事務所ニュース News
2021.2
K-018

経営バイタルの強化書 KEIEI VITAL

長期休暇明けのメールには要注意！

不審なメールに気をつけて！

年末年始等の長期休暇の際には、詐欺を目的としたなりすまし迷惑メールやメッセージが広く送信されることがあります。

新型コロナウイルスに関して給付金や助成金についてのスパムメール、所得税の還付金の振込先等の入力を求めるメールやそのメールから国税庁ホームページになりすました偽のホームページへ誘導する事例も見つかっています。

フィッシング詐欺の事例や手口を知って被害に合わないように対策をとりましょう。

正しいWebページを確認しましょう！

1 長期休暇時期の注意点

年末年始やお盆等長期休暇の際には、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

メールやメッセージには電子メールだけではなく、ショートメッセージ（SMS）を使ったものも送信されています。

フィッシング詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動している「フィッシング対策協議会」の報告書によると、昨年12月のフィッシング報告件数（海外含む）は、32,171件に上っています※1。

同月のフィッシング詐欺に悪用されたブランド件数（海外含む）は、63件となっており、Amazonをかたるフィッシングの報告が多く、全体の50%を占めており、次いで三井住友カード、楽天、アプラス（新生銀行カード）、MyJCB をかたるフィッシングの報告も含めた上位5ブランドで、報告数全体の約86%を占めています。

宅配業者の不在通知を装ったSMSについては、引き続き多くの報告があり、このSMSの送信元の電話番号は、同様のSMSから不正なアプリ（マルウェア等）のインストールへ誘導された被害者のものである可能性が高いため、返信したり電話をかけないよう、注意や配慮が必要です。

2 フィッシング詐欺とは

総務省の「国民のための情報セキュリティサイト※2」によるとフィッシング詐欺とは、送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報（ユーザID、パスワードなど）といった重要な個人情報を盗み出す行為のことを言います。

最近では、電子メールの送信者名を詐称し、もっともらしい文面や緊急を装う文面にするだけでなく、接続先の偽のWebサイトを本物のWebサイトとほとんど区別がつかないように偽造するなど、どんどん手口が巧妙になって

裏面へ続く→

きており、ひと目ではフィッシング詐欺であるとは判別できないケースが増えてきています。
パソコンだけでなく、スマートフォンでも同様に電子メールからフィッシングサイトに誘導される手口が増えています。
フィッシング詐欺の手口としては以下のようなものが挙げられます。

●電子メールでフィッシングサイトに誘導

典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物のサイトにそっくりな偽サイトに利用者を誘導します。そこでクレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取ります。

●電子掲示板などの情報でフィッシングサイトに誘導

電子メールだけではなく、電子掲示板やSNSの投稿サイトに、URLを記載してアクセスさせ誘導する手口です。

●表示されているURLを本物のURLに見せかけてアクセスさせる手口

電子メールや電子掲示板に投稿されたURLを実在するURLに見間違えるような表示にすることで誘導する手口です。例えば、アルファベットの一文字の（オー）oを数字の0にしたり、アルファベットの大文字の（アイ）Iを小文字の（エル）lにしたりして、閲覧者が見間違えたり、信用させたりする手口もあります。

また、新型コロナウイルスに関して「新型コロナウイルス感染症緊急経済対策にかかる特別定額給付金の申請手続き」を名目とするスパムメールがあり、その後も「二回目特別定額給付金の特設サイトを開設しました。」などを件名とするメールを不特定多数にばらまき、受信者を偽の給付金オンライン申請サイトに誘導するものがありました。この事例では、誘導先である偽申請サイト上の「よくある質問」や「関連サイト」のリンクは正規サイトにつながっており、利用者が本物のサイトと錯覚してしまう作りになっていました。だまされて「オンライン申請」に進んでしまうと偽の情報入力ページが現れ、その先のページでも運転免許証などの本人確認書類をアップロードするよう求められ、一連の要求に応じてしまった場合、それらすべての情報がサイバー犯罪者の手に渡ってしまうことになります。

所得税の確定申告時期も近づき、国税庁でも「不審なメールや偽サイトにご注意ください」として注意喚起をしています※3。

3 フィッシング詐欺の対策

フィッシング詐欺の対策としては、以下の点に注意することが重要です※2。

●正しいWebページを確認する

金融機関のID・パスワードなどを入力するWebページにアクセスする場合は、金融機関から通知を受けているURLをWebブラウザに直接入力するか、普段利用しているWebブラウザのブックマークに金融機関の正しいURLを記録しておき、毎回そこからアクセスするようにするなど、常に真正のページにアクセスすることを心がけましょう。また、本物のWebサイトのドメイン名やURLを常に意識して、正しいWebサイトにアクセスしているかを確認する、アクセス先のサーバ証明書の内容を確認する、などの対応を心がけましょう。

●SSL通信を確認する

通常、インターネットバンキングへのログインやクレジットカード番号などの重要な情報の入力画面では、SSLという暗号化技術を利用します。重要な情報を入力するWebページでは、SSLが採用されているかを毎回確認するようにしましょう。SSLで通信が行われていることは、WebブラウザのURL表示部分（アドレスバー）や運営組織名が緑色の表示になっているか、鍵マークが表示されているか、などで確認できます。重要な情報の入力を求めるページで、SSLが使用されていない場合は、まずはフィッシング詐欺を疑いましょう。

●相手先を確認する

金融機関などの名前で送信されてきた電子メールの中で、通常と異なる手順を要求された場合には、内容を鵜呑みにせず、金融機関に確認することも必要です。フィッシング詐欺であるかどうか判断が難しい場合には、メールの送信元の会社に連絡をしてみるのもよいでしょう。ただし、電子メールに記載されている相手の情報は正しいものとは限らないため、電話をかける場合には必ず正規のWebサイトや金融機関からの郵便物などで連絡先の電話番号を調べるようにしてください。

※1「2020/12 フィッシング報告状況」（URL:https://www.antiphishing.jp/report/monthly/202012.html）
※2「国民のためのセキュリティサイト」（URL:https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/05.html）
※3「不審なメールや偽サイトにご注意ください」（URL:https://www.nta.go.jp/data/021127jouhou.pdf）