UNIVERSWIFTNET

Echanges, discussions et pensées libres

L'escroquerie aux faux virements

~~~

Une menace réelle au scénario bien ficelé

Atelier

Date : 15 mars 2016

PUBLIC
~~~

L'escroquerie aux faux virements

Une menace réelle au scénario bien ficelé…

Ingénierie sociale

Cybercriminalité

Phishing & Malwares

Fraude au changement de coordonnées bancaires

Fraude Président

Manipulations psychologiques

Intimidations

Présentation des intervenants

Christophe LECOMTE

Adjoint du Directeur de la Division Trésorerie
et Financements Intra-Groupe

Céline PLACHOT

Chef de Produits Banque à Distance Entreprises

Yves DESTREBECQ

Responsable Prévention contre la Fraude

Ordre du jour

- La fraude aujourd'hui
- Focus sur l'ingénierie sociale
- Focus sur la cybercriminalité
- Comment se prémunir contre ces attaques ?

1. La fraude aujourd'hui

Le contexte actuel

Fraudeurs de mieux en mieux organisés

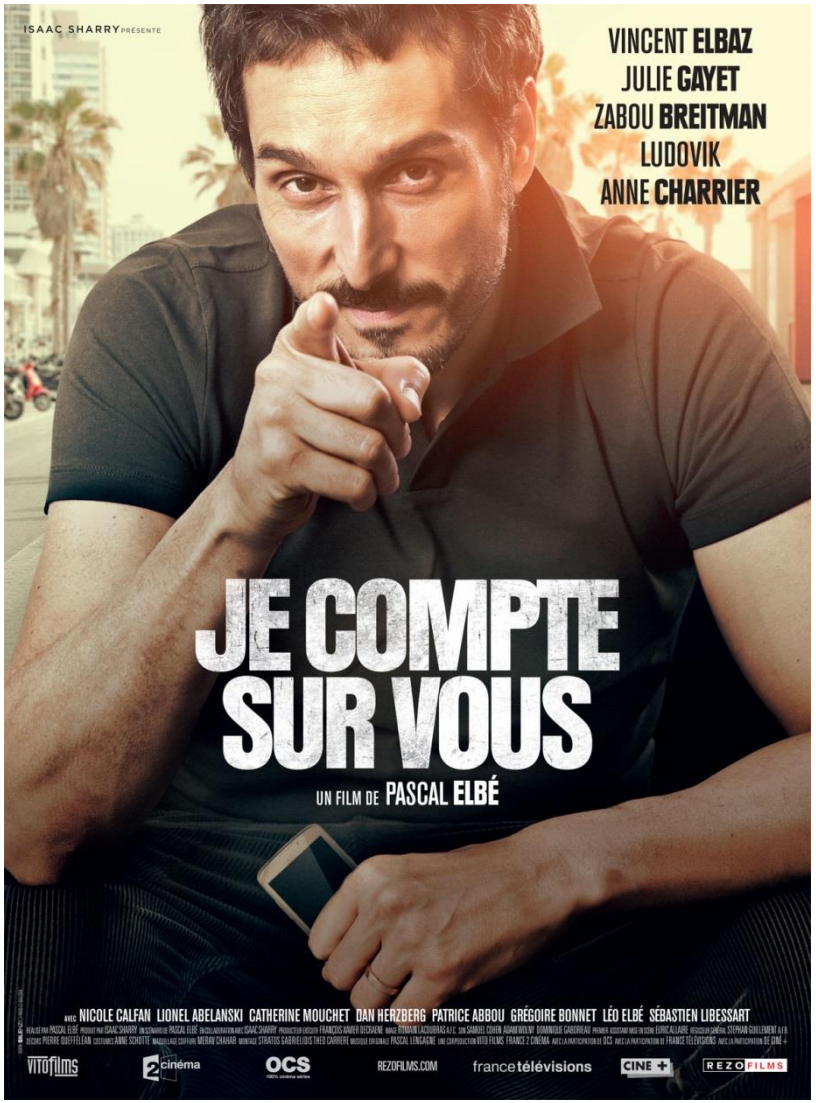
Techniques de fraude de plus en plus élaborées

Explosion de la fraude

L'évolution de la fraude ces dernières années

Domaines particulièrement touchés par la fraude aux virements				
Fraude par ruse (ingénierie sociale)			Fraude sur Internet (cybercriminalité)	
Fraude au président	Fraude au changement de coordonnées bancaires	Fraude à l'informatique	Phishing	Diffusion de malware

1. La fraude aujourd'hui



La **Fraude Président** inspire même le cinéma...

(Sortie le 30 décembre 2015 au cinéma)

2. Focus sur l'ingénierie sociale

Principaux modes opératoires des fraudeurs (liste non exhaustive…)

Fraude Président

Appel téléphonique, fax et/ou e-mail

usurpant l'identité d'une **personne influente de l'entreprise**

demandant avec **insistance**, à l'un des collaborateurs, la réalisation d'une

transaction exceptionnelle et confidentielle

Fraude au changement de coordonnées bancaires

Un escroc fait croire à un **changement de domiciliation bancaire**

d'un **créancier légitime** de l'entreprise

pour les **prochains règlements** de loyers ou de factures

Fraude informatique

L'escroc se fait passer pour un **technicien prestataire** de l'entreprise visée et tente d'obtenir par le collaborateur l'exécution de **« virements tests »**

Il peut aussi demander **l'installation de logiciels** qui permettront de **récupérer** des informations de sécurité ou de **pirater** le système informatique

2. Focus sur l'ingénierie sociale

Fraude au changement de coordonnées bancaires

Fraude au changement de coordonnées bancaires

Un escroc fait croire à un **changement de domiciliation bancaire**

d'un **créancier légitime** de l'entreprise

pour les **prochains règlements** de loyers ou de factures

Les constantes de ce type d'attaque

Les nouvelles coordonnées bancaires :

- sont le plus souvent **domiciliées à l'étranger**
- peuvent être adressées par **téléphone**, **e-mail** ou **courrier postal** (courrier spécifique ou facture incluant les nouvelles coordonnées bancaires)

Le dispositif mis en place : Comment se prémunir ?

- **Prendre son temps** pour effectuer les contrôles nécessaires
- Mettre en place et **respecter** une **procédure**
  - Procédure « 4 yeux » (saisie / validation)
  - Contre-appels systématiques, aléatoires ou selon les cas
- **Définir les formats acceptés** pour les changements de coordonnées bancaires (courrier signé de la Banque)
- **Sensibiliser le personnel** aux risques de fraude

La prévention est la première mesure à prendre pour se protéger

2. Focus sur l'ingénierie sociale

Comment se prémunir ?

Définissez et respectez les procédures
pour l'exécution de virements bancaires

Effectuez les vérifications indispensables
(légitimité de la demande, rapprochements bancaires quotidiens)

Limitez la communication

Coordonnées de l'O.C.R.G.D.F.
(Office Central de la Grande Délinquance Financière)

E-mail : ocrgdf-sec.dcpjaef@interieur.gouv.fr

Téléphone : +33 1 40 97 83 20

…cations bancaires

En cas d…

(contactez le… …est bien à l'origine de la demand… …Police)

Sensibilisez vos collaborateurs

Soyez vigilant (résistez aux tentatives d'intimidation et à la pression psychologique)

Pour en savoir plus…

2. Focus sur la cybercriminalité

Phishing / Vishing

Quel objectif ?

Il consiste, en se faisant passer pour une entreprise, une banque ou une organisation crédible, à demander au collaborateur de **saisir pour confirmation des données confidentielles** de son entreprise.

Comment ?

Le plus souvent, **réception d'un email** contenant de fausses informations, souvent alarmistes, ayant pour but d'inciter le client à divulguer des informations confidentielles

Par quelles voies ?

Emails, courriers, appels téléphoniques (vishing)

N.B. : Lorsque le phishing est effectué par email, il peut aussi servir à **diffuser un malware**

Virus bancaires / Malwares

Qu'est ce que c'est ?

Un type de **virus** développé à des fins malveillantes et introduit sur un ordinateur **à l'insu de son utilisateur**

Comment ?

- **Réception d'un email** contenant une pièce jointe
- **Téléchargement** d'un document ou un logiciel

Quel objectif ?

Espionner la victime et **récupérer** des données personnelles souvent confidentielles, permettant au fraudeur de l'escroquer

N.B. : le mot malware désigne un regroupement générique qui inclut tout type de programme malveillant (Cheval de Troie, ver, keylogger, etc.)

3. Focus sur la cybercriminalité
Comment se prémunir ?

Soyez vigilants à la réception d'emails

- ne répondez jamais à un email sollicitant la communication d'informations personnelles
- n'ouvrez pas les pièces-jointes
- ne cliquez pas sur les liens contenus dans un email dont vous ne connaissez pas l'expéditeur

Protégez votre parc informatique

- disposez d'un système d'exploitation, d'un antivirus et d'un pare-feu à jour
- installez en complément un logiciel contre les malwares bancaires (Trusteer, Webroot…)

A propos de vos applications bancaires

- connectez-vous régulièrement à votre application de banque à distance, vérifiez la dernière date de connexion, votre relevé de compte et déconnectez-vous via le bouton « déconnexion »
- ne partagez jamais vos identifiants de connexion (données strictement confidentielles)
- effectuez une ségrégation des pouvoirs

Pour en savoir plus…

Conclusion

Merci pour votre attention

~~~~~~~~~~

Questions / Réponses
~~~~~~~~~~