

セキュリティ事故の注意喚起～～フィッシングメール～～

フィッシングメールとは、銀行等の企業を装ってメールを送り、メールの受信者に、実在する企業の偽ホームページにアクセスさせて、そのページにおいてクレジットカード番号や ID・パスワード等を入力させるなどして、不正に個人情報等を入手する行為をいいます。

不正に入手した個人情報を悪用し、他人になりすまして買物をしたり、インターネットバンキングからお金を引き出したりするなど、大きな問題となっています。

2014年3月2日に下記（北島取締役宛）の三菱東京UFJ銀行を語るフィッシング詐欺メールが確認されましたので事例としてアップ致します。各自セキュリティ事故には十分ご注意下さいようお願い致します。

北島 昭夫

差出人: 三菱東京UFJ銀行 <hamu1570@yahoo.co.jp>
送信日時: 2014年3月2日日曜日 19:47
宛先: kitaguchi.wanze-647@q.vodafone.ne.jp
件名: 「三菱東京UFJ銀行」本人認証サービス

三菱東京UFJ銀行Eメール配信サービス

2014年「三菱東京UFJ銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。

以下のページより登録を続けてください。

https://entry11.bk.mufg.co.jp/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001

——Copyright(C)2014 The Bank of Tokyo-Mitsubishi UFJ,Ltd.All rights reserved——