滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R７年度 No.１５
今、注目のサイバーセキュリティに関する情報をお届けします。

社長や役員に成りすましたフィッシングメールに注意！

年初から、自組織の代表者や役員クラスに成りすまして、個人情報を窃取するフィッシングメールが県内の事業所に送付されています。御注意ください。

送付されたメール例

差出人：【当該企業名】〈第三者のメールアドレス〉
送信日時：２０２６年１月●日●曜日　●：●
宛先：【当該企業が実際に使用しているメールアドレス】
件名：【当該企業名】

社内連絡（しゃないれんらく）

お疲れ様でした・
メール受領後・最新の社内連絡網を作成の上・氏名・役職・個人連絡先電話番号を必ずご記載いただき・完成次第メールにてご返信ください・

【当該企業名】
【当該企業の代表者名】

この情報を提供いただいた事業所では、すぐに社内周知を図られており、被害は発生しておりません。

差出人に心当たりがなく、また、文面の日本語に違和感を感じたことや使われている漢字が簡体字であったことで代表者に確認されたところ、成りすましメールと分かったそうです。

この成りすましメールを解析すると、海外経由で送信されており、また、返信先(差出人)は、あたかも実在するような個人名のメールアドレスが設定されていますが、実際の返信先には、全く違うメールアドレスが設定されており、間違いなく個人情報の窃取を目的とした成りすましメールといえます。

当県警で展開しているセミナーでは、有名人や自組織の上司を騙るメールに注意していただくよう呼びかけているところ、こういった自組織の特別関係を狙ったメールには特に注意してください！！

～チェックポイント！～

○　心当たりのない送信元メールアドレスではないですか？
○　文章の内容や使われているフォントに違和感はないですか？
○　内容に違和感があれば、送信者に確認しましたか？
○　自社ホームページに代表者や役員を公開されている事業者は、ドメインや代表者の氏名等を無断で利用されやすいので、注意しましょう。

滋賀県警察本部　警備第一課　サイバー攻撃対策係　077-522-1231（代表）