2022 年 4 月 15 日

「ＬＴ会」会報第 22-5 号（総 230 号）

LT グループ

財務担当者を標的とするインターネット詐欺の手口と対策

インターネットの普及と発展に伴い、企業を狙うインターネット詐欺が次々と現れている。特に財務関係者が標的にされる詐欺事件は容易に察知できず、被害金額も巨額になることが多い。ここ数年に起きた典型的な事例を幾つかご紹介する。

事例 1：2016 年 3 月、広東省のある財政局の出納員が、公金 1786 万元を騙し取られた。
事例 2：2019 年 12 月、湖南省のある大企業の財務管理者が、検察職員を装った詐欺師に会社の資金 1919 万元を騙し取られた。
事例 3：2021 年 4 月、烏海のある会社の財務担当者が、上司を装った詐欺師に会社の資金 360 万元を騙し取られた。

こうした事件が起きると、企業の正常な経営に甚大な影響を受ける。このため、企業の日常的な管理において、従業員(特に財務関係者)のネットワークセキュリティ対策意識の強化を図ることが重要である。今回の会報では、企業に対するネット詐欺の主な手口や対策をご紹介する。業務運営のご参考にしていただきたい。

一、 企業を標的とするネットワーク詐欺の主な手口

1. 詐欺師が上司を装って、偽の状況をでっちあげ、財務担当者を信用させたうえ財務担当者を騙して送金させる。
2. 詐欺師が木馬ウイルスを使って財務担当者のパソコンや携帯電話を操作し、企業の銀行口座のパスワード等の情報を盗み資金を騙し取る。
3. 詐欺師が企業の従業員の携帯電話の連絡先を盗み出し、組織構造や人員構成などの情報を把握したうえ、財務担当者宛にメールなどで「送金指示」を間違いなく送る。

二、 企業を標的とするインターネット詐欺への防止策

1. 企業制度・規定の管理

まず企業自身の企業制度・規定を整備、確立し、以下の第 2～6 条の措置に従って実行する。次に企業制度・規定の周知を徹底し、制度・規定の内容を明確にし、適切な取り扱いを徹底する。最後に内部統制監査によって社内制度・規定を改善し、規範化する。

2. 企業の資金管理

(1) ネットバンクのキーに 3 段階の支払権限を設定し、出納が 1 段階として支払いの入力をし、財務が 2 段階として審査をし、最後に総経理が 3 段階として承認する。出納、財務及び総経理は無断で第三者にネットバンクを操作させてはならず、ネットバンクのパスワードは定期的に変更する。

(2) 財務は一定額以上の金額の支払いをする前に、必ず上司の審査と承認を経るようにし、送金口座や金額等の取引条件を無断で変更してはならない。一日の支払業務が完了したら、

当日のネットバンク取引明細を印刷して、承認済の原始証憑を添えて総経理に提出して照合を行う。総経理は照合後に署名または捺印し、財務部門がこれを保管する。

3. 情報セキュリティ管理の徹底

(1) パソコンは定期的にウイルスを駆除し、出所不明のリンクやソフトはクリックせず、定期的に重要資料のバックアップを取るようにする。

(2) 銀行の USB キーは使用後、直ちに抜いて、適切に保管する。

(3) 支払認証コードを第三者に教えない。

(4) 顧客のメールアドレスや口座に無断変更がないか定期的にチェックし、個人情報の漏洩を防止する。

4. 企業コミュニケーションの管理

(1) 定期的に通信詐欺防止の周知、トレーニングを行い、従業員に国家詐欺防止センターのアプリをダウンロードさせるようにする。

(2) 上司から新しい口座やメールなどで送金指示を受け取った場合、まず複数の関係者に確認し、規定どおりの送金承認プロセスを経るようにする。

5. 送金先のマスター登録・管理

(1) 送金先は予めマスター登録を行い、マスター登録先の変更・新規登録があれば、必ず社内の承認プロセスを経て、登録を行うようにする。

(2) 財務担当者が送金を行う時、上司の承認があっても必ずマスター登録先をチェックし、登録がない、または登録内容と送金内容に不一致があった場合、送金を拒否する体制と社内制度の構築も重要である。

6. 不定期的に内部統制監査の実施

不定期に内部統制監査を実施し、現金棚卸や銀行照合表、銀行出入金記録をチェックすることで、企業の管理、制度、資金の安全上の問題を発見し、リスク管理意識を高め、インターネット詐欺を未然防止する。

以 上