Contexte

Le contexte de M@Banque, tel que détaillé dans le TP « identité numérique », s'applique aussi à ce TP. Veuillez vous référer au TP en question si besoin.

Problématique

Des courriels frauduleux sont adressés aux clients, qui prennent l'apparence de messages émis par M@Banque. Ils les invitent à compléter un contrat dématérialisé d'ouverture de compte avec leurs informations personnelles. Si les clients remplissent le document, les pirates peuvent récupérer leurs informations d'identification pour accéder à leurs comptes. Mme. Schmitt sollicite votre expertise pour trouver une solution technique à cet acte de malveillance et rétablir l'e-réputation de M@Banque.

Identification de la fraude

Voici le courriel reçu par les clients de M@Banque :

De : juridique@mabanques.com
À : client@gmail.com
Sujet : M@BANQUE – validation de contrat

M@Banque

Cher(e)s clientes et clients de M@Banque

Vous trouverez en pièce-jointe le contrat d'ouverture de compte bancaire à compléter et à nous renvoyer pour confirmer votre engagement pris via notre site.

Vous devez nous confirmer notamment votre identifiant et votre mot de passe d'accès à vos comptes. Voici pouvez le faire soit en répondant à ce mail ou bien via ce lien.

Nous sommes heureux de vous compter parmi nos nouveaux clients

Le service juridique
juridique@mabanques.com

Identifiez les éléments permettant de détecter que le courriel contenant un contrat dématérialisé est frauduleux. Vous pouvez prendre appui sur :

- Les différents cours
- Des recommandations de la CNIL (ex : https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant)
- Des recommandations de l'ANSSI (ex : https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/)

Juridique

Déterminez le délit et les peines encourues par les pirates pour cet acte de malveillance.

Signature par courriel

Démontrez qu'une solution telle que PGP ou GPG, basée sur de la cryptographie asymétrique répond bien aux exigences de la législation concernant la signature électronique. Imaginez une nouvelle procédure d'échange par courriel entre M@Banque et ses clients qui utilise ce type de solution et qui rendrait caduque la fraude détectée.

Coffre-fort numérique

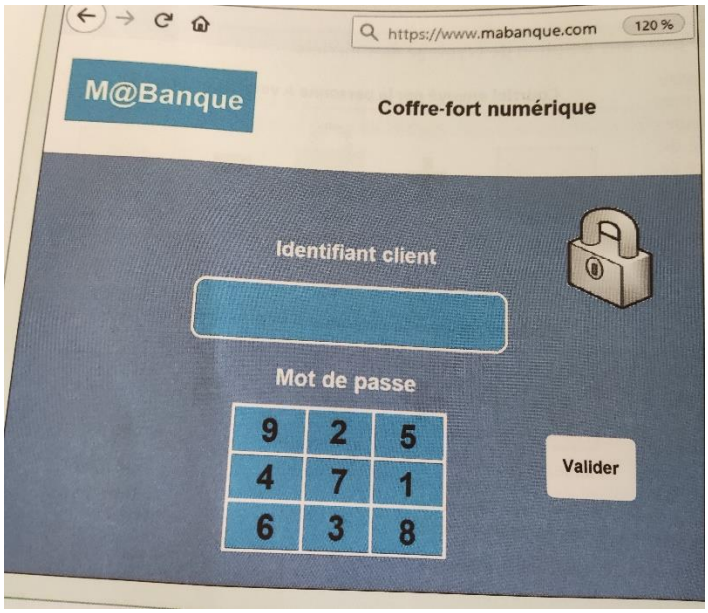
M@Banque souhaite mettre en place un coffre-fort numérique qui serait une solution de stockage d'informations. Son objectif est de conserver les données intactes et de permettre leur restitution à l'identique à un utilisateur accrédité. Le coffre-fort numérique doit donc garantir, avant tout, l'intégrité des informations dans le temps.

Ce service est désormais proposé aux particuliers, sous la forme d'un espace de stockage sécurisé, qui nécessite une identification. Ses fonctionnalités permettent la récupération automatique des différents types de documents confiés par le client (relevés bancaires, fiches de paie, factures, …). Une fois configuré, cet outil met aussi à disposition du client les différents documents produits par M@Banque (ex : relevé de comptes, contrats, …).

M@Banque garantit à l'utilisateur un accès exclusif du service par la mise en œuvre des mesures suivantes :

- Une identification par un identifiant et un mot de passe personnels ;
- Un chiffrement des données et des documents lors du stockage et du transfert

Voici une capture d'écran du nouveau service de coffre-fort :



1) **Expliquez en quoi ce genre de service permet de réduire le risque d'attaque par phishing comme celle subie dernièrement.**
2) **Expliquez en quoi la mise en place d'un tel service peut participer à améliorer l'e-réputation de M@Banque.**
3) **Expliquez pourquoi ce service, tel qu'il est actuellement, ne peut pas être utilisé pour de la signature électronique.**