Lettre Cyber 67 Mai 2022

LE *SOCIAL ENGINEERING* :

Ce type d'attaque n'est pas basé sur l'outil informatique ou sur l'exploitation de failles matérielles ou logicielles, mais sur une autre faille : **L'HUMAIN (VOUS !).** Après avoir récupéré le maximum d'informations (que vous avez laissées sur la toile) sur vous et votre entreprise, les escrocs vont vous (ou quelqu'un de votre entreprise) **manipuler** afin de vous/lui **soustraire des informations du système de traitement automatisé de données ou de s'y introduire** sans avoir besoin de procéder à un quelconque piratage.

La **persuasion et la manipulation** sont les clefs de voûte de cette technique. Divers **scénarios** peuvent être utilisés. L'objectif principal du malfaiteur est d'exercer une **pression psychologique** en invoquant **l'urgence ou la confidentialité, pour obtenir un virement.** Cette méthode a été popularisée dans les années 1980 par Kévin MITNICK reconnu comme l'un des plus grands hackers.

Internet et les réseaux sociaux professionnels ... ATTENTION :

Internet et les réseaux sociaux ont pris une place prépondérante dans le relationnel entreprise / clientèle. Portez une attention toute particulière sur ce que vous postez sur votre entreprise, vous et vos collaborateurs :

- Ne divulguez pas les organigrammes **des personnels** et les **différents services avec des coordonnées directes**.
- Ne postez pas vos **absences, déplacements** professionnels avec une localisation précise.
- Limitez au maximum la divulgation des numéros de téléphones et adresses mails professionnels.
- Ne divulguez jamais vos informations sensibles à une personne par téléphone ou via des messageries. Ne le faites que si vous êtes sûr de la connaître physiquement.
- Changez régulièrement vos mots de passe.
- Soyez vigilant et ne croyez pas aux offres très « spéciales » et « alléchantes »…

Comment se protéger :

Les scénarios d'attaque sont nombreux. Une **sensibilisation** des collaborateurs sur les enjeux et la criticité des informations est primordiale.

On peut envisager la mise en place de **tests** pour faire en sorte que les collaborateurs d'une entreprise aient connaissance des moyens et des techniques utilisés.

Une formation sur les bonnes pratiques est nécessaire.

La double authentification :

Parmi les différents moyens de lutte pour éviter des virements, le principe de la double authentification s'avère performant. Le facteur humain étant le maillon faible, n'acceptez jamais d'effectuer un paiement ou un virement sans avoir préalablement pris attache de vive voix avec le chef d'entreprise pour vérifier la véracité de la transaction.

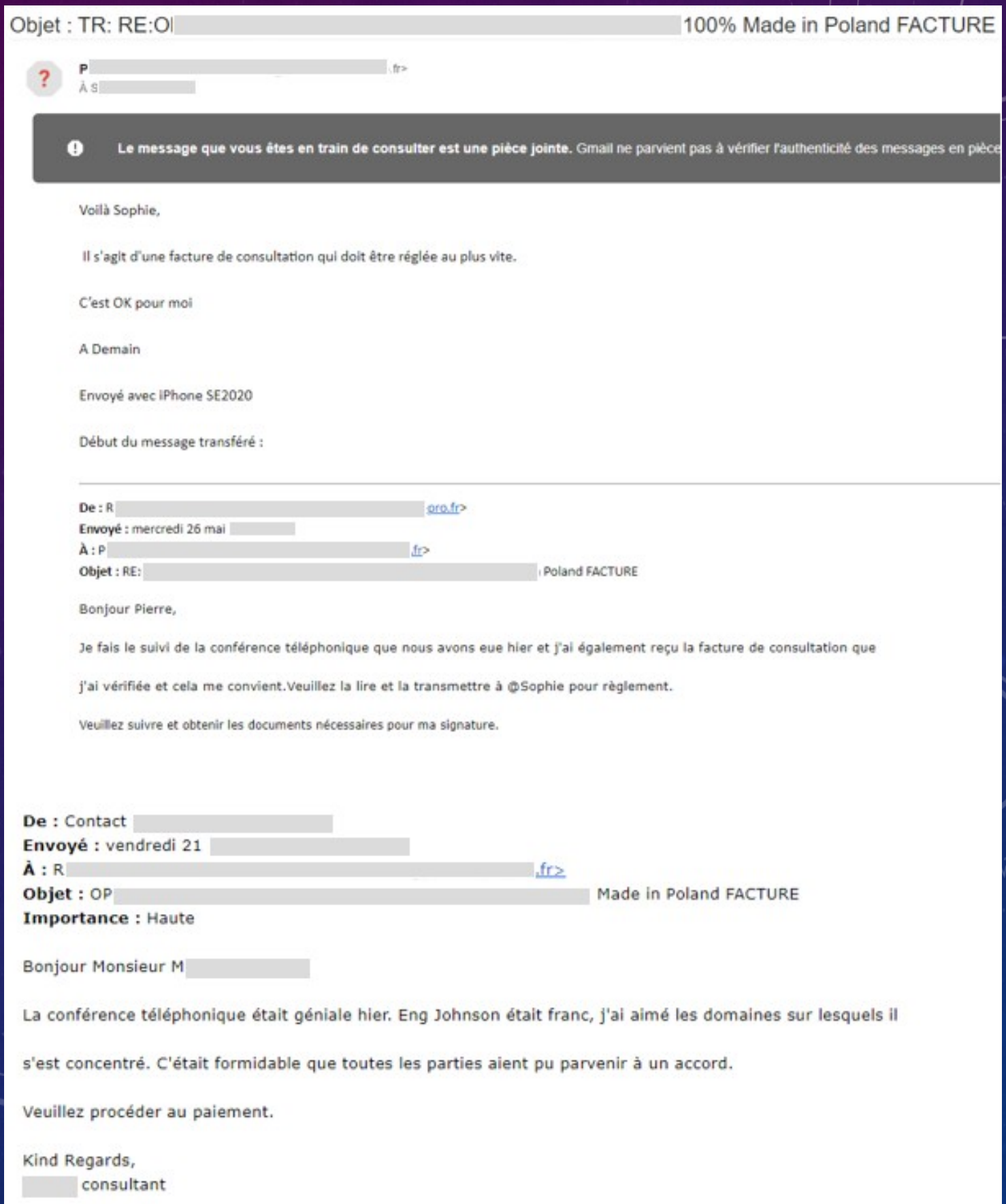
On peut également décider de mettre en place un **« code »** connu seulement du décisionnaire et de l'agent payeur. Ce code peut être une phrase qui doit figurer dans chaque demande de paiement ou de transaction.

Recevoir cette lettre info par mail, envoyez-nous votre demande :

Arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou patrick.wolfert@gendarmerie.interieur.gouv.fr

A titre d'exemple :

Une entreprise a été victime d'un faux ordre de virement suite au recueil de l'organigramme complet de la société sur internet. Les escrocs ont fabriqué un faux échange de mail pour que le paiement soit réalisé :



Objet : TR: RE:O 100% Made in Poland FACTURE

P .fr>
À S

Le message que vous êtes en train de consulter est une pièce jointe. Gmail ne parvient pas à vérifier l'authenticité des messages en pièce

Voilà Sophie,

Il s'agit d'une facture de consultation qui doit être réglée au plus vite.

C'est OK pour moi

A Demain

Envoyé avec iPhone SE2020

Début du message transféré :

De : R oro.fr>
Envoyé : mercredi 26 mai
À : P .fr>
Objet : RE: Poland FACTURE

Bonjour Pierre,

Je fais le suivi de la conférence téléphonique que nous avons eue hier et j'ai également reçu la facture de consultation que

j'ai vérifiée et cela me convient.Veuillez la lire et la transmettre à @Sophie pour règlement.

Veuillez suivre et obtenir les documents nécessaires pour ma signature.

De : Contact
Envoyé : vendredi 21
À : R .fr>
Objet : OP Made in Poland FACTURE
Importance : Haute

Bonjour Monsieur M

La conférence téléphonique était géniale hier. Eng Johnson était franc, j'ai aimé les domaines sur lesquels il

s'est concentré. C'était formidable que toutes les parties aient pu parvenir à un accord.

Veuillez procéder au paiement.

Kind Regards,
consultant