Qu'est-ce qu'un message d'hameçonnage (phishing) ?

Qu'est-ce qu'un message d'harponnage (spear phishing) ?

Le cas particulier de l'arnaque au président

Comment reconnaître un message frauduleux

Que faire si on est destinataire d'un message frauduleux

Que faire si on est victime d'un message frauduleux

Qu'est-ce qu'un message d'hameçonnage (phishing) ?

Technique d'escroquerie utilisée par des fraudeurs qui consiste à se faire passer pour quelqu'un d'autre afin de soutirer des renseignements personnels ou sensibles à la personne visée.

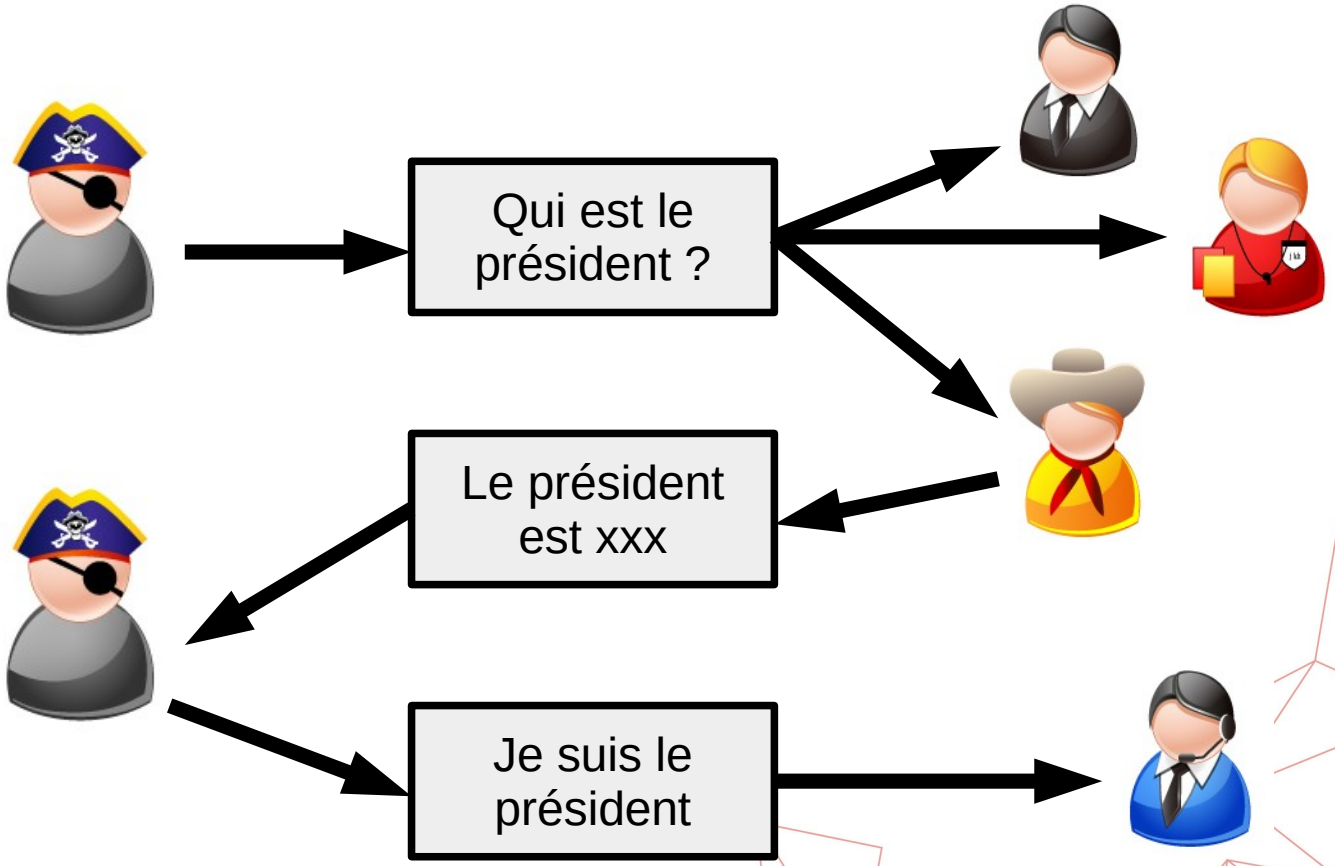
- Identifiants => phishing ou intrusion
- Coordonnées bancaires => vol
- Informations sur d'autres personnes => harponnage

Qu'est-ce qu'un message d'harponnage (spear phishing) ?

Variante d'hameçonnage s'adressant à des personnes ciblées.

Précédé par une ou des campagnes de recueil d'informations sur les cibles qui permettent de personnaliser l'attaque et de rendre le message le plus vraisemblable possible.

Qu'est-ce qu'un message d'harponnage (spear phishing) ?



Auteur des icônes : https://www.zcool.com.cn/u/418607/

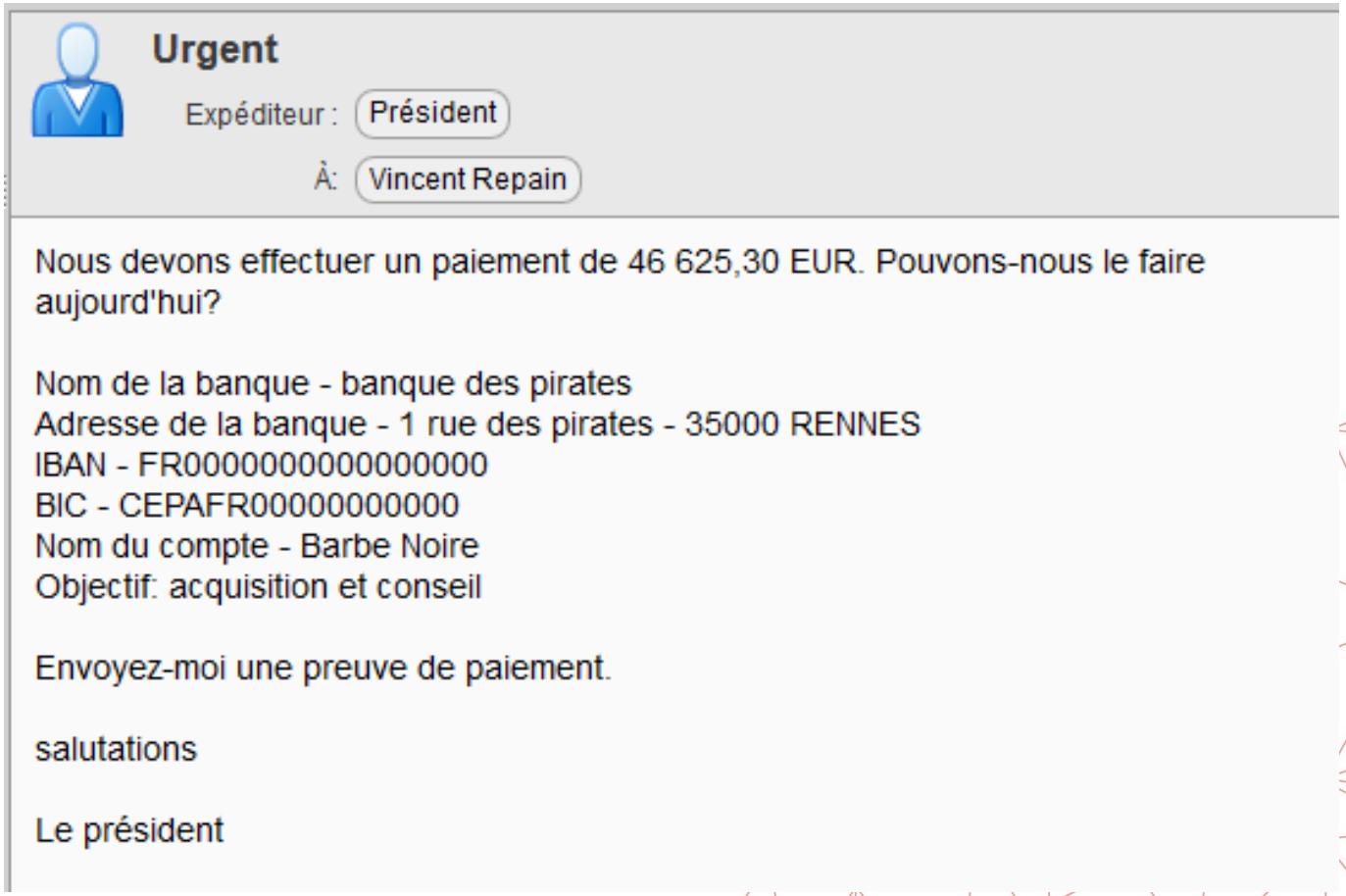
Le cas particulier de l'arnaque au président ou de l'escroquerie aux faux ordres de virement

La fraude au président consiste à se faire passer pour un des dirigeants d'une entreprise ou d'une administration pour convaincre la cible d'effectuer un virement à un tiers.

Le « changement de RIB » consiste à se faire passer pour un fournisseur et à demander de diriger les versements pour ce fournisseur vers un compte bancaire appartenant aux escrocs.

Le cas particulier de l'arnaque au président ou de l'escroquerie aux faux ordres de virement

Exemple



Urgent

Expéditeur : Président

À: Vincent Repain

Nous devons effectuer un paiement de 46 625,30 EUR. Pouvons-nous le faire aujourd'hui?

Nom de la banque - banque des pirates
Adresse de la banque - 1 rue des pirates - 35000 RENNES
IBAN - FR0000000000000000
BIC - CEPAFR00000000000
Nom du compte - Barbe Noire
Objectif: acquisition et conseil

Envoyez-moi une preuve de paiement.

salutations

Le président

Comment reconnaître un message frauduleux

Quelques pistes :

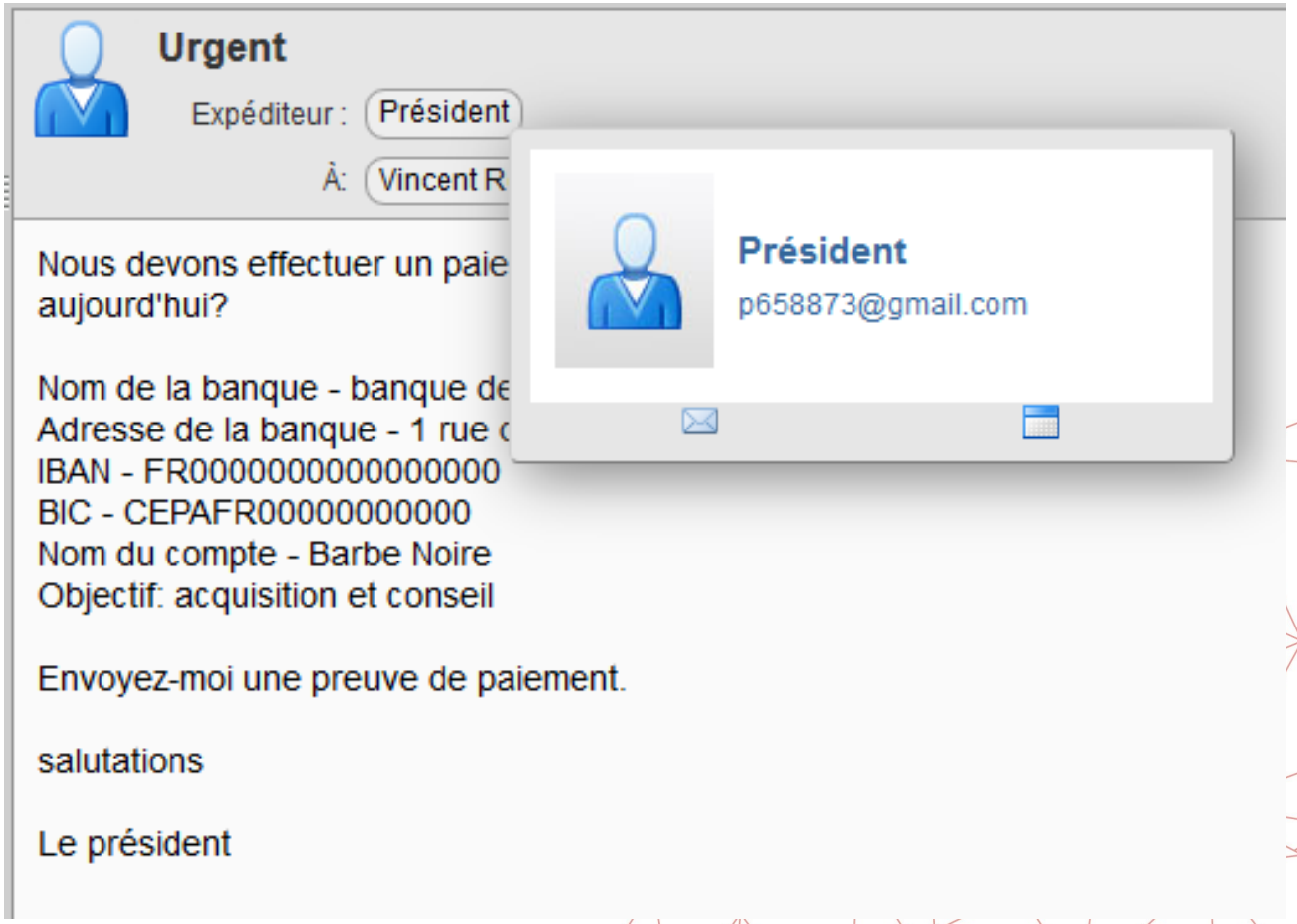
- Le style et l'orthographe sont fantaisistes
- Le message a un caractère d'urgence
- Une discrétion absolue est demandée
- Le nom de l'expéditeur ne correspond pas à l'adresse mail : attention, l'inverse ne signifie pas que le message est légitime

Se poser les questions suivantes :

- Ce qui est écrit est-il vraisemblable ?
- Est-ce que j’attends bien un tel message de cet interlocuteur ?
- Pourquoi est-ce qu’on s’adresse à moi ?
- Est-ce qu’il y a un lien ou une pièce jointe étrange dans le message ?

Comment reconnaître un message frauduleux

Exemple



Comment reconnaître un message frauduleux

Attention également aux adresses ressemblant à **univ-rennes1.fr** :

- xxx@univ-rennesl.fr
- xxx@univ.rennes1.fr
- xxx@univ-rennes1.fr.com
- etc.

Que faire si on est destinataire d'un message frauduleux

Ne jamais répondre
Ne pas cliquer sur les liens dans le message
En cas de doute et si vous connaissez l'expéditeur affiché, contactez-le pour vérifier la légitimité du message, en particulier en cas de « fraude au président »

Faire un ticket dans la catégorie « DSI - Informatique réseau et téléphonie / Sécurité / Phishing »

Et joindre le message suspect comme indiqué

Que faire si on est destinataire d'un message frauduleux

Les liens dans un message peuvent pointer vers un fichier à télécharger ou une fausse page d'authentification

Précautions à prendre en s'authentifiant

Vérifiez que la page d'authentification provient bien de l'université :
Dans la plupart des cas, l'adresse de la page commence par :

https://sso-cas.univ-rennes1.fr/login?service=

C'est le service d'authentification centralisé de Rennes 1

Dans de rares autres cas l'authentification se fait dans l'application (Octime par exemple) : vérifiez que vous la connaissez

Exemple de lien frauduleux

https://sso-cas.univ-rennes1.fr.com/login?service=

https://site-pirate.com/sso-cas.univ-rennes1.fr

Que faire si on est victime d'un message frauduleux

Si je suis victime de l’attaque (j'ai indiqué mon identifiant/mot de passe sur un site de pirates ou si j’ai fait une opération dont je réalise qu’elle est probablement pas légitime)

Changer immédiatement son mot de passe via les pages Sésame, annuler si possible l’opération indue, prévenir le référent fonctionnel de l’application concernée.