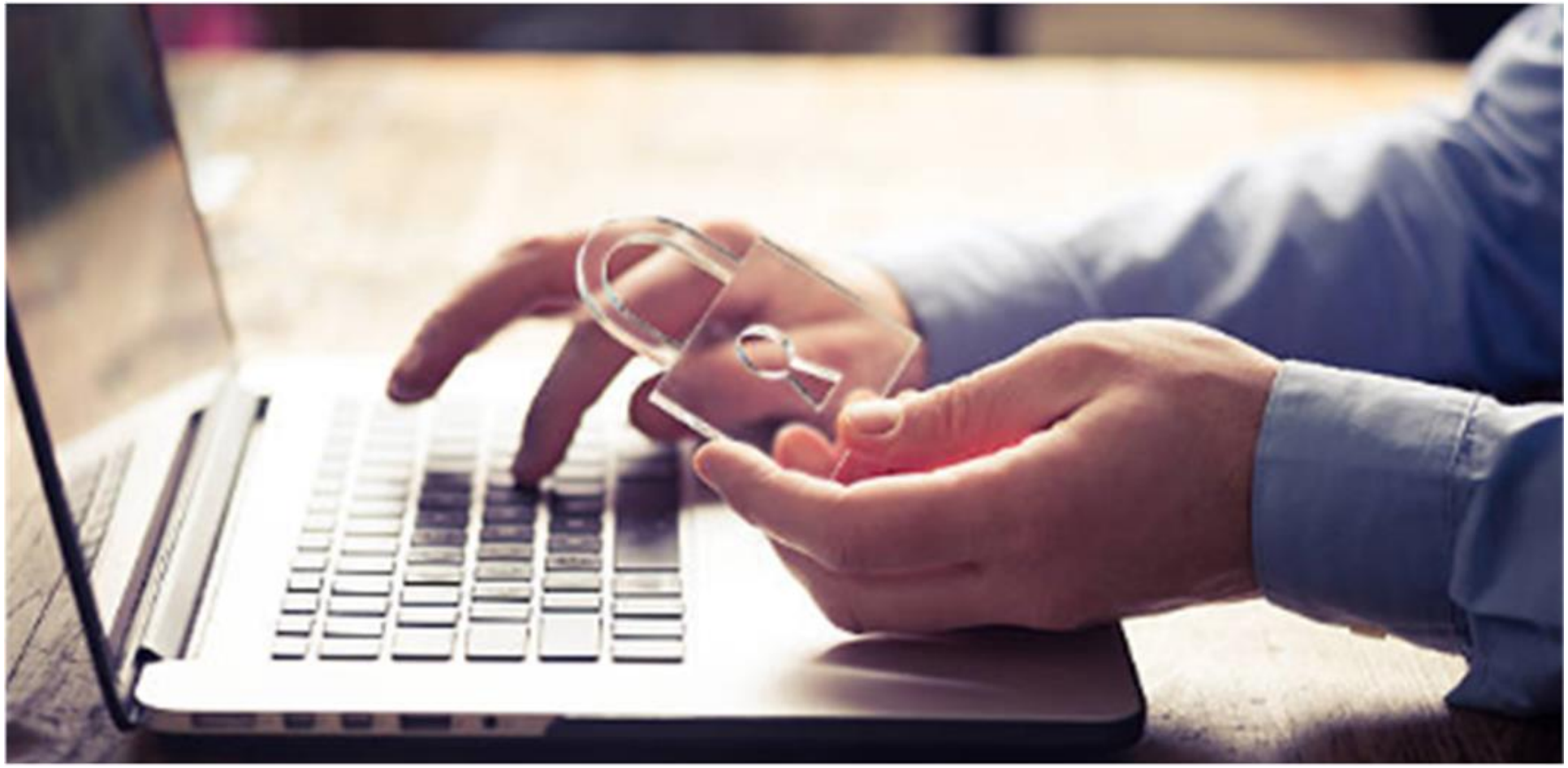
ENTREPRISES PROFESSIONNELS

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**

2 entreprises sur 3 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€**
- 14 % des entreprises attaquées ont subi **un préjudice moyen supérieur à 100 K€**

Les **5 principales tentatives de fraude**

1. **47%** Faux président
2. **46%** Faux fournisseur
3. **38%** Autres usurpations d'identité (banques, avocats, CAC…)
4. **32%** Intrusion dans le SI
5. **25%** Faux client

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

51% Réaction ou initiative humaine personnelle

32% Procédures de contrôle interne

17% Dispositif technique (IT)

Etude Euler Hermès–DGCG – 2021 – panel de 300 entreprises – tous secteurs

Fraude par ingénierie sociale (1/2)

Technique astucieuse d'usurpation d'identité

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 & PARA-BANCAIRES

EBICS TS

OPPENS

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 & PARA-BANCAIRES

EBICS TS

OPPENS

Fraude par ingénierie sociale (2/2)

Technique astucieuse d'usurpation d'identité

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 & PARA-BANCAIRES

EBICS TS

OPPENS

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)

Ensemble des délits commis au moyen du réseau internet

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

SOLUTIONS PARA-BANCAIRES

ASSURANCE CYBER RISQUES

PARTENARIAT CYBERSEC&YOU

OPPENS

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.

SOLUTIONS PARA-BANCAIRES

ASSURANCE CYBER RISQUES

PARTENARIAT CYBERSEC&YOU

OPPENS

Cybercriminalité (2/2)

Ensemble des délits commis au moyen du réseau internet

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.

SOLUTIONS PARA-BANCAIRES

ASSURANCE CYBER RISQUES

PARTENARIAT CYBERSEC&YOU

OPPENS

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

SOLUTIONS PARA-BANCAIRES

PARTENARIAT CYBERSEC&YOU

OPPENS

EBICS TS

Sécuriser et fiabiliser vos télétransmissions

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 ESPACE 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)

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

Partenariat CYBERSEC&YOU (1)

Se protéger contre les risques cyber

Le groupe Crédit du Nord a signé un partenariat avec **Cybersec&You** (2), agrégateur de solutions de cyber-protection pour accompagner et aider les Entreprises, Professionnels, et Institutionnels à **construire un rempart face aux cybercriminels**.

L'offre de protection proposée par notre partenaire Cybersec&You se compose :

d'un **diagnostic cyber offert**, pour analyser votre niveau de protection cyber et vous recommander les solutions à mettre en place pour garantir un niveau de protection minimum

d'un **pack Cybersec&You Elémentaire** qui inclut des solutions permettant de garantir ce niveau de protection minimum :

un **antimalware prédictif** et une **sauvegarde sécurisée et automatisée** (3

de **boucliers** proposant une protection cyber qui s'ajustent aux besoins de votre entreprise et protègent votre système d'information et vos utilisateurs: protection du site web, sécurisation des accès à distance…

NEW

PARCOURS

- Présentation du partenariat et remontée de contact auprès de Cybersec&You pour mise en relation,
- Diagnostic cyber offert,
- A l'issue du diagnostic, un RDV est proposé pour présentation du pack Cybersec&You.

LES + CONTRE LA FRAUDE

- Antimalware **prédictif** composé de moteurs dotés d'Intelligence Artificielle pour contrer des cyber-attaques de plus en plus complexes (4),
- **Sauvegardes et restaurations de données** pour permettre une reprise d'activité suite attaque
- **Des boucliers** pour une couverture complète adaptée aux besoins des différentes organisations
- Offre complémentaire à l'Assurance Cyber risques

(1) Partenariat non disponible pour les clients de la Société de Banque de Monaco. (2) Cybersec&You agissant en qualité de mandataire solitaire d'un groupement comprenant par ailleurs les sociétés Atempo et Metsys. (3) Sauvegardes réalisées sur une box en local et sur un cloud souverain. (4) En lien avec les pratiques ANSSI pour les PME (www.ssi.gouv.fr)

Assurance cyber risques

S'assurer contre les risques cyber

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 =< 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**

OPPENS

Face à la recrudescence des fraudes, Oppens vous propose une offre qui vient compléter l'assurance cyber-risques et les solutions Cybersec&You pour faire face à la cybercriminalité.

Les experts Oppens répondent à une problématique bien réelle : une entreprise ne peut pas être efficacement protégée seulement avec des outils de sécurité. La sensibilisation des salariés est devenu indispensable pour renforcer cette protection. En effet, les criminels ciblent principalement les salariés pour les faire tomber dans un piège, 90% des cyberattaques commencent par un email de phishing.

C'est pour cela qu'Oppens aide à corriger ce risque humain avec une forte sensibilisation de vos collaborateurs sur le sujet à travers :

Sensibiliser et former vos collaborateurs.

- Des exercices de phishing pour évaluer et entraîner vos salariés sur les techniques frauduleuse destinée à les leurrer.
- Des formations pour que vos salariés soient en capacité de comprendre les risques informatiques pesant sur l'entreprise et qu'ils soient en mesure d'appliquer au quotidien les règles et bonnes pratiques nécessaires pour contrer les attaques.
- Des e-learning de modules courts pour un apprentissage approfondi au rythme des apprenants.
- Des entraînements continus permettant à votre entreprise de créer une culture saine et consciente de la sécurité.

PARCOURS

- Présentation du partenariat et remontée de contact auprès de Cybersec&You pour mise en relation,
- **RDV préalablement fixé avec** votre organisation sur les procédures à mettre en place pour lutter contre la cyber criminalité

LES + CONTRE LA FRAUDE

Des prestations de sensibilisations, de formations et de mise en situation des salariés, comme les tests de phishing pour créer un véritable rempart en cas d'attaque.

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). 11, rue des Saussaies 75008 Paris. Tél : 01 49 27 49 27
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 plate-forme « cybermalveillance.gouv.fr »