

ウィリアム博士の今さら聞けない!!
IT
セキュリティ⑫



フォーバル取締役副社長
ウィリアム斉藤

「振り込め詐欺」と「ソーシャルエンジニアリング」は同じこと?!

「振り込め詐欺」は、当初「オレオレ詐欺」と呼ばれ、お年寄りの住む家を狙って電話をかけ、家族が交通事故を起こした、家族が電車の中で痴漢行為をはたらいた、などと架空の事故をネタに、今すぐお金を振り込めば示談で収めることができるなどと誘い、事実関係を把握させる隙を与えず示談金を騙し取るという手口です。

この「振り込め詐欺」と同じ成りすましによる心理戦略をコンピュータに置き換えたのが、「ソーシャルエンジニアリング」です。「ソーシャルエンジニアリング」では、情報システム管理者に成りすまし、ログオンIDとパスワードを聞き出す初歩的なものから、クレジットカード会社や銀行の関係者に成りすまして、カードの暗証番号を聞き出すまで、その手口は多種多様です。

情報を聞き出す手口も、「振り込め詐欺」と同じように電話を利用するものから、電子メールで返信させ、Webページのテキストフィールドに入力させるものまでさまざまです。「ソーシャルエンジニアリング」の場合も、冷静になってよく考えてみれば、システム管理者はネットワークに関するすべての権限を有しているので、ネット

ワークユーザーのパスワードを聞き出すこともなく、あらゆる処理を実行することが可能なのです。また、クレジットカード会社や銀行の担当者、カード利用者や預金者の暗証番号を聞き出すことがありえないことは、各クレジットカード会社や銀行が日頃から注意を呼びかけていることからわかります。

たとえ知識を持っていたとしても、巧みな話術により、パスワードや暗証番号を聞き出してしまうところ、が、「ソーシャルエンジニアリング」の恐ろしいところです。

最近の「ソーシャルエンジニアリング」の手法は、あらかじめ個人情報を入力しておき、氏名や住所、自宅の電話番号や家族構成、クレジットカードやキャッシュカードの利用履歴など、関係者しか知りえない情報を提示し、疑いの余地を与えないという手法が増え始めています。

「ソーシャルエンジニアリング」の手口は、メールやWebサイトを利用する以外に、電話による場合もあり、ファイアーウォールが万全でも、すべてを防げるというわけにはいきません。「ソーシャルエンジニアリング」により、たった一人のログオンIDとパ

スワードが流出することで、企業のネットワーク全体に大きなダメージを与えてしまう可能性も否定できません。

「ソーシャルエンジニアリング」に対抗していくためには、パソコン利用者一人ひとりが新たな手口を常に勉強し、セキュリティに対する意識を高く持ち続ける必要があります。企業においては、全社一丸となり、最新のセキュリティ情報を共有し、自宅パソコンを利用している人は、インターネットサイトなど、常に最新の情報を勉強していくという常日頃からの心がけがとて重要となるでしょう。

一年間、ご愛読いただき、ありがとうございました。四月号からは、「総合ITセキュリティ・サービス」を提供しているフォーバルクリエーティブの馬場重通上席テクニカルスペシャリストが担当させていただきます。最新情報を織り交ぜながらご案内していきます。ぜひ、ご期待ください。

ウィリアム斉藤

1971年ロサンゼルス生まれ。91年、I/O Software 設立。暗号や生体認証の専門家。米国防省IT・セキュアアドバイザー。日本では、総ソリジョン・カンパニー、フォーバルの副社長兼最高技術責任者を務める。「ウィリアム博士のボード教室」(<http://www.mysecurity.co.jp>)もご覧ください。