TYPOLOGIE D'UNE ATTAQUE :

- Prise de renseignements sur internet en source ouverte
- Société.com, infogreffe, véric.com etc. (on peut trouver la signature du dirigeant dans les documents payants et des infos sur le CA)
- Réseaux sociaux
- Site web de la société
- Recherche de la signature du dirigeant pour la falsifier sur l'ordre de virement

- Appels téléphoniques
- Noms et coordonnées des personnes aux postes clés (notamment financiers)
- Récupération des coordonnées du directeur financier ou du trésorier
- Récupération d'informations sur les contrats en cours et à venir
- Récupérations d'informations financières

- Envoi d'emails et contact téléphonique à la trésorière
- Falsification de l'adresse email du Président
- Parfois intervention d'un faux cabinet d'avocat
- Indices de manipulation :
  - Notion impérative d'urgence
  - Flatter l'orgeuil (qualités professionnelles de la trésorière)
  - Stricte confidentialité pour isoler la victime
  - Utilisation du levier psychologique de l'autorité

- Diversion du service financier
- Eventuellement appel d'un faux policier pour faire diversion

LES AUTEURS :

- Ils utilisent des plate-formes de redistributions téléphoniques pour masquer l'origine des appels
- Ils utilisent des anonymisateurs sur internet pour masquer leurs adresses IP (type VPN hidemyass.com)

LES SIGNAUX D'ALARME :

Lors d'une communication, certains signaux peuvent indiquer qu'une tentative de manipulation est en cours.
Notamment lorsque l'interlocuteur :
- *Refuse de fournir un numéro pour le rappeler*
- *Formule une demande inhabituelle*
- *Fait valoir son autorité*
- *Fait valoir l'urgence de la situation*
- *Menace d'exercer des représailles*
- *Semble mal à l'aise lorsqu'il est questionné ou élude les questions*
- *Cite des noms de collègues*
- *Fait des compliments ou flatte son correspondant*
- *Utilise la séduction*

Ces indices, lorsqu'ils sont détectés lors de la conversation doivent éveiller la méfiance de l'interlocuteur et générer un réflexe de prudence et de vérification.

LA PRÉVENTION DES ESCROQUERIES PAR « FOVI » :

Sensibiliser non seulement les dirigeants des entreprises, mais aussi les employés des services comptables et trésorerie, y compris les secrétaires, les standardistes et l'ensemble du personnel susceptible d'être contacté pour exécuter un virement. Le service informatique est également une cible privilégiée.

Ne pas fournir d'informations sensibles sur les déplacements du président ou l'absence de responsables ou directeurs, notamment financier. Préférer informer de leur non disponibilité temporaire sans préciser les dates ou horaires. Demander les coordonnées de l'appelant en précisant que la personne absente le rappellera dès qu'il sera disponible.

Instaurer un processus de vérification formalisé, connu uniquement des personnes concernées par les virements et éventuellement un système de signatures multiples, pour les paiements internationaux ou pour les grosses sommes.

Renforcer les contrôles sur les paiements à destination de la région chinoise du Wenzhou (principale destination des fonds provenant des escroqueries), de Hong Kong, de la Grande-Bretagne, des pays de l'Est, des états baltes, du Chypre, de la Suisse et du Liechtenstein.

Vérifier attentivement (à la lettre près) l'adresse mail du donneur d'ordre.

Rompre la chaîne des mails : Pour les courriers électroniques se rapportant à des virements internationaux, plutôt que d'utiliser le bouton « répondre », saisir soi-même l'adresse mail habituelle du partenaire ou d'une manière générale, du donneur d'ordre.

Les fautes d'orthographe dans les mails et les erreurs dans les noms et les fonctions des dirigeants doivent éveilles l'attention.

En cas de doute, regarder, le cas échéant avec l'informaticien de la société, la source (entête) des mails douteux. Si le message provient d'Israël ou du Nigéria, la méfiance s'impose...

Se méfier des mails provenant des webmails gmail, yahoo, mail.com ou gmx (Global Message eXchange, anciennement Caramail), souvent utilisés par les auteurs d'escroqueries par faux ordres de virements.

Conserver les mails susceptibles de provenir des escrocs.

Ne pas attendre d'être victime d'une escroquerie par FOVI, pour informer les cabinets d'avocats qui représentent l'entreprise à l'étranger, sur ce type d'escroquerie bien particulier. Cela permettra de gagner un temps précieux en cas de transfert frauduleux pour faire bloquer les fonds.