PHISHING - Alerte sécurité du 16/06/2016

Depuis le début du mois de juin 2016, plusieurs entreprises rhônalpines ont reçu des e-mails de phishing semblant provenir de banques.
Ceux-ci comportaient des instructions visant à mettre à jour le logiciel du lecteur d'authentification et de sécurisation des transactions bancaires.

Le ***phishing*** (ou ***hameçonnage***, ou ***filoutage***) est une technique consistant à faire croire à la victime qu'elle s'adresse à un tiers de confiance (*banque, administration, etc.*) en vue de lui soutirer des renseignements tels que des mots de passe, des numéros de carte de crédit, des coordonnées bancaires, des renseignements d'état-civil, etc.

Le phishing est une forme d'attaque informatique reposant sur l'**ingénierie sociale (1)**. Elle peut être commise par le biais de courriers électroniques, de faux sites internet, tout autre moyen électronique voire même par téléphone.

Ces derniers jours, plusieurs entreprises rhônalpines ont reçu des mails tel que celui figurant ci-dessous :

De : CyberPlus

Envoyé : vendredi 3 juin 2016 18:16

À : [redacted]

Objet : Spam Message important !

Importance : Haute

Bonjour,

Le département technique procéde à une mise à jour importante de logiciel programmée de facon à améliorer la qualité de nos services .

Nos vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer votre PassCyberPlus :

??? pourquoi pas gentillesse tant que nous y sommes

Lien frauduleux

Confirmer votre PassCyberPlus

Nous vous remercions pour la confiance que vous acordez à nous et restons à votre disposition .

Cordialement,

Ceci est un troisiéme et dernier rappel nous vous invitant a accéder a votre formulaire dés que possible,

Ces courriels, rédigés dans un *français approximatif*, voire *peu académique*, contiennent un lien renvoyant vers un faux site bancaire hébergé à l'étranger. Ne surtout pas cliquer dessus.

POUR INFO : Le lecteur d'authentification « *PassCyberPlus* » (*nom d'un des appareils mis à disposition par les banques, mais il en existe d'autres*) est un outil visant à sécuriser les transactions bancaires. Il permet à l'utilisateur d'une part de s'identifier formellement et d'autre part de lui fournir un code à usage unique.

Par mesure de sécurité, aucune banque ne vous transmettra d'e-mail vous invitant à saisir des données personnelles.

(1) ***L'ingénierie sociale*** (ou *social engineering* en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme,l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il désire obtenir.

Quelques bonnes pratiques :

1. Vérifier soigneusement l'adresse Internet (*www.nom-du-site.com...*) vers laquelle on vous renvoie et s'assurer qu'il s'agit bien à la lettre près de l'adresse signalée dans le mail. (*Contrôler également la présence du « https » et du cadenas*).

2. Ne jamais cliquer sur un lien compris dans un e-mail où l'on demande au destinataire de se connecter afin de réactiver un compte bancaire ou de réaliser des modifications sur ce compte.

3. Même si l'adresse comprise dans l'e-mail est conforme à l'adresse officielle de votre banque, il est très facile pour le pirate de vous renvoyer vers un site frauduleux. Vérifiez toujours que le site sur lequel vous êtes connecté correspond bien exactement, à la lettre près, au site de votre banque.

4. Dans le doute, contacter l'expéditeur officiel du message pour déterminer s'il en est bien l'expéditeur et s'il est effectivement nécessaire de réactiver un compte ou de procéder à une modification de données.

5. Signaler immédiatement à la banque, tout e-mail suspect, même si vous n'avez pas la certitude qu'il s'agit d'un mail de phishing.

6. Pensez à communiquer à votre conseiller bancaire un numéro de téléphone portable et un e-mail. Maintenir ces données à jour et signaler rapidement tout changement.

Si c'est trop tard :

Vous avez déjà saisi des informations sur un site frauduleux, change immédiatement votre mot de passe et contactez rapidement votre conseiller bancaire.

Pour aller plus loin :

PHISHING INITIATIVE FRANCE : Le service Phishing Initiative offre à tout internaute la possibilité de lutter contre les attaques de phishing. En dénonçant ici l'adresse d'un site de phishing francophone, chaque site fera l'objet d'une validation et d'un blocage dans les navigateurs. En contribuant, vous diminuez l'impact de cette cybercriminalité et empêchez d'autres internautes d'être victime de fraude. https://phishing-initiative.fr/

SITE DE VOTRE BANQUE : Un onglet « a***ssistance*** » ou « ***signalement*** » peut avoir été mis à votre disposition pour signaler toute tentative de fraude.

SIGNALEZ L'ABUS D'UTILISATION D'INFORMATIONS PERSONNELLES : Si vous pensez avoir été victime d'une escroquerie par *phishing*, signalez le immédiatement sur la plateforme « PHAROS » (plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements) à l'adresse suivante :Cette plateforme permet de signaler les sites internet dont le contenu est illicite, mais aussi la réception de *phishing.* Votre signalement sera traité par un service de police spécialisé dans ces questions. **www.internet-signalement.gouv.fr**

COMMENT SE PROTÉGER DU FISHING : www.securite-informatique.gouv.fr

CONSEIL DU JOUR :

Réfléchir avant de cliquer et non pas l'inverse !!!

En cas de problème avéré :

Déposer rapidement plainte **auprès du service de police ou de gendarmerie territorialement compétent.**

Cellule Intelligence Économique régionale
☎·: 04.37.85.21.15