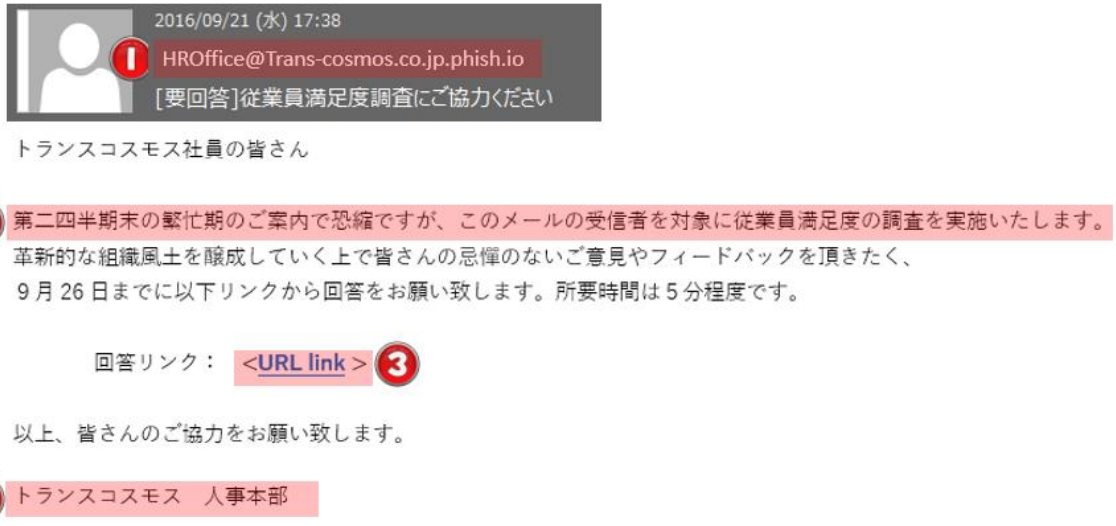
フィッシングメールとは?

フィッシングメール（なりすましメール）とは、ターゲットとなる個人に対して信頼される主体（企業、政府団体など）になりすまし、ユーザー名、パスワード、銀行口座情報、クレジットカード情報、その他個人・組織の経済的価値がある情報を盗み取るための攻撃です。個人に対するコンタクトの多くはメールや電話によって行われます。搾取された情報は個人になりすましたログインに悪用され、結果経済的な損失に繋がります。**昨今被害が相次いでいる標的型メール攻撃においても、フィッシングメールと不正プログラムが含まれる添付ファイルが組み合わせられたり、あるいはメール本文に添付した URL からウィルス感染を引き起こす Web サイトへの誘導が試みられるため、厳重な注意が必要となっています。**

今回、ソーシャルエンジニアリングテストの一環として送付させていただきましたフィッシングメールについての解説を以下に記します。



フィッシングメールを見分けるための方法

1	メールが企業のアドレスではない一般的なアドレス、または自社のメールドメインに似ているが異なるアドレスから送付されている
2	第二四半期末の従業員満足度調査を実施すると記載されているが、通常こういったことが行われていない場合、周りの方にも同様のメールが送付されているか確認する。
3	調査のためにリンクをクリックすることと記載されているが、URL が自社のドメイン(例：xx.transcosmos.co.jp など)であることを確認する。特に外部のアドレスを参照している場合に注意し、周りの同僚にも確認する。
4	当調査の人事本部の発信となっているが、特に日本企業の場合であれば担当者名を付けるのが一般的である。通常こういったメールが人事本部から送付されるか、周りの同僚に確認をする

フィッシングメールからあなたを守るための最良のプラクティス

1	どのようなメールでのリクエストであっても、個人情報や機密情報をメールで送信しない 少しでも不審な点があれば、同僚や発信元に確認を行う
2	頼んでいない、あるいは自分に関係がないメールのリンクや添付ファイルを開かない
3	リンクをクリックせず、カーソルをリンクに重ね、信頼できるアドレスかを確認する。 （特に、外部の URL になっている場合、要注意）

Antuit サイバーセキュリティチーム