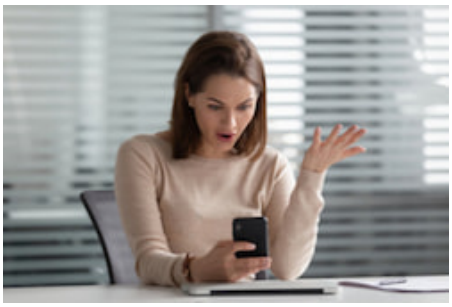
最新セキュリティマネジメント（第17回）

ビジネスメール詐欺の手口と対策が丸わかり

2022.10.24



2022年9月28日に独立行政法人情報処理推進機構（IPA）がビジネスメール詐欺対策のための特設ページを立ち上げた。BEC（Business E-mail Compromise）といわれるビジネスメール詐欺のパターンや対策、被害にあった場合の対応などを分かりやすくコンパクトにまとめたものだ。ビジネスメール詐欺の被害が広がる中で、しっかりと目を通しておくことをお勧めする。どんなページなのか概要を紹介しよう。

詐欺のパターンから被害の対応までを解説

特設ページではビジネス詐欺メールとして主な2つのパターンを取り上げている。「取引先との請求書を偽装」するタイプ1と、「経営者などになりすます」タイプ2だ。

タイプ1は攻撃者が取引先になりすます。偽の請求書などを送りつけて、攻撃者が用意した口座に振り込みをさせるのが目的だ。IPAが確認したところ、海外の企業と取引を行っている企業で見られるようだ。自社の担当者や海外子会社の担当者になりすますケースもあるという。

タイプ2は攻撃者が企業の経営者や幹部社員になりすまし、従業員に対して攻撃者が用意した口座に振り込みをするように指示するものだ。攻撃の対象となるのは企業内の財務や経理の担当者だ。「秘密の案件で相談がある」「相談したいことがあるので少し時間があるか」といった問い合わせを装う。電話のオレオレ詐欺と似た手口だ。

こうしたビジネスメール詐欺を防ぐにはどうしたら良いのか。特設ページでは対策として「普段と異なるメールに注意」「電信送金に関する社内規定の整備」「ウイルス・不正アクセス対策」の3つを挙げている。

さらに、ビジネスメール詐欺被害に遭ってしまった場合の対応についても解説している。送金のキャンセルや組み戻し手続き、状況把握や時系列の記録と証跡の収集、暫定対応と原因調査、そして社内外に向けた注意喚起とグループ会社などを含めた情報共有などだ。必ずしも資金が戻ってくるとは限らないが、送金後すぐに連絡することは有効な手段とされる。振込口座が海外の場合には、FBIやインターネット犯罪苦情センターのIC3への通報も有効だという。

ドラマ仕立ての字幕付きの動画コンテンツも… 続きを読む