

第7回 ウォルマート(Wal-Mart)を偽った攻撃

小売業世界トップレベルの売上、規模をほこる企業である「ウォルマート」の顧客をターゲットにしたフィッシング攻撃の事例についてご紹介します。本事例では、ユーザ側にアカウント管理の不徹底という過失がある等の情報を通知し、不安がらせる事で、詐欺用のウェブサイトに誘導し、個人情報の入力を促しています。

- - - - 「APWG Phishing Activity Trends Report 2005年12月 日本語版」より - - - -

ウォルマート (Wal-Mart) を偽った攻撃

ウォルマートを偽った攻撃では、HTML形式のEメールによって、自分のログオン・アカウントが外部の者によって利用されたことを通知されます。そのEメールに記載されている情報は以下のようなものです。

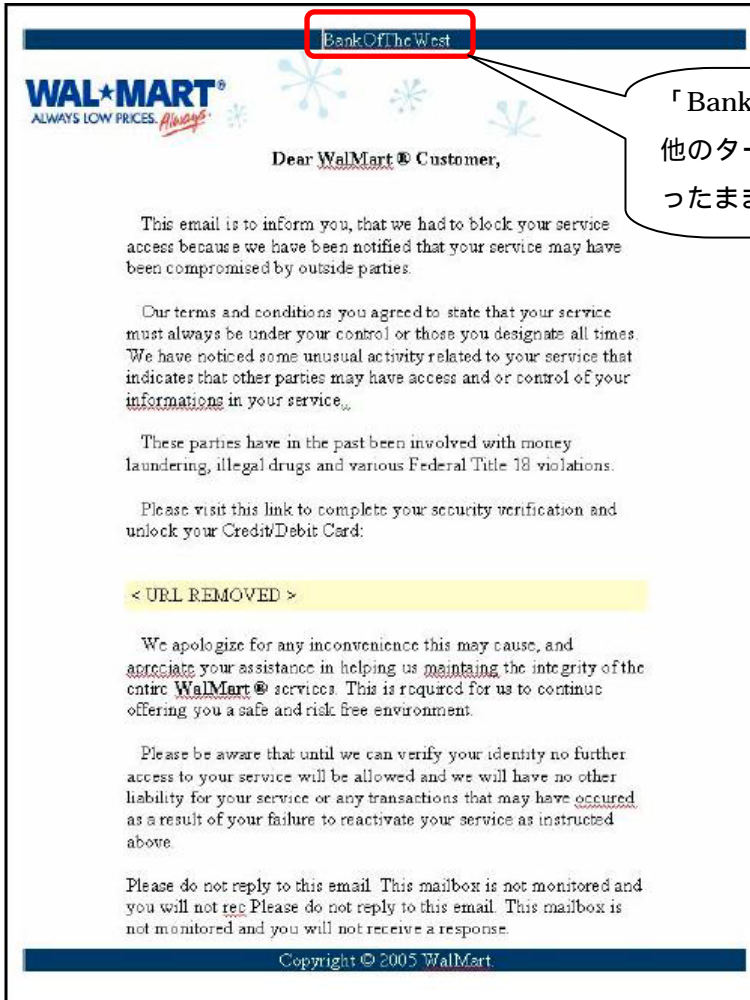
- ・ 不正使用の可能性のある為、サービスを停止している事
- ・ サービス利用規約で、自らにアカウント管理の責任があることに同意していた事
- ・ 資金洗浄や違法ドラッグなど、連邦制定法に抵触する事件を起こした犯人グループが情報を不正に利用する危険性がある事

まず、フィッシング詐欺犯はこれらを記載する事で、ユーザの不安を煽ります。その上で「以下のサイトにアクセスしてカード情報を入力し、セキュリティ確認を実施して下さい」というメッセージで詐欺用ウェブサイトへ誘導することにより、ユーザがEメール中のリンクをクリックする確率を上げていました。

Eメールのリンク先である米国内の詐欺用ウェブサイトでは、ユーザにウォルマートのウェブサイト(www.walmart.com)用のログオンIDを要求します。その後、クレジットカード情報、その他の詳細な個人情報の入力を要求するといったものでした。

なお、この詐欺用ウェブサイトは、過去に他のターゲットを狙ってフィッシング詐欺に使われた事があり、修整し忘れたのかページタイトルが「Wal-Mart」ではなく「Bank of the West」と表示されていました。下に実際にWal-Mart攻撃で使用された詐欺用ウェブサイトの画面がありますが、ページ上部にあるブルーのバナー部分を見ると「Bank of the West」と表示されているのがわかります。

～ フィッシング詐欺トピックス ～



「Bank of the West」と書かれている。
他のターゲットを狙った際の情報が残ったまま。