

PREVENTION CONTRE LA FRAUDE (ingénierie sociale et cybercriminalité)



Groupe Crédit du Nord



PLUS LOIN, AVEC VOUS

**Banque
Courtois**

**Banque
Kolb**

**Banque
Laydernier**

**Banque
Nuger**

**Banque
Rhône-Alpes**

**Banque
Tarneaud**

**Société
de Banque Monaco**

**Société
Marseillaise de Crédit**

**Crédit
du Nord**

Une fraude en constante progression

Les entreprises sont **toujours autant victimes de fraudes**



7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude



1 entreprise sur 4 a subi au moins une **fraude avérée**

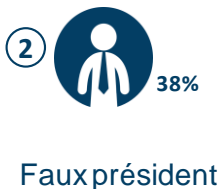


33 % des entreprises attaquées ont subi un **préjudice moyen supérieur à 10 K€**



10 % des entreprises attaquées ont subi un **préjudice moyen supérieur à 100 K€**

Les **5 principales tentatives de fraude**



Les **dispositifs** ayant permis de **déjouer des fraudes**

51%
Réaction ou initiative humaine personnelle



32% Procédures de contrôle interne

17% Dispositif technique (IT)



Fraude par ingénierie sociale (1/2)



FAUX FOURNISSEUR

Usurpation de l'identité d'un fournisseur, d'un bailleur ou de tout autre créancier de l'entreprise (fournisseur d'énergie, d'accès à internet...) pour demander un changement de coordonnées bancaires afin de détourner les prochains règlements de loyers ou de factures.



ALERTES

- Nouvelles coordonnées bancaires domiciliées à l'étranger
- Une adresse mail très proche (à une lettre ou un caractère près) de la véritable adresse du fournisseur



RECOMMANDATIONS

- Sensibiliser le personnel
- Prendre le temps de la réflexion
- Effectuer un contre appel (n° de téléphone et contact référencés)
- Mettre en place une ségrégation des rôles (dissocier saisie et validation des ordres de virements...)
- Mettre en place des procédures internes, une communication et un droit d'alerte



SOLUTIONS BANCAIRES

EBICS TS

Virements sécurisés

SepaMail Diamond

Technique
astucieuse
d'usurpation
d'identité



FAUX PRESIDENT

Consiste à se faire passer pour l'un des dirigeants d'une entreprise afin de convaincre un collaborateur qui a pouvoir sur les comptes bancaires, d'effectuer un virement urgent et confidentiel vers un compte le plus souvent domicilié à l'étranger. Ce virement peut être justifié par une acquisition de société, une remontée de dividende, un contrôle fiscal par exemple.



ALERTES

- Demande urgente et confidentielle
- Non respect des procédures internes
- Virement inhabituel (montant important vers un compte inconnu ou un pays vers lequel l'entreprise n'a pas d'activité)
- Usage de la flatterie / de l'intimidation



RECOMMANDATIONS

- Sensibiliser le personnel
- Ne pas se laisser isoler et communiquer au sein de votre entreprise
- Résister à la pression et se reporter aux procédures internes
- Mettre en place une ségrégation des rôles (dissocier saisie et validation des ordres de virements...)
- Mettre en place des procédures internes, une communication et un droit d'alerte
- Limiter la diffusion d'informations sur les réseaux sociaux



SOLUTIONS BANCAIRES

EBICS TS

Virements sécurisés



Fraude par ingénierie sociale (2/2)



FAUX TEST INFORMATIQUE

Se faire passer pour un prestataire informatique de l'entreprise, voire de la banque, afin de demander l'exécution d'un « virement test » vers un compte domicilié à l'étranger.



ALERTES

- Un interlocuteur vous proposant de l'aide sur vos outils de paiement
- Demande de virement test > 1 €
- Demande de prise en main à distance
- Demande d'identifiant/mot de passe bancaire

La Banque ne sollicite pas le client pour : un virement test, une demande d'information confidentielle, ou la prise de contrôle à distance du PC du client



RECOMMANDATIONS

- Sensibiliser le personnel
- Prendre le temps de la réflexion
- Mettre fin à toute discussion et contacter un interlocuteur référencé chez le prestataire informatique ou la banque
- Mettre en place des procédures internes, une communication et un droit d'alerte



SOLUTIONS BANCAIRES

EBICS TS

Virements sécurisés

Technique
astucieuse
d'usurpation
d'identité



FAUX CLIENT

Consiste à détourner la livraison de marchandises en se faisant passer pour un client.



ALERTES

- Toute modification de l'adresse de livraison d'une commande client



RECOMMANDATIONS

- Sensibiliser le personnel
- Vérifier l'existence du prospect ou du client et de son adresse physique
- Mettre en place des procédures internes, une communication et un droit d'alerte



Cybercriminalité (1/2)



PHISHING (ou hameçonnage)

Escroquerie qui consiste à prendre l'identité d'une entreprise connue sur un e-mail ou sur un faux site internet pour inciter les destinataires à communiquer des informations confidentielles (mot de passe, n° de carte bancaire, ...)



ALERTES

- Mail anxiogène (anomalie, argent bloqué...), service suspendu. Demande de renseignements sur le mail ou sur un site
- Mail promotionnel (gain d'argent, concours gagné...)
- Mail qui comporte souvent des fautes d'orthographe
- Demande d'informations personnelles ou bancaires



RECOMMANDATIONS

- Sensibiliser le personnel
- Avoir un esprit critique par rapport à la demande et faire preuve de prudence en toutes circonstances
- Si connexion sur un site, vérifier que le préfixe « https » est présent devant l'adresse du site
- Mettre en place une solution anti virus et anti malware et veiller à leurs mises à jour

ASSURANCE
CYBER RISQUES

Ensemble
des délits
commis
au moyen du
réseau internet



RANSOMWARE (ou rançongiciel)

Logiciel informatique malveillant prenant en otage les données. Il chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.



ALERTES

- Mail ou spam suspect qui contient un lien hypertexte ou une pièce jointe
- Attention aux clés USB qui vous sont données et qui peuvent contenir des logiciels malveillants
- Ne pas télécharger de logiciels, notamment gratuits, sur des sites inconnus



RECOMMANDATIONS

- Sensibiliser le personnel
- Ne jamais cliquer sur un hyperlien ou une pièce jointe dans un mail suspect et ne pas y répondre
- Mettre en place une solution anti virus et anti malware et veiller à leurs mises à jour
- Maintenir à jour vos logiciels
- Sauvegarder régulièrement vos données sur des disques durs externes déconnectés du réseau
- Mettre en place des audits réguliers de votre système d'information
- En cas d'attaque, déconnecter votre ordinateur du réseau ou l'éteindre. Ne pas payer de rançon.

ASSURANCE
CYBER RISQUES



Cybercriminalité (2/2)



TROYEN

Logiciel qui s'installe sur un ordinateur à l'insu de son propriétaire et qui permet aux fraudeurs de prendre son contrôle à distance.



ALERTES

- Mail ou spam suspect qui contient un lien hypertexte ou une pièce jointe
- Attention aux clés USB qui vous sont données et qui peuvent contenir des logiciels malveillants



RECOMMANDATIONS

- Sensibiliser le personnel
- Ne jamais cliquer sur un hyperlien ou un pièce jointe dans un mail suspect et ne pas y répondre
- Mettre en place une solution anti virus et anti malware et veiller à leurs mises à jour
- Maintenir à jour vos logiciels
- Sauvegarder régulièrement vos données sur des disques durs externes déconnectés du réseau
- Mettre en place des audits réguliers de votre système d'information
- En cas d'attaque, déconnecter votre ordinateur du réseau ou l'éteindre. Ne pas payer de rançon.

ASSURANCE
CYBER RISQUES

Ensemble
des délits
commis
au moyen du
réseau internet



DENI DE SERVICE

Attaque ciblée qui consiste à saturer un site internet (ou un serveur téléphonique) pour le mettre hors service. Des milliers d'ordinateurs contaminés (ex. troyen) sont utilisés simultanément pour attaquer une même cible.



ALERTES

- Pic de surcharge sur votre site internet ou de votre serveur téléphonique



RECOMMANDATIONS

- Mettre en place une solution anti virus et anti malware et veiller à leurs mises à jour
 - Mettre en place des audits, des diagnostics de vos systèmes
 - Mettre en place et paramétrer des infrastructures internet pour suivre et absorber les pics de charge
- Veiller à rendre indépendante l'architecture du site internet de celle de votre base client interne

ASSURANCE
CYBER RISQUES



EBICS TS

EBICS est un protocole de communication sécurisé qui permet l'échange de fichiers entre les clients et les établissements bancaires. Il offre un haut niveau de sécurisation, de fiabilité et de rapidité.

La solution **EBICS TS** est un **processus unique avec l'ensemble de vos banques** pour la télétransmission de vos fichiers d'ordres accompagnés des signatures électroniques des personnes habilitées.

Chaque signataire doit disposer d'un certificat stocké sur une clé USB pour signer ses remises d'ordres. Les Banques du Groupe Crédit du Nord préconisent le certificat 3S KEY (Swift) multi banques et multi pays.



FONCTIONNEMENT

- Emission d'un fichier d'ordres
- Signature du fichier par 1 ou 2 signataires habilités
- Télétransmission en banque du fichier signé
- Après vérifications, la banque traite le fichier d'ordres

Le logiciel de communication bancaire ESP@CE FLUX du Groupe Crédit Du Nord vous permet la télétransmission EBICS avec vos différents partenaires bancaires.

LES CONTRE LA FRAUDE

- Dématérialisation des signatures
- Double signature sur les opérations sensibles
- Maîtrise des pouvoirs de vos signataires : plafonds, signature simple ou double ou double par groupe* (ségrégation des rôles)

Sécuriser et
fiabiliser vos
télétransmissions

* une personne du premier groupe doit obligatoirement signer avec une personne du second groupe



SEPAmail DIAMOND

SEPAmail DIAMOND est un service de vérification des coordonnées bancaires France (BIC + IBAN) d'un client ou d'un fournisseur – personne physique ou personne morale – en préalable d'une opération de virement ou de prélèvement, auprès des Banques partenaires du réseau SEPAmail.

Ce service permet de s'assurer de l'envoi des fonds au bénéficiaire adéquat et supprimer de toute erreur de saisie de coordonnées bancaires.

Vérification
de coordonnées
bancaires
(BIC + IBAN)



FONCTIONNEMENT

- Transmission des BIC/IBAN à vérifier, au format XML via le protocole EBICS ou Swiftnet
- A réception du fichier, la banque transmet les demandes aux banques teneuses des comptes, puis met à disposition les réponses aux demandes de vérifications ainsi obtenues
- La vérification de coordonnées bancaires est valable uniquement sur des comptes ouverts en France

LES CONTRE LA FRAUDE

- SEPAmail DIAMOND permet de détecter si l'IBAN existe vraiment et s'il appartient bien au titulaire présumé du compte
- Vérification de l'IBAN avec le SIREN (si personne morale) ou avec le nom et la date de naissance (si personne physique)



Sécurisation des virements émis

L'offre de sécurisation des virements consiste à contrôler tous les virements SEPA et non SEPA émis via les canaux de télétransmission (EBICS, SWIFT, PESIT/SFTP, e-transfert).

Les vérifications sont effectuées sur la base d'une liste blanche que vous nous aurez transmise, sur laquelle doit figurer les pays destinataires autorisés de virements, avec ou sans bénéficiaire. Il est également possible de gérer des montants plafonds en euros par opération.



FONCTIONNEMENT

- Transmission des listes blanches via le service de télétransmission NORTRANS sous protocole EBICS TS exclusivement
- Envoi d'un SMS d'information au correspondant sécurisé à chaque chargement de liste
- Mise à disposition d'un avis de prise en charge pour chaque rejet d'opération (ARA)

LES CONTRE LA FRAUDE

- Blocage automatique des virements non autorisés par votre liste blanche, quel que soit le protocole d'émission (internet, EBICS, Agence...)

Contrôle des virements SEPA et non SEPA émis



Virements confidentiels

Le service Virement Confidentiel vous permet de protéger vos données sensibles ou confidentielles contenues dans les virements SEPA que vous effectuez.

Par exemple, pour des virements de salaires, de dividendes, ..., les noms et les IBAN (5 derniers chiffres) des bénéficiaires sont masqués sur l'ensemble des restitutions : relevés de compte, avis de prise en charge, rejets...



FONCTIONNEMENT

- Transmission des virements SEPA confidentiels (SCC) à la banque par EBICST, EBICS TS ou SWIFTNET,
- Format de fichier xml identique à celui du virement SEPA non confidentiel (SCT), seul le file format change,
- Débit en compte du montant global des virements compris dans le fichier de virements confidentiels.

Assurer la confidentialité de vos virements SEPA sensibles

LES CONTRE LA FRAUDE

- Protection des données sensibles lors d'émission de virements SEPA
- Permet de désigner des signataires EBICS TS spécifiques



Assurance cyber risques

Suite à une cyber attaque, les conséquences peuvent être nombreuses et importantes pour votre entreprise : vol de données confidentielles, interruption de l'activité entraînant des pertes financières, demandes de rançon, contaminations du système informatique suite à un virus...

L'**assurance cyber risques** vous protège et couvre efficacement votre entreprise contre les risques cyber, de leur gestion à leur indemnisation car elle prend en charge à la fois les coûts financiers d'une attaque cyber et sa résolution. Par ailleurs, si votre activité est à l'arrêt suite à une attaque, les pertes financières subies sont prises en charge.



CRITERES D'ELIGIBILITE

- être client du Groupe Crédit Du Nord,
- être immatriculé en France avec ses éventuelles filiales au sein de l'Espace Economique Européen,
- avoir un Chiffre d'Affaires Global \leq 100 M€
(+ de 30% de ce CA ne doit pas être réalisé aux USA et/ou au Canada)
- disposer d'une procédure de back-up hebdomadaire,
- disposer d'une procédure de restauration des données,
- disposer d'un antivirus, antimalware et pare-feu,
- procéder aux mises au jour de tous les dispositifs informatiques.

LES CONTRE LA FRAUDE

- **Assistance en cas d'incident**
(expertise informatique, conseils juridiques, consultants en gestion de crise, restauration des données...)
- **Prise en charge des dommages subis par l'assuré**
(perte d'exploitation, enquête d'une autorité administrative)
- **Protection en Responsabilité Civile en cas d'atteinte aux données de tiers**

S'assurer
contre les
risques cyber



En cas de fraude avérée

La récupération des fonds dépend des actions engagées simultanément par plusieurs acteurs et en priorité de votre réactivité pour informer la banque.

INGENIERIE SOCIALE

1

. Prévenir votre **hiérarchie** immédiatement

2

. Contacter au plus vite votre **agence bancaire**
 . Faire son possible pour le blocage des fonds
 . Réinitialiser si nécessaire les codes d'accès à vos canaux à distance

3

. Contacter la **police** ou la **gendarmerie**
 . **Déposer plainte** et la **transmettre à votre banque**
 . Demander le gel des fonds par l'intermédiaire d'Europol / Interpol et de l'attaché de sécurité intérieure dans les pays destinataires

Services de police compétents en matière de fraude par ingénierie sociale :

Compétence nationale : Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF). 101, rue des Trois Fontanot 92000 Nanterre. Tél : 01 40 97 84 17

Paris et petite couronne : Brigade des Fraudes aux Moyens de Paiement (BFMP). 36, rue du Bastion 75017 Paris. Tél : 01 87 27 72 00

En province : SRPJ ou Brigade de recherches de la Gendarmerie

CYBERCRIMINALITE

1

. Prévenir votre **hiérarchie** immédiatement
 . Vérifier que le système d'information n'est pas infecté
 . Solliciter un investigateur en cybercriminalité rattaché à chaque Police judiciaire régionale

2

. Informer la **police** et déposer une plainte sur la plateforme « cybermalveillance.gouv.fr »



Crédit du Nord – Société Anonyme au capital de EUR 890 263 248 – SIREN 456 504 851 – RCS Lille – N° TVA FR83 456 504 851 – Siège Social : 28, place Rihour - 59000 Lille – Siège Central : 59, boulevard Haussmann - 75008 Paris – Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 739. **Banque Courtois** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 18 399 504 – SIREN 302 182 258 – RCS Toulouse – N° TVA FR15 302 182 258 – Siège Social : 33, rue de Rémusat - BP 40107 - 31001 Toulouse Cedex 6 – Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 867. **Banque Rhône-Alpes** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 12 562 800 – SIREN 057 502 270 – RCS Grenoble – N° TVA FR82 057 502 270 – Siège Social : 20 et 22, boulevard Edouard Rey - BP 77 - 38041 Grenoble Cedex 9 – Siège Central : 235, Cours Lafayette - 69451 Lyon Cedex 06 – Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 988. **Banque Laydernier** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 24 788 832 – SIREN 325 520 385 – RCS Annecy – N° TVA FR87 325 520 385 – Siège Social : 10, avenue du Rhône - 74997 Annecy Cedex 09 – Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 972. **Banque Tarneaud** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 26 702 768 – SIREN 754 500 551 – RCS Limoges – N° TVA FR69 754 500 551 – Siège Social : 2 et 6, rue Turgot - 87011 Limoges Cedex. Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 953. **Banque Nuger** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 11 444 581 – SIREN 855 201 463 – RCS Clermont-Ferrand – N° TVA FR88 855 201 463 – Siège Social : 5, place Michel de l'Hospital - 63000 Clermont-Ferrand – Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 937. **Banque Kolb** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 14 099 103 – SIREN 825 550 098 – RCS Epinal – N° TVA FR37 825 550 098 – Siège Social : 1 et 3, place du Général de Gaulle - BP 1 - 88501 Mirecourt Cedex – Direction Centrale : 2, place de la République - BP 50528 - 54008 Nancy Cedex. Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 859. **Société Marseillaise de Crédit** – Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 24 471 936 – SIREN 054 806 542 – RCS Marseille - N° TVA FR79 054 806 542. Siège Social : 75, rue Paradis - 13006 Marseille – Société de Courtage d'Assurances immatriculée à l'ORIAS sous le N° 07 019 357. – **Société de Banque Monaco** - Société Anonyme monégasque au capital de EUR 82 000 000 - Siège social : 27 avenue de la Costa - Le Park Palace 98000 Monaco - N° RCI Monaco 19 S08 179 - N° TVA intracommunautaire FR80 000 143 809.

