OF BIRTH
6. COUNTRY OF RESIDENT

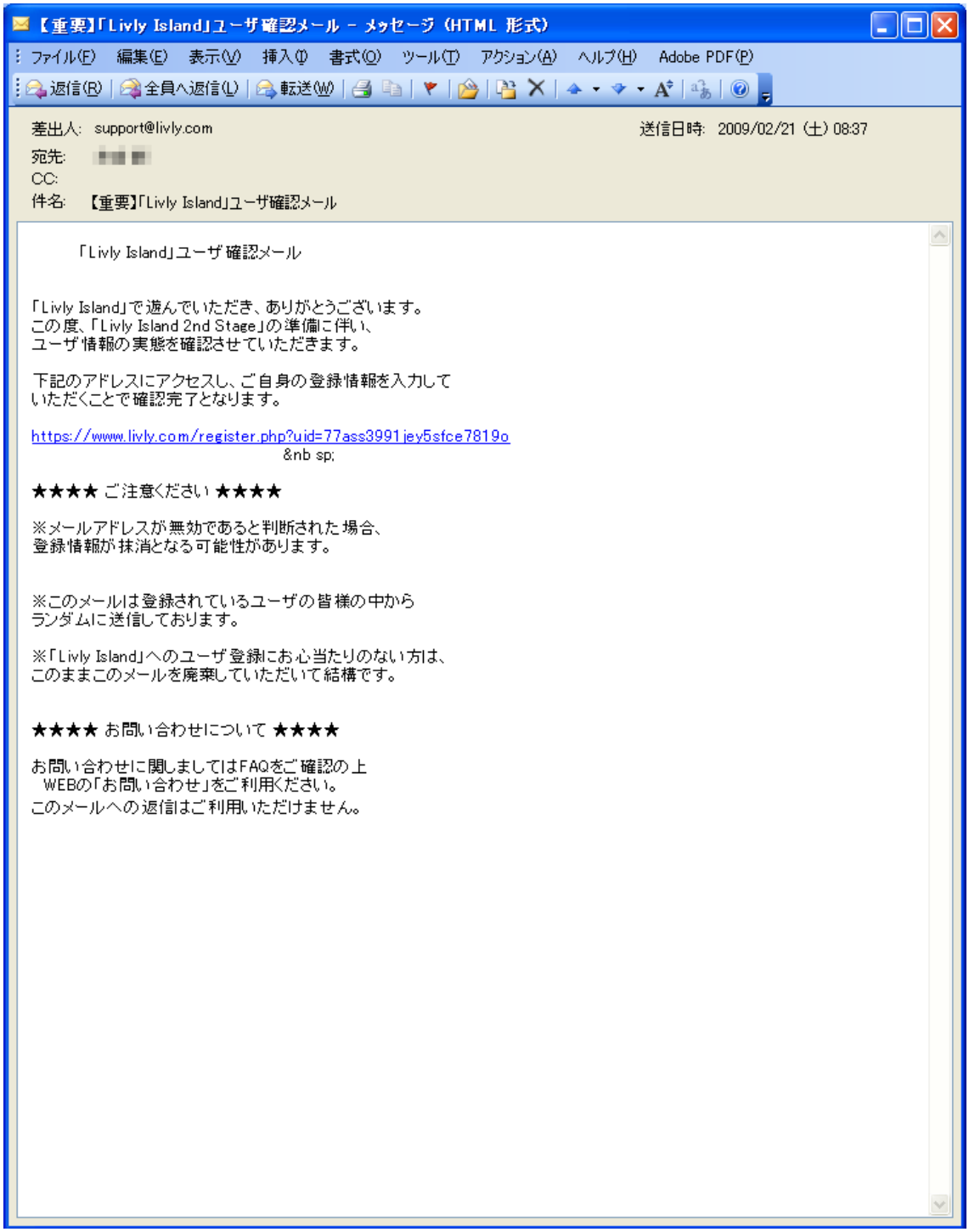
Your response with the requested information should be sent to reach me at my personal email address below: peter.wong44@yahoo.com.hk

I shall then provide you with more details on this operation when I hear from you.

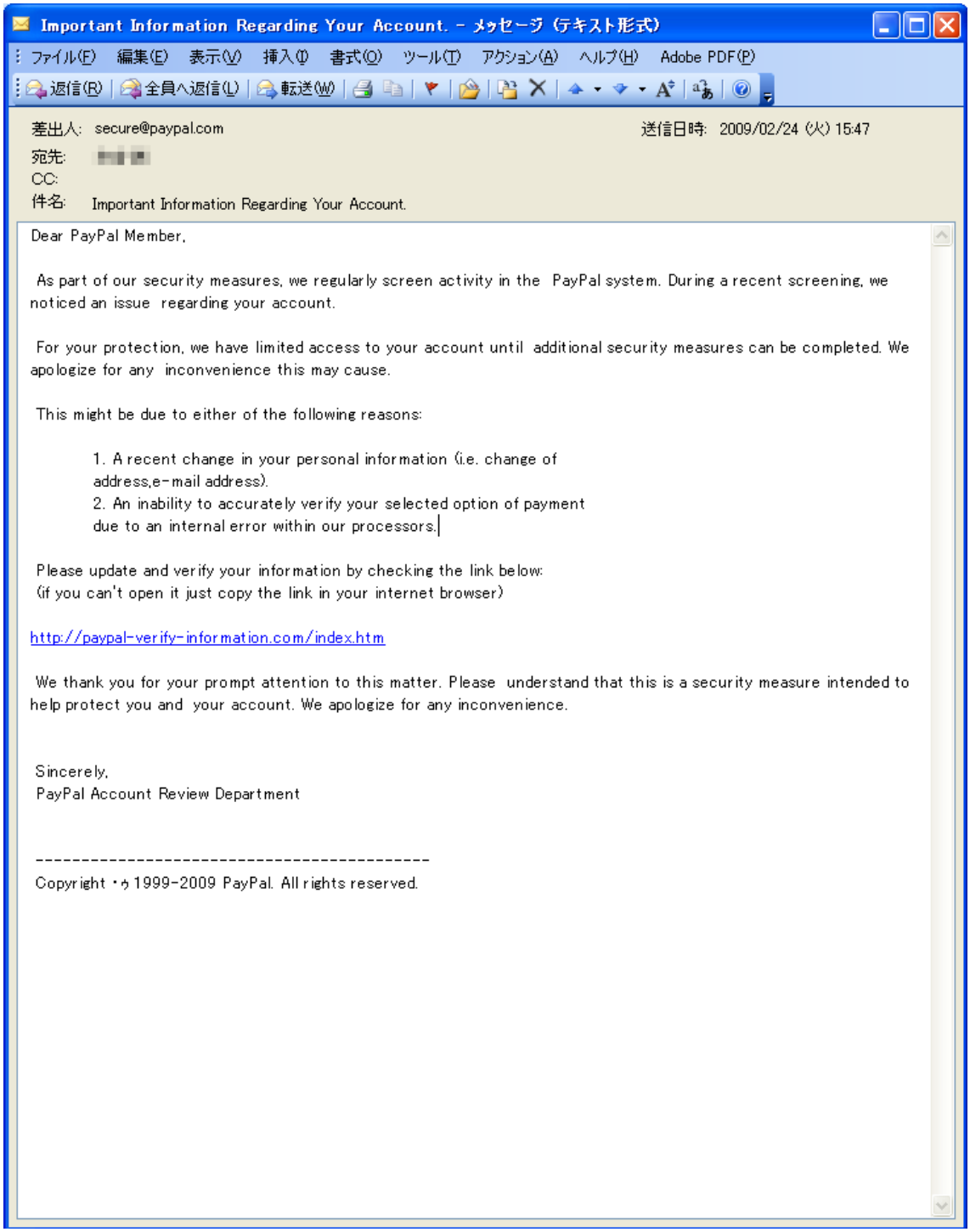
Sincerely,

Mr. peter Wong

今月新たに「Livly Island」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「support@livly.com」、件名は「【重要】「Livly Island」ユーザ確認メール」で、日本語で書かれた HTML 形式のメールになっています。メールは、ユーザ情報の実態を確認するとし、偽サイトへ誘導します。



今月新たに「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「secure@paypal.com」、件名は「Important Information Regarding Your Account.」で、英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、セキュリティの面での問題があり、情報の更新を促し、偽サイトへ誘導します。



差出人および件名、偽サイト URL の一覧を、下表に纏めます。

今月確認された「PayPal」をかたるフィッシングメールの一覧

1	差出人	Secure@paypal.com
	件名	Important Information Regarding Your Account.
	偽サイト URL	paypal-verify-information.com/index.htm
2	差出人	Service@paypal.com
	件名	Account Expired ! Please renew your account !
	偽サイト URL	classiccarcollectionkogan.com/files/liaz/index.php
3	差出人	PayPal security <accounts@paypal.com>
	件名	Confirm Yout Account
	偽サイト URL	paypal.update.your.information.limited.account.epersonalinformation.com/pp/index.htm

※メール本文の内容は、上記メール画像の内容と酷似しているため省略します。

※偽サイトには、悪意のあるソフトウェアが仕込まれている場合がありますので、不用意にアクセスしないようにしてください。

1.5. フィッシングサイトの動向

「Yahoo!」をかたるフィッシングサイトは、会員情報の更新を促し、個人情報を登録させようとします。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。

「citibank」をかたるフィッシングサイトは、新着メッセージがあるとし、個人情報を入力させようとします。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。

1.6. フィッシング関連の不正プログラム情報

MS08-067 の脆弱性を悪用したワームの亜種が確認されています。今月確認されたのは、「Conficker B++」です。基本的には既存のバージョンと同様ですが、新たに加えられた新機能により Conficker Cabal が行っている対策を無効化させてしまう可能性があるようです。

今後も同様な手段で新たなワームやウイルスが発生する可能性がありますので、CheckPC!のサイト http://www.checkpc.go.jp/等を参考に、セキュリティ対策を行うことが必要です。

1.7. その他の動向

QR コードを悪用したフィッシング攻撃が確認されています。この手口は、URL を意識せずカメラで撮影するだけでアクセスできるという特徴を悪用し、悪意あるユーザが、偽サイトや悪意あるサイトに飛ぶように設定された QR コードを既存の QR コードに重ねて貼り、個人情報を搾取しようとする手口です。対策として、QR コードを表示してアクセスさせる場合、URL も合わせて表示させるようにし、QR コードが貼り付けてあるサイトやチラシ等に記載されている情報と差異がないかチェックすることが重要です。

関連 URL：
QR コードを使ったフィッシングに気をつけろ！ 2009/02/21（slashdot.jp）
http://slashdot.jp/security/09/02/21/0116201.shtml

1.8. 総括

先月に引き続き、「Yahoo!」をかたるフィッシングが確認されています。メールそのものの数は減りましたが、先月と同様巧妙に作られた偽サイトへ誘導するので、引き続き注意が必要です。また、金融関連の企業をかたるフィッシングが多く確認されました。

昨今のフィッシングは、様々な手口を使い、ユーザのちょっとした油断を突いて個人情報を搾取しようと狙っています。引き続きフィッシングに対する注意を行うとともに、Microsoft 社のセキュリティ情報に対する迅速な対応を行う必要があります。