GUADELOUPE
BANQUE ET ASSURANCES

Alerte Sensibilisation

Madame, Monsieur,

L'été est propice à la multiplication des tentatives de fraudes, les escrocs profitant des congés dans les entreprises.

En relais des institutions telle que la Fédération des Banques Françaises et la Banque de France, nous vous informons que les tentatives de fraudes aux ordres de virement visant les entreprises se multiplient. Ces tentatives d'escroqueries sont liées à :

- de la fraude à caractère technologique tels que **« Phishing »** (collecte frauduleuse d'informations par voie informatique), injection de virus (« **Malware** ») dans le système d'information, **détournement des lignes téléphoniques** pour l'envoi de codes confidentiels...

- des pratiques d'ingénierie sociale qui consistent pour un fraudeur à se faire passer pour un dirigeant en abusant un collaborateur de l'entreprise afin d'obtenir un transfert d'argent avec des techniques d'intimidation, essentiellement basées sur l'urgence, le secret, la flatterie ou la menace.

Phishing , Malware ……

Les piratages informatiques n'arrivent pas qu'aux autres

- Maintenez à jour antivirus et anti-spyware de vos ordinateurs
- Effectuez les mises à jour sécuritaires de votre système (Windows, MAC OS, …)

(Voir message ci-dessous)

Réflexes obligatoires

Activation d'un anti-virus et d'un pare-feu (firewall). Il en existe de nombreux sur le marché, parfois gratuits ou déjà présents sur votre ordinateur (firewall Microsoft Windows par exemple)

Maintenance permanente de l'antivirus et de l'anti-spyware (logiciel malveillant), et **scan régulier** afin de détecter/éradiquer les malwares présents sur l'ordinateur. Au moins une fois par semaine.
Effectuez régulièrement **les mises à jour de votre système** pour charger les évolutions liées à la sécurité.

Attention aux mails d'origine inconnue avec une pièce jointe ou un lien.
Attention aux sites douteux, sites de téléchargement illégal …

Si un logiciel malveillant est détecté, faites-le éradiquer par votre anti-virus ou votre anti-spyware, **et seulement après vérification de la bonne fin**, modifiez les codes secrets d'accès à tous les services Internet protégés par ce type de contrôle d'accès.

Le Crédit Agricole a récemment constaté de tentatives de virements frauduleux, signés au moyen de certificats électroniques, avec saisie du mot de passe.

Il ne s'agit pas cependant d'une faille sécuritaire des certificats.

Après investigation par le *CERT Crédit Agricole*, il apparait que les postes des clients concernés sont infectés par un malware permettant à un fraudeur d'en prendre le contrôle à distance, et notamment d'enregistrer la saisie du mot de passe de son certificat.

Face à cette situation, nous rappelons les mesures de vigilance sécuritaire suivantes :

- **Il est de la responsabilité du client de veiller sur la sécurité de son poste et d'utiliser un antivirus à jour avec des scans réguliers**
- **Le détenteur du certificat doit en garder le contrôle exclusif ; il ne doit notamment jamais en divulguer le mot de passe**
- **Le mot de passe par défaut (cas des certificats sur clé usb) doit impérativement être changé lors de l'installation, comme le rappelle le manuel d'installation ; par la suite, le mot de passe doit être changé régulièrement**
- **La clé usb contenant le certificat doit être retirée après usage**
- **La non-répudiation de l'usage du certificat (authentification, signature) est incompatible avec une prise de main à distance par une assistance téléphonique**

Le Crédit Agricole devra faire une demande de révocation du certificat électronique compromis (la signature d'un virement frauduleux est une compromission) dès qu'elle aura connaissance de la fraude

Ingénierie Sociale

Parmi les techniques de fraudes les plus courantes, l'Ingénierie Sociale* peut se définir comme "l'art de manipuler son interlocuteur" pour qu'il réalise une action ou divulgue une information confidentielle.

Elle peut prendre de multiples formes, par exemples :

- Usurper l'identité d'un dirigeant de l'entreprise, d'un fournisseur, d'un bailleur…pour obtenir l'émission d'un virement…
- Détourner des lignes téléphoniques et des courriels…
- Prendre le contrôle des serveurs à distance…
- Prétexter des tests de compatibilité ou d'ordres SEPA en se faisant passer pour votre banque…

QUELQUES CRITERES D'ALERTE* :

(*) Liste non exhaustive.

- Demande exceptionnelle, urgente et confidentielle
- Réception d'e-mail avec une adresse de l'expéditeur incohérente, des erreurs de syntaxe ou des fautes d'orthographe, un lien ou un site avec une adresse URL inexacte, une absence de mention « https » dans l'adresse internet du site visité ou du cadenas indiquant une connexion sécurisée ; ne cliquez pas sur les liens ; n'ouvrez pas les pièces jointes ; ne répondez pas.
- Opération inhabituelle vers des bénéficiaires et/ou des comptes inconnus pour un montant important.
- Demande de virement de montant élevé pour un test ou demande de prise de contrôle à distance de l'ordinateur du collaborateur.
- Un de vos fournisseurs ou bailleur communique de nouvelles coordonnées bancaires par fax ou courriel : mieux vaut vérifier la légitimité de la demande en effectuant un contre-appel vers un numéro déjà référencé
- Un site ou un service de votre entreprise ne reçoit aucun appel téléphonique pendant une période inhabituellement longue
- Une de vos connaissances appelle sur votre portable en indiquant que votre ligne fixe ne répond pas ou qu'un inconnu répond à votre place

Gardez à l'esprit que votre banque ne vous sollicitera jamais pour :
- Demande de réalisation de virements tests. Les demandes de test sont toujours à l'initiative du client pour des montants ne dépassant jamais quelques euros.
- Demande de communication d'informations confidentielles par téléphone ou e-mail, en particulier un identifiant ou un mot de passe.
- Prise de contrôle de votre ordinateur

Ecoutez votre intuition : si une demande vous paraît suspecte, c'est probablement qu'elle l'est!

QUE FAIRE EN CAS D'ALERTE OU DE FRAUDE SUPPOSEE ?

Agissez immédiatement : prévenez votre responsable et alertez votre banque.

Vérifiez régulièrement les opérations effectuées sur vos comptes et votre carte bancaire.

CAISSE REGIONALE DE CREDIT AGRICOLE MUTUEL DE GUADELOUPE, société coopérative à capital variable, agréée en tant qu'établissement de crédit
Siège social : Petit-Pérou - 97176 ABYMES CEDEX - No SIRET : 314 560 772 00217 - Code APE : 6419Z - RCS : 93D129
Société de courtage d'assurance immatriculée au Registre des Intermédiaires en Assurance sous le no 07 029 548.

En complément

Des vidéos produites par la Fédération Bancaire Française en partenariat avec la Direction Centrale de la Police judiciaire sont disponibles sur le site de la FBF via le chemin d'accès suivant :
http://www.fbf.fr

Accueil / La banque des entreprises et des professionnels / Moyens de paiement /

Pour rappel les principales consignes de la FBF :
ORDRES DE VIREMENT DES ENTREPRISES

9 RÉFLEXES SÉCURITÉ

1. Respecter une procédure interne pour l'exécution des virements
2. Sensibiliser spécifiquement les collaborateurs au risque d'escroquerie
3. Être en veille sur les escroqueries aux entreprises
4. Maîtriser la diffusion des informations concernant l'entreprise
5. Faire preuve de bon sens
6. Prendre le temps d'effectuer des vérifications
7. Veiller à la sécurité des accès aux services de banque à distance
8. Sécuriser les installations informatiques
9. Contacter rapidement la banque et la police en cas d'escroquerie (ou de tentative)