Ensemble pour lutter contre la fraude

HSBC

Contexte

Retour sur les fraudes qui touchent les entreprises, quelles que soient leurs tailles, et sur les moyens de s'en prémunir.

550 Millions
d'euros de perte cumulée.

Plusieurs milliers
de sociétés victimes implantées en France et/ou filiales domiciliées sur l'Union Européenne.

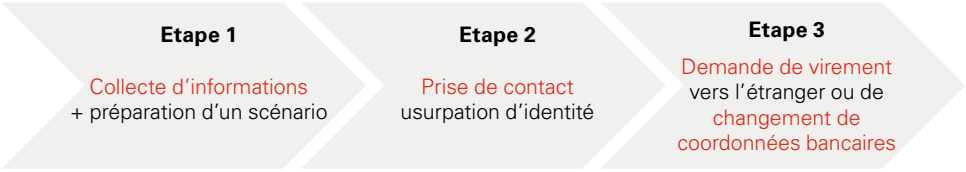
Ce sont les chiffres de la fraude par ingénierie sociale, également appelée FOVI (Faux Ordres de Virements Internationaux) en cumul depuis 2010, communiqués par l'OCRGDF (Office Central pour la Répression de la Grande Délinquance Financière).

La fraude par ingénierie sociale

Les fraudes au « président » et fraudes aux changements de coordonnées bancaires, sont celles qui font le plus de victimes.

L'ingénierie sociale : Qu'est-ce que c'est ?

La manipulation d'un interlocuteur au sein d'une entreprise pour qu'il effectue une transaction bancaire.



La première étape : la collecte d'informations et la préparation d'un scénario

Elle consiste pour le fraudeur à collecter l'ensemble des informations nécessaires à la réalisation de la fraude (organigrammes, activités, acteurs clés, adresses mail…). Ces informations sont récupérées sur Internet ou frauduleusement auprès de l'entreprise (phishing et appels téléphoniques notamment). A partir des informations récupérées, un scénario est élaboré.

La seconde étape : la prise de contact

- L'escroc met en confiance son interlocuteur au sein de l'entreprise, en utilisant des adresses mails très proches ou identiques aux originales, et/ou des numéros de téléphones situés dans la même zone géographique.
- Il peut utiliser divers moyens de persuasion pour contraindre son interlocuteur au sein de l'entreprise : flatterie, perspective d'ascension sociale, mais peut aussi, à l'inverse, utiliser la menace de sanctions si la personne ciblée est réticente.

La dernière étape : la demande de virement vers l'étranger ou de changement de coordonnées bancaires

- Les demandes de virements revêtent toujours un caractère exceptionnel et urgent. Elles sont souvent sollicitées la veille de week-ends ou de jours fériés afin de réduire les possibilités de contrôle.
- Le bénéficiaire du virement est presque toujours domicilié à l'étranger.

Les principales formes d'ingénierie sociale

Fraude « au président » :
Demande urgente et confidentielle de virement vers un compte étranger par une personne qui se présente comme occupant un poste important au sein de l'entreprise, ou par une personne qui se présente comme représentant d'un cabinet d'avocat ou d'audit mandaté par l'entreprise.

Exemple récurrent : virement confidentiel dans le cadre d'une OPA sur une société étrangère.

Fraude au changement de coordonnées bancaires :
Usurpation de l'identité d'un fournisseur ou bailleur de l'entreprise pour demander le changement de coordonnées bancaires afin de détourner le paiement des prestations ou loyers à son profit.
L'adresse e-mail a des caractéristiques très proches ou identiques à celles de l'interlocuteur habituel de la personne au sein de l'entreprise qui va procéder aux changements de coordonnées bancaires.

Fraude à l'informatique (notamment virements tests SEPA) **:**
L'escroc se fait passer pour un prestataire de l'entreprise, voire de la banque, et demande l'exécution d'un « virement test » vers un compte étranger. Il peut aussi demander l'installation de logiciels qui permettront de récupérer des informations de sécurité ou de pirater le système informatique de l'entreprise.

Protégez votre entreprise contre l'ingénierie sociale

Il est possible de protéger votre entreprise contre ce type d'attaques avec des mesures simples et faciles à mettre en place.

- Maîtrisez la diffusion d'informations concernant l'entreprise et ne communiquez pas d'éléments susceptibles de faciliter le travail des fraudeurs.
- Sensibilisez vos collaborateurs aux risques de fraude.
- Définissez et respectez une procédure interne pour l'exécution des virements.
- Séparez les pouvoirs relatifs aux applications de banque à distance : évitez que l'un des utilisateurs au sein de votre entreprise puisse tout faire (ajouter un compte bénéficiaire, saisir une opération, la valider).
- Soyez en veille sur les escroqueries aux entreprises : les modes opératoires des fraudeurs évoluent sans cesse.
- Privilégiez les flux émis via nos canaux électroniques aux flux papiers : les flux faxés sont moins sécurisés que les flux électroniques pour lesquels des contrôles complémentaires sont disponibles (Digipass, séparation des pouvoirs.....).
- Prenez le temps au sein de votre entreprise d'effectuer les vérifications nécessaires avant de valider une transaction.

- **Est-ce bien mon fournisseur qui m'adresse ses nouvelles coordonnées bancaires domiciliées à l'étranger ?**
- **Cette demande de virement me parait-elle normale ou habituelle ?**
  Dans le cas contraire, refusez d'effectuer l'opération, résistez à la pression et communiquez sans délai auprès de votre hiérarchie.

La cybercriminalité

La cybercriminalité est apparue avec Internet et s'est depuis considérablement sophistiquée et amplifiée en s'adaptant aux nouvelles technologies et innovations.

La cybercriminalité : qu'est-ce que c'est ?

Il s'agit de cyberattaques visant à récupérer de l'information dans les systèmes informatiques des entreprises, notamment les identifiants de connexion aux outils de banque à distance, dans le but de détourner des fonds en réalisant des virements.

Les principales formes de cybercriminalité

Le phishing
Il consiste, en se faisant passer pour une entreprise, une banque ou une institution connue, à vous demander par email de fournir des données confidentielles, ou diffuser un malware sur le poste informatique.

Le malware
Il s'agit d'un type de virus développé à des fins malveillantes et introduit sur un ordinateur à l'insu de son utilisateur par le biais d'un email avec pièce jointe, ou du téléchargement d'un document ou d'un logiciel depuis un site internet piraté. L'objectif est de récupérer directement auprès des entreprises des données personnelles souvent confidentielles, permettant au fraudeur de vous escroquer, ou de vous orienter vers un site frauduleux lors de votre connexion à votre banque à distance.

Le ransomware
Il s'agit d'un malware dont le but est de chiffrer des données afin de demander à leur propriétaire d'envoyer de l'argent (rançon) en échange de la clé qui permettra de les déchiffrer. Il peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange de la rançon demandée. A noter que le paiement se fait bien souvent en monnaie virtuelle (exemple : bitcoin).

Exemple récurrent : Envoi d'un e-mail de relance concernant une facture impayée. L'e-mail semble contenir une facture en pièce jointe. En cliquant sur la pièce jointe, un malware s'installe sur le poste de travail.

Protégez votre entreprise contre la cybercriminalité

- Soyez vigilants lorsque vous envoyez ou recevez un e-mail :
  - Ne répondez jamais à un email sollicitant la communication d'informations personnelles. En particulier, HSBC ne vous demandera jamais d'informations confidentielles par e-mail.
  - Ne cliquez pas sur les liens et pièces jointes contenus dans un email dont vous ne connaissez pas l'expéditeur
  - Privilégiez les messageries sécurisées comme celles d'Elys PC ou celles équipées de protocole de sécurité type TLS (Transport Layer Security) pour communiquer avec votre banque
- Protégez votre parc informatique :
  - Disposez d'un système d'exploitation, d'un antivirus et d'un pare-feu à jour
  - Installez en complément Trusteer (pour les clients Elys PC) ou Webroot (pour les clients HSBC*net*), logiciels offerts par HSBC, et spécialisés contre les malwares bancaires

  Trusteer
- A propos de vos applications de communication bancaire HSBC :
  - Connectez-vous régulièrement à votre application de banque à distance, vérifiez la date de dernière connexion, votre relevé de compte et déconnectez-vous via le bouton « déconnexion »
  - Ne partagez jamais vos identifiants de connexion et conservez-les dans un endroit sécurisé (données strictement confidentielles)
  - Séparez les pouvoirs des utilisateurs : évitez que l'un des utilisateurs puisse tout faire (ajouter un compte bénéficiaire, saisir une opération, la valider).

Comment HSBC France vous accompagne

HSBC France prend très au sérieux ces menaces et a mis en place un programme de prévention de la fraude, composé notamment :

- De campagnes de communication sur la fraude
- De conférences clients en partenariat avec les services de Police
- De formations régulières de nos collaborateurs pour qu'ils puissent vous accompagner au quotidien
- D'applications bancaires toujours plus sécurisées

En savoir plus sur www.hsbc.fr/securite

Que faire en cas de fraude ?

1. **N'attendez pas, agissez sans délai en nous contactant (au choix) :**

- **Votre interlocuteur habituel ou votre agence HSBC**

- **HSBC Relations Clients Entreprises**

0810 83 84 85 Service 0,05 € / min + prix appel

+33 1 55 69 74 53 depuis l'étranger.
Du lundi au vendredi de 8h30 à 18h.

2. **Effectuez en parallèle un dépôt de plainte qui entraîne l'action officielle d'un service de Police**

Pour en savoir plus :

Contactez votre chargé d'affaires habituel

Appelez le **0810 83 84 85** Service 0,05 € / min + prix appel

Du lundi au vendredi de 8h30 à 18h00.

Connectez-vous sur www.business.hsbc.fr

Suivez HSBC Commercial Banking

HSBC France - Société Anonyme au capital de 337 189 135 euros - SIREN 775 670 284 RCS Paris
Siège social : 103, avenue des Champs-Elysées - 75008 Paris
Banque et intermédiaire en assurance immatriculé auprès de l'ORIAS
(Organisme pour le Registre des Intermédiaires en Assurance - www.orias.fr) sous le n° 07 005 894.
Ref : 16.000.31 - 12/2017