相次ぐフィッシング被害

ウェブメールサービスが標的に

今年4月から6月にかけて、組織が利用するウェブメールサービス（Office365、Active!Mail、Deepmail、Gmailなど）を狙ったフィッシング被害が相次いだ。7月以降も被害を確認しており、今後も引き続き注意が必要である。

独立行政法人情報処理推進機構（IPA）が確認したフィッシングの手口は次の通りである。

組織で利用しているウェブメールサービスのシステム管理者を装い、送信エラーやメールボックスがいっぱいであるなどと記載されたメールが、利用者宛てに送られる。利用者がメールに記載されているURLをクリックすると、ウェブメールサービスの正規のログインページを模した偽ログインページに誘導される。そのページで利用者がIDとパスワードを入力してしまうと、それらが詐取される。

IPAへの届け出情報では、偽ログインページは、ウェブメールサービスの英語版の標準デザインに酷似していた事例や、組織のロゴを使用した独自のデザインに模してある事例など、本物のログインページに似せてつくられていた。

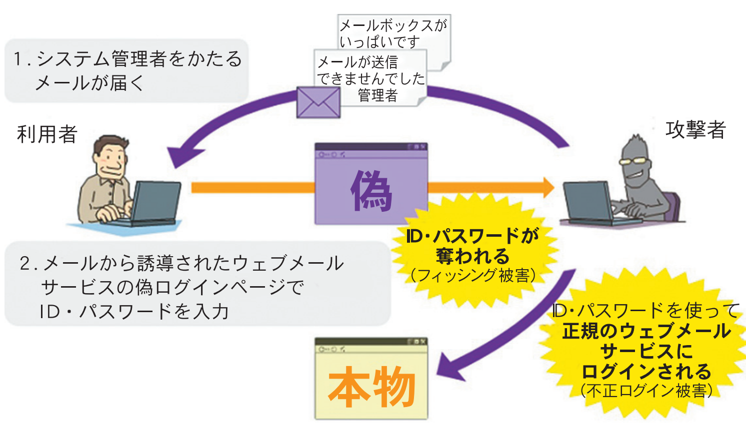
ID・パスワードを詐取されたことで、ウェブメールサービスに不正ログインされ、当該アカウントの設定を変更され、受信メールが外部転送されたり、当該アカウントが踏み台にされ、他組織へのフィッシングメールが送信されたりする。

判断に迷ったら確かな情報源で確認

■利用者の対策

フィッシングは、フィッシングメールが送られてくることから始まる。典型的なフィッシングの手口や、フィッシングメールの特徴といった基本を知ることにより、多くの場合でフィッシングメールかどうかを判断することが可能である。フィッシングの手口や対策などの具体的な内容については、フィッシング対策協議会にて提供されているガイドライン（https://www.antiphishing.jp/report/guideline/）を参考にしてほしい。

ウェブメールサービスを狙ったフィッシングの例



また、メールのリンク機能は便利だが、不審なサイトへの誘導にも使われる。そのため、メール内のリンクを安易にクリックしない習慣をつけてほしい。よく利用するサイトは、あらかじめお気に入りに登録しておき、それを使用してアクセスする。何もしていないのに突然送られてきたメールのリンクは、特に警戒してほしい。

昨今では、送信元や文面が本物らしく、とても巧妙で判別が難しい場合もある。そのため、これまで届いたことのない内容のメールやリンクのクリックを誘う内容のメールなどが届いた際に、それが本物かどうか判断に迷った場合は、確かな情報源を使って確認することを推奨する。メール本文に記載されている連絡先に連絡をしたり、届いたメールへ返信して問い合わせたりすることは、相手にこちらの情報を与えることになってしまうので避けてほしい。

■管理者の対策

誰しも、知らない危険を避けることは困難である。そのため、利用者啓発が必要である。手口・対策・事例などメールの真偽を判断するために必要な情報を、具体的に・継続的に・最新の情報で、利用者に提供してほしい。

しかし、手口や対策を知っていても、誰もが・いつでも・全てのメールを正しく見分けることは容易ではなく、以前より注意喚起を行っていたという組織でも被害が出ている。そのため、利用者啓発のみならず、2段階認証の利用、不審サイトへのアクセスの遮断、フィッシング対策機能を持つセキュリティーソフトの導入など、利用の目的や環境に応じたシステム的なセキュリティー対策の実施を検討してほしい。

（独立行政法人情報処理推進機構・江島将和）