ビジネス e メール詐欺: オンラインセキュリティ脅威の増加

2017 年 8 月

ビジネス e メール詐欺は、詐欺犯が、お客様の業務委託先、商品仕入先、債権者、またはお客様自身の代表取締役等の重役になりすまして、e メールを、お客様の支払担当部署に送ることをきっかけとして発生します。例えば、お客様の支払担当部署に届く e メールには、次のようなものがあります。

- ○ 代表取締役や CEO からと思われる e メールで、緊急の送金実行の依頼があります。このような依頼には、「この件については極秘で、誰にも話してはならない」といった追加の指示が、往々にしてなされます。
- ○ 商品仕入先からの e メールで、代金受取口座番号の変更に伴い、今後の商品代金の送金先を、新しい口座にするように通知されます。

いずれの場合にも、サイバー犯罪者は、送信元の e メールアドレスを、既知の e メールアドレスであるかのように偽装するため、このタイプの詐欺を認識するのは容易ではないことがあります。詐欺犯は、実際のユーザーの e メールアカウントに不正侵入し、そこから直接 e メールを送信することさえします。

お客様のご対応

お客様の支払担当部署および関連社員に、これらのタイプの詐欺についての理解、周知を促進し、警戒するよう注意を喚起することが最初のステップです。

さらに、次のような対策の導入を検討します。

- ○ E メールによる送金指図は、異なる通信手段（例：電話やインスタントメッセージ）で、e メール発信者に確認するなど、2 段階の確認プロセスを含む送金安全対策。
- ○ 返信は、常に登録されている連絡先に宛てて行うプロセス。
  - o E メールには、直接返信しない。
  - o E メールに記載されている電話番号やその他の情報を利用しない。

ビジネスメール詐欺の被害が疑われる場合には、至急、送金銀行にお問い合わせください。

本件につきましてご照会等ございましたら、以下までお問い合わせください。

香港上海銀行東京支店　グローバルキャッシュマネージメント部
電話: 03-5203-3247
E メール: jcsc@hsbc.co.jp