Guide de sensibilisation aux fraudes

L'actualité sanitaire modifie probablement le fonctionnement habituel de votre entreprise. Ces conditions particulières engendrent un contexte encore plus favorable pour des fraudeurs qui envisageraient de tirer profit de la situation actuelle. Pour vous aider à prendre les précautions utiles, nous vous proposons ce guide de sensibilisation aux principales fraudes.

'Vous être utile' reste notre priorité.

Banque de Tahiti

Fraude au président

Le fraudeur contacte un salarié par email ou téléphone. Il se fait passer pour le président de la société et lui demande d'effectuer une opération généralement exceptionnelle.

- Les signaux d'alerte sont les suivants:
  - L'opération est qualifiée d'urgente
  - L'opération est qualifiée de confidentielle
  - La personne se faisant passer pour le président utilise la flatterie ('je sais que je peux compter sur vous')
  - La personne se faisant passer pour le président utilise l'intimidation ('c'est un ordre')

Banque de Tahiti

Fraude au technicien

Une personne se faisant passer pour un technicien contacte un salarié prétendument pour l'assister sur son application bancaire et parvient à réaliser des virements frauduleux.

- Les signaux d'alerte sont les suivants:
  - Une information sur un changement de solution bancaire, une migration technique, etc.
  - Une demande de prise en main à distance sur le PC
  - Une invitation à faire un test de virement
  - Une invitation à communiquer un code d'identification ou un mot de passe
  - Une invitation à saisir des informations dans une interface que vous ne connaissez pas

Banque de Tahiti

Fraude au fournisseur

Le fraudeur contacte un salarié par email, téléphone ou courrier pour l'informer d'un changement de coordonnées bancaires.

Lors de toute demande de modification de coordonnées bancaires, vérifiez l'identité de votre interlocuteur en le contactant sur des coordonnées sûres, que vous avez déjà utilisé précédemment pour communiquer avec lui.

Par ailleurs, soyez particulièrement vigilant concernant les comptes domiciliés à l'étranger (c'est-à-dire dont l'IBAN ne commence pas par 'FR').

Banque de Tahiti

Falsification d’email

Le fraudeur utilise une adresse email ressemblant à une adresse connue pour entrer en communication avec des salariés ou des clients.

Le signal d’alerte est principalement le nom de domaine utilisé, qui ressemble à celui de l’entreprise mais avec quelques différences, par exemple: une faute dans l’ordre des caractères, un sous-domaine ou encore une extension peu usuelle.

Banque de Tahiti

‘Phishing’

Un salarié reçoit un email semblant provenir de l’établissement bancaire de votre entreprise ou de tout autre opérateur avec lequel vous interagissez habituellement (administration, fournisseur d’électricité, etc.). Le lien contenu dans l’email dirige le salarié vers une page frauduleuse dans laquelle il lui est demandé de saisir des informations telles que identifiants, mots de passe ou encore numéro de carte bancaire.

- Les signaux d’alerte sont les suivants:
  - La présence d’un lien dans l’email
  - Les fautes d’orthographe dans l’email
  - L’adresse de l’email
  - La demande de saisie d’information

Banque de Tahiti

‘Malware’

Un salarié reçoit un email contenant généralement un lien ou un document. En cliquant sur le lien ou en ouvrant le document, le salarié installe à son insu un logiciel malveillant (‘malware’) sur le réseau de votre entreprise.

- Les signaux d’alerte sont les suivants:
  - Un expéditeur inconnu ou une adresse email suspecte
  - La présence d’un lien ou d’une pièce jointe dans l’email
  - Les fautes d’orthographe dans l’email
  - La déformation du logo de la société prétendument émettrice

Banque de Tahiti