TP Preuve Electronique

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.

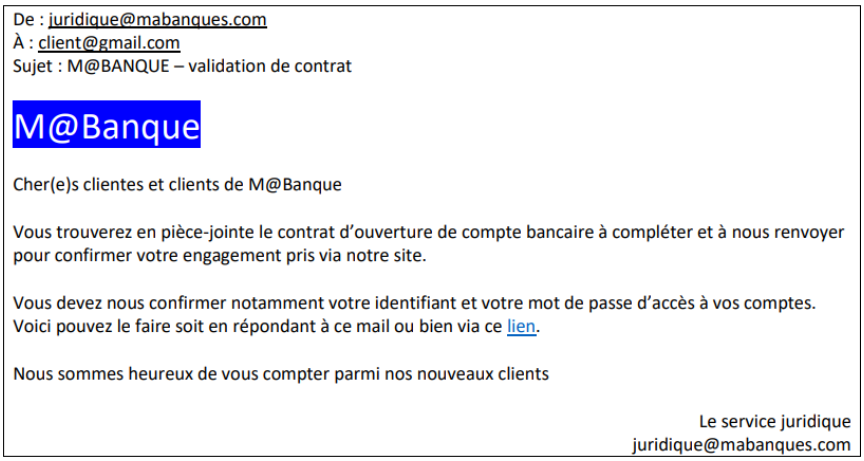
Problématique

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.

Table des matières

1) 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 :

*L'adresse email de l'expéditeur qui peut sembler suspecte ou différente de celle attendue (juridique@banques.com) le (s) à après le mot banque qui n'est pas au pluriel met la puce à l'oreille.

*Le manque de détails personnalisés, comme le nom du client ou des informations sur le compte bancaire

*La demande d'informations sensibles telles que l'identifiant et le mot de passe d'accès au compte (Il ne faut jamais divulguer des informations sensibles par email !!)

*L'absence de signature électronique ou de tout autre mécanisme de sécurité pour protéger les informations sensibles

*L'utilisation d'un lien qui peut sembler suspect ou qui ne correspond pas à une adresse web connue de la banque (en pointant le curseur de sa souris sur le lien sans cliquer on peut le voir)

*Une grammaire ou une orthographe incorrecte dans le contenu du courriel

*Une absence de numéro de téléphone de la banque pour pouvoir vérifier l'authenticité de la demande.

2) Juridique

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

L'envoi d'un courriel frauduleux contenant des informations sensibles, comme un contrat dématérialisé, pourrait être considéré comme un acte de phishing, qui est une forme de fraude en ligne visant à obtenir des informations personnelles ou financières. Les peines pour ce délit varient selon les lois de chaque pays.

En France, le phishing est régi par la loi Informatique et Libertés, qui prévoit des peines allant jusqu'à 5 ans de prison et 75 000 euros d'amende pour les infractions les plus graves. Les pirates pourraient également être poursuivis pour d'autres délits tels que l'escroquerie, la violation de la vie privée ou la violation de données personnelles.

Il est important de noter que les peines réelles pour ce type d'infraction peuvent varier considérablement en fonction des circonstances et de la juridiction. Il est donc important de consulter un avocat pour obtenir des informations plus précises sur les peines encourues dans un cas spécifique.

3) 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.

PGP (Pretty Good Privacy) et GPG (GNU Privacy Guard) sont des solutions de cryptographie asymétrique qui permettent de chiffrer et de signer électroniquement des données pour garantir leur intégrité et leur confidentialité. Ces solutions répondent aux exigences de la législation concernant la signature électronique car elles permettent de créer une signature numérique unique et non répudiable pour chaque message électronique.

Une procédure d'échange par courriel entre M@Banque et ses clients qui utilise PGP ou GPG pourrait se dérouler comme suit :

1) M@Banque génère une paire de clés publique/privée pour chaque client. La clé publique est rendue disponible pour tous les clients, tandis que la clé privée est conservée en sécurité par M@Banque.

2) Lorsque M@Banque envoie un courriel à un client, elle utilise la clé publique du client pour chiffrer le message et créer une signature numérique unique à l'aide de sa propre clé privée.

3) Le client reçoit le courriel chiffré et vérifie la signature numérique en utilisant la clé publique de M@Banque. Cela lui permet de s'assurer que le message provient bien de M@Banque et qu'il n'a pas été altéré en cours de route.

4) Le client déchiffre le message en utilisant sa propre clé privée pour récupérer les informations.

5) Le client signe et chiffre son propre message en utilisant sa propre clé privée et la clé publique de M@Banque pour garantir l'authenticité de ses informations.

Avec cette procédure, il serait beaucoup plus difficile pour un pirate de frauder les clients de M@Banque en envoyant des courriels frauduleux, car la signature numérique unique et non répudiable garantirait l'authenticité des messages échangés entre M@Banque et ses clients.

Il est important de noter que pour qu'une telle procédure fonctionne correctement, il est nécessaire de garantir la sécurité des clés privées et de veiller à la mise à jour régulière des clés publiques pour éviter les risques de compromission. Il est également important que les clients soient formés à l'utilisation de cette technologie pour éviter les erreurs d'utilisation.

4) 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.

Un coffre-fort numérique comme celui décrit permet de réduire le risque d'attaque par phishing en utilisant plusieurs mécanismes de sécurité :

Identification par un identifiant et un mot de passe personnels : Cela garantit que seuls les utilisateurs autorisés peuvent accéder aux données stockées dans le coffre-fort numérique, ce qui réduit les risques d'accès non autorisé.

Chiffrement des données et des documents : Le chiffrement des données et des documents lors du stockage et du transfert empêche les pirates d'accéder aux données en clair, même s'ils parviennent à les voler ou à les capturer lors d'une transmission.

On peut même imaginer une authentification à double facteur : Cela garantit que seul l'utilisateur ayant accès à un deuxième facteur (comme un code envoyé par SMS ou une clé matérielle) peut accéder au coffre-fort numérique, ce qui augmente considérablement la sécurité de l'accès.

2) Expliquez en quoi la mise en place d'un tel service peut participer à améliorer l'e-réputation de M@Banque.

La mise en place d'un coffre-fort numérique peut participer à améliorer l'e-réputation de M@Banque en offrant plusieurs avantages :

La sécurité des données : En garantissant l'intégrité des données stockées dans le coffre-fort numérique, M@Banque peut rassurer ses clients sur la sécurité de leurs informations personnelles et financières, ce qui contribue à renforcer la confiance en la banque.

La conformité réglementaire : En se conformant aux normes de sécurité et de confidentialité, M@Banque peut montrer qu'elle respecte les exigences légales et réglementaires, ce qui contribue à renforcer sa crédibilité.

La transparence : En offrant un accès sécurisé aux clients à leurs données et aux documents produits par M@Banque, cette dernière peut montrer sa transparence et sa volonté de faciliter les relations avec ses clients, ce qui contribue à renforcer la confiance en la banque.

La flexibilité : En permettant aux clients de stocker et de récupérer automatiquement différents types de documents, M@Banque peut montrer qu'elle prend en compte les besoins et les attentes de ses clients, ce qui contribue à renforcer la satisfaction de ses clients.

En somme, la mise en place d'un coffre-fort numérique permet à M@Banque de montrer sa capacité à protéger les données de ses clients, de se conformer aux normes de sécurité et de confidentialité, d'être transparente dans sa gestion des données et de prendre en compte les besoins et les attentes de ses clients. Tout cela contribue à renforcer la confiance en la banque et à améliorer son e-réputation.

3) Expliquez pourquoi ce service, tel qu'il est actuellement, ne peut pas être utilisé pour de la signature électronique.

Le service de coffre-fort numérique tel qu'il est décrit ne peut pas être utilisé pour de la signature électronique car il ne répond pas à toutes les exigences légales et techniques requises pour une signature électronique valide.

Absence de certification : Le service de coffre-fort numérique ne propose pas de mécanisme de certification pour vérifier l'identité de l'expéditeur d'un document, ce qui est nécessaire pour garantir l'authenticité des documents électroniques.

Absence de preuve : Le service de coffre-fort numérique ne propose pas de mécanisme pour générer et conserver des preuves de signature pour les documents stockés, ce qui est nécessaire pour garantir la validité de la signature électronique.

Il est important de noter que la signature électronique est un processus complexe qui nécessite des mécanismes de sécurité spécifiques pour garantir l'authenticité, l'intégrité et la non-répudiation des documents électroniques. Le service de coffre-fort numérique tel qu'il est décrit ne permet pas de répondre à toutes ces exigences, il n'est donc pas adapté pour de la signature électronique.