危険なフィッシング詐欺の見破り方

ラテラルフィッシングメール攻撃の脅威

- サイバー攻撃者はフィッシングメールを送付するために、正規ドメインに侵入
- 乗っ取られたメールアカウントが悪用されて、多くの既存のメール保護システムをバイパス
- 企業に固有の高度な標的型メッセージを悪用
- 正規のログインページを偽装したページへ誘導し、ユーザ名とパスワードを盗み出す
- 平日、勤務時間中にラテラルフィッシング攻撃を実施

セキュリティの意識向上が必要
多要素認証が必要
最新 IT セキュリティ情報のアップデート
過去の詐欺判別方法はあてにならない

年々巧妙化するフィッシング攻撃に対し、以前は有効であったセキュリティ対策の常識がすでに通用しなくなってきている危険があります。
昔なら日本語の表現がおかしなメールが多く、そうした古いフィッシング攻撃の見分け方を知っている人は、怪しいと思ったメールは開かないという常識で対処してきたのですが、最近の詐欺メールは本物と見分けがつかず、以前の常識が通用しません。
最新の詐欺攻撃の手法に関する情報がアップデートされておらず、IT リテラシーが低い人がマスコミなどを通じて対策方法を公開したため、かえって詐欺被害を助長してしまっているケースがあります。
たとえば、「世界一受けたい授業」という TV 番組でフィッシング詐欺にあうリスクを減らす方法は？という問題で、URL にカーソルを合わせ、ホップアップの同じ URL の文字列が表示されていれば本物のサイトに接続、違っていればフィッツシング詐欺だと解説していました。しかし、最近のフィッツシング詐欺は、偽のページによく似た URL のアドレスを使用しています。ユーザは、いちいち本物のアドレスなんて覚えていません。最初から、偽の URL を表示しておけばホップアップと同じになり、本物だという証拠にはなりません。
また、以前「ブラウザで鍵マークがつき、緑色の表示がされたサイトは 90% 安全」と発言した東大の准教授が話題になりましたが、https を使用するのは今では当たり前なので、偽の Web ページでも簡単に SSL 対応できます。これも、かえって安心だと思ってクリックさせるリスクを大きくしています。
フィッツシング詐欺の中でも、特に詐欺を見分けることが難しいのが、「ラテラルフィッシングメール」です。これは、正規ドメインから送られてくるため、偽のドメインから送られてくるメールを排除する検閲をシステム化している企業でもすり抜けて受信してしまいます。そして、すでに乗っ取られているため、なりすまして本物を偽装している場合、詐欺と疑う方が難しいです。
このように高度なフィッシング詐欺が横行している現状では、中途半端な詐欺の判別方法を信じて、かえってクリック率を上げてしまう危険があります。そのため、私たちは常に最新情報を入手し、可能な限り万全のセキュリティ対策を施し、全社社員が IT セキュリティのリテラシーを上げ続ける努力が必要です。