FRAUDE ET CYBERRISQUES

KIT DE SENSIBILISATION EN ENTREPRISE

2 entreprises sur 3 ont été victimes d'une tentative de fraude en 2021*

Avez-vous pris les mesures pour protéger votre entreprise ?

*D'après le Baromètre Euler Hermes - DFCG 2021

BNP PARIBAS CASH MANAGEMENT

Octobre 2022

BNP PARIBAS

La banque d'un monde qui change

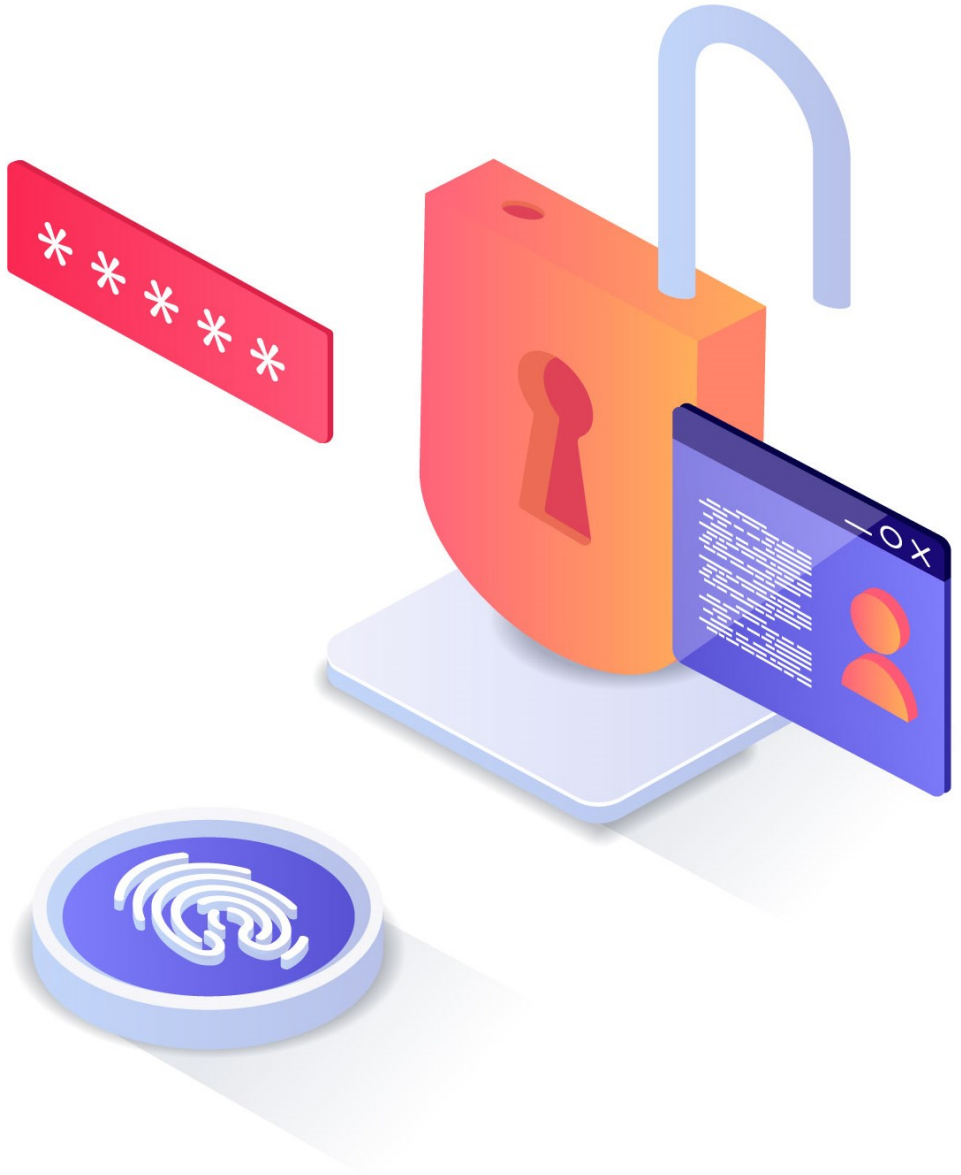
01 INTRODUCTION
Sensibilisez vos équipes !

02 LES DIFFÉRENTS SCHÉMAS DE FRAUDE
Fraude au président, au faux fournisseur...

03 LES TECHNIQUES DE FRAUDE
Vol d'information par ingénierie sociale, usurpation...

04 LES CYBERRISQUES
Hameçonnage, logiciel malveillant, maliciel bancaire...

05 CONCLUSION
Les bons réflexes, en cas de sinistre



SENSIBILISEZ VOS ÉQUIPES !

Pour se protéger contre les fraudes et les risques cyber, il ne suffit pas de mettre en place des procédures, des outils et des contrôles.

Il est très important de sensibiliser et de former vos équipes à détecter et mettre en échec les tentatives de fraudes ou de cyberattaques. En effet, dans la majorité des cas, **les fraudeurs exploitent la faille humaine**.

- **Faites de véritables sessions de sensibilisation** : ne vous contentez pas d'envoyer des emails.
- **N'oubliez pas les nouveaux arrivants, intérimaires**, etc. Ce sont des cibles idéales. Intégrez la sensibilisation au parcours du nouvel arrivant.
- **Formez les équipes de comptabilité et trésorerie, mais n'hésitez pas à sensibiliser tous vos collaborateurs** susceptibles de donner des informations aux fraudeurs ou d'être infecté par un malware.
- **Renouvelez vos sessions de sensibilisation** : les menaces évoluent et la vigilance de vos équipes doit être entretenue.
- **Complétez les sessions de sensibilisation en donnant des consignes écrites** très claires à vos collaborateurs.

Pour vous aider à sensibiliser vos équipes, ce document contient des conseils de bon sens et des consignes concrètes que vous pourrez si besoin adapter à votre entreprise et communiquer à vos collaborateurs.

LES DIFFÉRENTS SCHÉMAS DE FRAUDE

LA FRAUDE AU PRÉSIDENT

EXEMPLE

Votre président vous contacte par e-mail, WhatsApp ou téléphone (vous reconnaissez sa voix !) pour effectuer un virement urgent :

« Nous effectuons une opération financière strictement confidentielle. Je vous ai choisi pour votre discrétion et votre travail irréprochable. Le cabinet juridique vous contactera pour les détails de l'opération. »

https://youtu.be/RbzWx5qiQDc

LES INDICES QUI DOIVENT VOUS ALERTER

- Un email évoquant une acquisition stratégique, un brevet, un contrôle fiscal, etc.
- L'appel d'un avocat d'affaire, conseil juridique, auditeur, policier, etc.
- L'urgence de la situation (acquisition, contrôle fiscal, etc.).
- Le secret et la confidentialité (« surtout n'en parlez pas. Voici un numéro de téléphone pour crypter nos conversations ... »).
- La flatterie (« on m'a dit que je pouvais compter sur vous »).
- L'intimidation (« vous écoutez ce que je vous dis ?! C'est urgent ! »).

SE PROTÉGER

- Sachez que votre équipe de direction ne vous demandera jamais d'exécuter de paiement hors procédure.
- Prévenez vos responsables : une personne bien intentionnée ne peut vous demander de leur cacher des informations.
- Respectez la séparation des pouvoirs :
  - Si vous possédez les droits pour faire des paiements importants tout seul, vous êtes en risque. Parlez-en à votre responsable (personne ne doit posséder les trois pouvoirs de création de compte tiers, saisie de virement, et validation).
  - Evitez les ordres et validations par fax : il est facile pour les fraudeurs de se procurer des spécimens de signature.
  - Les moyens de validation sont personnels : ne les confiez jamais à un collègue, et refusez si un collègue vous confie les siens.
- Procédez à des vérifications de bon sens :
  - Vérifiez les adresses e-mail : les fraudeurs utilisent parfois des adresses ressemblantes (par exemple : jean.dupont@sale-team.com au lieu de jean.dupont@sales-team.com).
  - Vérifiez l'identité de votre interlocuteur en le recontactant à des coordonnées sûres (pas celles communiquées par l'interlocuteur).

À SAVOIR

- Les fraudeurs utilisent des services d'appels dématérialisés et simulent des numéros de téléphone locaux. Ils utilisent des techniques de « phone spoofing » pour afficher de faux noms et numéros de téléphone. ils utilisent également de faux comptes WhatsApp avec les photos de dirigeants.
- Les fraudeurs connaissent souvent parfaitement l'entreprise et savent contrefaire les voix (« deepfake »).
- En cas d'échec de la fraude, le fraudeur peut rappeler le dirigeant lui-même en se faisant passer pour un policier ou pour la banque.

Nous constatons une augmentation du nombre de piratage de boîtes mail, restez donc vigilant même lorsque l'adresse e-mail est légitime.

LA FRAUDE AU PRÉSIDENT

Les signes qui doivent vous alerter

- Spoofing d'email
- Date proche de vacances / jours fériés
- Contexte particulier
- Confidentialité
- Flatterie
- Urgence
- Implication de tierces parties (cabinet juridique / audit…)

RE: Demande à traiter en urgence !

JS

john.smith@qwerty-analysis.com <john.smith@presidency.com>

Mercredi 17 juin à 12:02

À : kate@qwerty-analysis.com

Kate,

Ces derniers mois, nous avons travaillé en coordination avec la SEC et sous leur supervision à l'acquisition d'une entreprise chinoise. Cette offre de reprise doit demeurer strictement confidentielle, absolument personne ne doit en être informé.

Le COVID-19 semble jouer en notre faveur puisque notre offre a été acceptée plus tôt que prévu. L'annonce officielle de ce rachat aura lieu vendredi 4 juillet dans les bureaux, en présence du comité exécutif au complet.

J'ai personnellement choisi de vous confier ce dossier en raison de votre discrétion et de votre travail remarquable au sein du groupe. Merci de contacter sans délai notre cabinet juridique (robert.johns@kpmg-lawyer.com). Il vous transmettra les informations nécessaires afin que vous puissiez transférer les fonds au plus vite.

Merci de m'envoyer un relevé des comptes de l'entreprise.

Ce dossier est extrêmement sensible; aussi, je vous prie de bien vouloir communiquer avec moi uniquement via cette adresse mail (john.smith@presidency.com) afin de ne pas enfreindre les réglementations de la SEC.

John Smith

LA FRAUDE AU FAUX FOURNISSEUR (ET FAUX BAILLEUR, FACTOR…)

EXEMPLE

Votre fournisseur vous contacte par email, téléphone, courrier pour vous notifier un changement de coordonnées bancaires :

« Suite à notre conversation téléphonique, je vous prie de trouver ci-dessous nos nouvelles coordonnées bancaires. »

https://france3-regions.francetvinfo.fr/grand-est/marne/chalons-en-champagne/arnaque-au-faux-president-l-entreprise-cder-de-chalons-en-champagne-escroquee-de-15-millions-d-euros-1962454.html

https://youtu.be/VWplA1pJJsw

LES INDICES QUI DOIVENT VOUS ALERTER

- Toute notification de **changement de compte** bénéficiaire (par courrier, lettre recommandée, par email, sur la facture, par téléphone, etc.).
- Un **changement de coordonnées** d'un fournisseur (email, téléphone …).

SE PROTÉGER

- Lors de toute demande de **modification de coordonnées** (email, téléphone …) ou **changement de compte bancaire, vérifiez l'identité de votre interlocuteur** en le contactant à des coordonnées sûres (et non celles communiquées par lui) **dès réception de la demande**.
- **Soyez très vigilant pour vos plus grands fournisseurs**.
- **Méfiez-vous si le nouveau compte est domicilié à l'étranger** :
  - Code ISO du pays : deux 1ères lettres de l'IBAN et 5ème et 6ème du code BIC.
  - Chypre : CY17002001280000001200527600 - BIC : ABKLCY2N
  - France : FR7630046001290029721519546 -BIC : ABCDFR1N
- **Complétez vos procédures avec une solution de validation de compte, telle que celle fournie par le partenaire de BNP Paribas : ID S.** (sis-id.com). Demandez une démo à votre chargé d'affaires.
- **Désignez quelques personnes responsabilisées, autorisées** à modifier les coordonnées bancaires et téléphoniques.

À SAVOIR

- Les fraudeurs utilisent des **lettres recommandées** depuis 2016.
- La **fraude au loyer** (ou fraude au faux bailleur), est une variante de la fraude au faux fournisseur (attention aux faux actes notariés).
- La fraude au **faux factor** est une autre variante.
- Dans un 1er temps, les fraudeurs **volent de vraies factures** au fournisseur, par email, courrier, téléphone, ou intrusion informatique.
- **Attention** : les fraudeurs utilisent des adresses email ressemblant à celle de votre fournisseur, mais aussi de la vôtre ; ils peuvent ainsi s'interposer dans tous vos échanges d'emails. Voir aussi page 7.

Nous constatons une augmentation du nombre de piratage de boîtes mail, restez donc vigilant même lorsque l'adresse mail de votre interlocuteur est légitime.

LA FRAUDE AU FAUX TECHNICIEN

EXEMPLE

Un escroc se faisant passer pour un technicien de la banque vous contact, prétextant un dysfonctionnement technique.

Par des mécanismes d'emprise psychologique élaborés vous mettant en parfaite confiance, l'escroc parvient à récupérer vos codes d'accès et de validation à vos sites de banque en ligne.

En se connectant ainsi à distance sur vos outils, il est libre d'émettre et de valider des paiements à son profit.

Une variante se basant sur des techniques similaires, consiste purement et simplement pour l'escroc à prendre le contrôle de votre ordinateur, en vous faisant accepter la prise en main de votre PC par ce dernier.

LES INDICES QUI DOIVENT VOUS ALERTER

- **Tout interlocuteur vous proposant de l'aide sur vos outils de paiement** dont vous n'avez pas sollicité personnellement l'intervention, même s'il semble connaître des indications précises sur votre compte : montant de votre solde ou de vos transactions récentes, etc.
- Une **approche** consiste à prétendre que vos paiements pourraient être bloqués si vous ne donnez pas vos codes à votre interlocuteur. **Souvenez vous qu'un employé de la BNP Paribas ne vous demandera jamais vos codes par téléphone ou par mail**.
- Des **questions sur vos outils, processus de paiement ou votre organisation**.
- Une invitation à prendre à distance la main sur votre PC ou une incitation à faire un test de virement.
- Un **lien que vous ne connaissez pas** (par exemple www.id5.com/bnp, www.tin.com/sepa8, www.is.gd/sepabnp, www.tinyurl.com/migration).

Les fraudeurs peuvent appeler leurs victimes après avoir commis une fraude *pour poser des questions en prétendant aider leurs victimes à récupérer leur argent. En réalité, ils cherchent à collecter des informations pour améliorer leur technique de fraude ou gagner du temps avant que vous ne demandiez le recall. Si vous avez été victime d'une fraude et que le fraudeur vous contacte à nouveau,* ***raccrochez immédiatement.***

SE PROTÉGER

- **Ne donnez jamais aucun code à personne** (ex. : numéro généré par votre lecteur sans fil, mot de passe, code PIN ...).
- **Ne vous fiez pas au numéro de téléphone** ou au nom qui s'affiche : les fraudeurs peuvent afficher le numéro de votre chargé d'affaires.
- **Contactez votre interlocuteur habituel** en utilisant des coordonnées sûres pour vérifier l'identité de toute personne prétendant faire partie de nos équipes (ou de votre éditeur, de Microsoft, etc.).
- **Refusez la prise en main à distance de votre PC à toute personne** dont l'identité n'est pas sûre : ne vous rendez pas sur une adresse Internet, ne cliquez pas sur un lien.
- **Ne réalisez jamais de test à la demande d'un technicien** : n'ajoutez pas de compte tiers, ne validez pas de transaction ou de remise. Même de votre initiative, ne faites jamais de test supérieur à 1 €.
- **Protégez votre réseau informatique et vos PC** contre les intrusions informatiques et les logiciels malveillants.

À SAVOIR

- **Aucun technicien BNP Paribas n'est censé vous contacter** pour faire de quelconque mise à jour, maintenance, tests, etc., sauf si vous avez sollicité personnellement l'intervention des équipes d'assistance.
- **Les escrocs connaissent très bien les outils bancaires** ; ils sont souvent au courant des incidents et des opérations commerciales en cours, voire même du nom de votre chargé d'affaires.
- Pour mieux vous berner, le fraudeur peut réaliser des **appels préalables**, au cours desquels il vous aide sans vous escroquer.
- Si vous êtes équipé d'un lecteur sans fil, le fraudeur peut vous dire : « Ne me communiquez surtout pas votre code PIN. **Donnez-moi seulement le code qui s'affiche sur votre lecteur sans fil** ».

- Un nouveau schéma de ce type de fraude consiste à vous contacter pour la **mise à jour de vos boîtiers d'identification**. Soyez vigilant !

LA FRAUDE AU FAUX EMPLOYÉ / FAUX SALAIRE

EXEMPLE

C'est une variante de la fraude au fournisseur :

- L'un de vos employés contacte vos référents RH par email, téléphone, courrier pour notifier un changement de coordonnées bancaires.
- Puis vous payez le salaire sur un compte frauduleux.

RE: Changement de RIB

JS **john.smith@gmail.com** Hier à 12:02

À : kate@qwerty-analysis.com

Bonjour Kate,
Je vous contacte avec mon adresse mail personnelle car je n'arrive plus à me connecter à mon adresse professionnelle depuis hier. J'en ai parlé au support IT mais en attendant leur retour et avec la fin du mois approchant, j'ai préféré vous contacter tout de suite.
J'ai récemment changé de banque et j'aimerai que vous transféreriez mes prochains salaires sur le RIB que vous trouverez ci-joint.
Prévenez moi sur cette adresse mail quand le changement sera effectif.
Cordialement.
John Smith

LES INDICES QUI DOIVENT VOUS ALERTER

- Toute notification de **changement de compte** bénéficiaire (par courrier, lettre recommandée, par email, sur la facture, par téléphone, etc.).
- Un **changement de coordonnées** d'un employé (email, téléphone ...).
- En particulier si le compte est **domicilié dans un pays étranger ou dans une banque qui n'est pas de premier plan (en particulier les néo-banques)**.

SE PROTÉGER

- Lors de toute demande de **modification de coordonnées** (email, téléphone ...) ou changement de **compte bancaire, vérifiez l'identité de votre interlocuteur** en le contactant à des coordonnées sûres (et non celles communiquées par lui) **dès réception de la demande**, par exemple sur **son numéro de téléphone professionnel** (ou son mail professionnel retrouvé dans l'annuaire).
- **Méfiez-vous si le nouveau compte est domicilié à l'étranger** :
  - Code ISO du pays : deux 1ères lettres de l'IBAN et 5ème et 6ème du code BIC.
  - Chypre : CY17002001280000001200527600 - BIC : ABKLCY2N
  - France : FR7630046001290029721519546 -BIC : ABCDFR1N
- **Complétez vos procédures avec une solution de validation de compte, telle que celle fournie par le partenaire de BNP Paribas : ID S.** (sis-id.com). Demandez une démo à votre chargé d'affaires.
- **Désignez quelques personnes responsabilisées, autorisées** à modifier les coordonnées bancaires et téléphoniques.

À SAVOIR

- Les fraudeurs utilisent des **lettres recommandées** depuis 2016.
- Les fraudeurs **connaissent souvent parfaitement l'entreprise** et peuvent utiliser les informations collectées sur internet pour se faire passer pour votre employé.
- **Attention** : jusqu'à présent généralement opérée par email, cette fraude devient de plus en plus sophistiquée et dangereuse. Les fraudeurs n'hésitent pas à appeler par téléphone, contrefaire une voix, etc.
- **Vérifiez les adresses email** ! Les fraudeurs utilisent parfois des adresses ressemblantes (par exemple jean.dupont@sale-team.com au lieu de jean.dupont@sales-team.com) mais attention : il arrive aussi que les fraudeurs écrivent depuis les boîtes mails légitimes des salariés qu'ils ont pu réussir à pirater (ce cas est de plus en plus fréquent) !

LES FRAUDES AU CHÈQUE

EXEMPLE

Envoi d'un chèque puis demande de remboursement par virement

Un client ou un prospect vous fait parvenir un règlement par chèque, d'un montant bien supérieur à la facture. Prétextant une erreur, il vous demande d'encaisser le chèque et de lui retourner par virement l'excédent reçu, moins une commission pour s'excuser de la contrainte. Le chèque se révèlera faux, mais votre virement sera lui bien réel !

Variante : le chèque peut être du bon montant et le faux client peut simplement demander le remboursement par virement, prétextant une annulation.

« Veuillez trouver ci-joint le règlement de la facture pour la location de l'espace pour le séminaire prévu dans 2 mois. »
Le montant est le double attendu

▶

« Mes excuses, j'ai confondu le montant avec celui d'un autre devis. Pouvez vous me virer le surplus ? Je vous prie de conserver 10% supplémentaire pour votre compte afin de m'excuser le dérangement occasionné »

Il existe d'autres typologies de fraudes avec les chèques:

- **Utilisation par un malfaiteur d'un chèque perdu ou volé**.
- **Falsification d'un chèque par un malfaiteur**. Ce procédé consiste à modifier frauduleusement le montant ou le bénéficiaire d'un chèque valide, subtilisé par exemple dans la boîte au lettre du bénéficiaire.

LES INDICES QUI DOIVENT VOUS ALERTER

- **Une personne domiciliée à l'étranger, vous contacte par mail** (rédigé en anglais ou dans un français très approximatif) et se dit intéressée pour acquérir un bien ou service.
- L'acheteur vous envoie alors **un chèque dont la somme est bien supérieure à celle convenue initialement** et trouve une **excuse pour justifier la différence**.
- Il vous demande de lui **restituer une partie** du surplus. Un **dédommagement vous est généreusement accordé** pour vos propres frais et dérangement.

SE PROTÉGER

- **Si vous acceptez les règlements par chèque et recevez un chèque d'un montant supérieur à la vente, nous vous invitons à ne pas l'encaisser**.
- **Ne remboursez jamais un client par virement s'il a payé par chèque avant de vous être assuré auprès de votre banque que le chèque a été dûment encaissé** (le fait que le montant apparaisse sur votre compte ne signifie pas que la banque a déjà vérifié si le chèque était approvisionné).
- Privilégiez dans la mesure du possible les paiements électroniques aux chèques, surtout à l'étranger (délais de traitement long et complexe...).
- Un carnet de chèque doit être conservé dans un lieu sécurisé. Les occasions de vol sont multiples, notamment lors de l'envoi des carnets de chèques.
- **En cas de fraude, signaler les faits à la police ou gendarmerie**. Conservez tous les documents en votre possession (mails échangés avec l'escroc, chèque etc..) afin de faciliter les investigations.

À SAVOIR

- En France, les chèques représente 44% du montant des Fraudes, alors qu'ils ne représentent que 4% des transactions.
- La réglementation n'impose **pas de montant maximum pour un chèque**, mais pour certaines transactions comme par exemple l'achat d'une voiture d'occasion entre particulier, le chèque de banque reste la norme.
- En cas d'erreur dans la rédaction de votre chèque avec **une différence entre le montant en chiffre et celui en lettre, seul ce dernier sera pris en compte lors de son encaissement** ! (en référence à l'article L131-10 du Code Monétaire et Financier).
- Un **chèque émis est valable pendant un an et 8 jours** (à partir de la date de son d'émission).

Un chèque est crédité au plus tard un jour ouvré après son enregistrement. Mais attention ! Ce n'est pas parce que l'argent apparaît sur votre compte bancaire que la somme est réellement disponible ! Un chèque peut être rejeté sous un délai moyen de 8 jours.

LA FRAUDE MONÉTIQUE (CARTE CORPORATE)

EXEMPLE

Une personne mal intentionnée subtilise des données bancaires (Num carte, code CB, code SMS) dans le but de réaliser des paiements à l'insu du titulaire légitime.

« - Bonjour, je suis M. MARTIN, technicien BNPP, je vous contacte par rapport à des transactions inhabituelles détectées sur votre carte de paiements.
- Avez-vous récemment effectué un paiement de 936,5€ chez Leroy Merlin »

Plusieurs typologies de fraude à la carte existent :

- La fraude suite à une perte ou un vol de carte : notamment après observation de votre code, un escroc utilisera la ruse pour vous subtiliser votre carte.
- La fraude par Skimming dit « White Plastic » : un distributeur trafiqué permet à l'escroc de copier votre carte. Pratiqué notamment dans les pays utilisant uniquement la piste de la CB
- La fraude sur internet (VAD / VADS) : vol des données carte
  - SIM SWAP : Certains fraudeurs interceptent le code à usage unique envoyé par SMS par votre banque en se faisant envoyer une carte SIM par votre opérateur téléphonique.
  - Usurpation d'identité d'un tiers de confiance: Les fraudeurs appellent le client en se faisant passer pour une institution connue (Banque de France…), le service fraude de BNP Paribas, ou une entité digne de confiance.

LES INDICES QUI DOIVENT VOUS ALERTER

- Lors de l'appel, le client est mis sous pression face à une urgence, par exemple une fraude en cours.
- L'interlocuteur rassure le client en lui demandant d'annuler les paiements réalisés via la communication du code reçu par SMS. Il s'agit en réalité du code permettant de valider le paiement.

SE PROTÉGER

- Ne pas se fier au numéro affiché, les fraudeurs pouvant simuler un numéro légitime.
- En cas de doute sur l'interlocuteur, raccrocher et rappeler l'interlocuteur habituel, sur des coordonnées de confiance.
- Jamais BNP Paribas ne demandera de valider des opérations par téléphone.
- En cas de mouvement suspect ou doute, changer immédiatement les codes de connexion, et contacter BNP Paribas pour mettre en place les mesures de sécurisation appropriées, par exemple le renouvellement de la carte.
- Renseignez vous et communiquer à vos équipes :

À LIRE ÉGALEMENT
Assurance Banque Epargne – Info Service : Plateforme d'informations sur le monde de la banque mis en place par la BdF, l'ACPR et l'AMF

À VOIR ÉGALEMENT
La fraude à la carte : les bonnes pratiques

À SAVOIR

- En cas de fraude sur votre carte Corporate, Procurement, Virtuelle, Voyage ou Achat BNP Paribas :
- 1. Opposez immédiatement la carte
  - Par téléphone en contactant votre service client dédié ou le centre d'opposition
  - ou en ligne sur le site internet dédié à la gestion de la carte
- 2. Contestez les opérations frauduleuses dans les meilleurs délais

Si vous faites opposition par téléphone, votre interlocuteur vous guidera dans cette démarche. Si vous faites opposition sur internet, le formulaire de contestation est disponible directement en ligne. Vous disposez d'un délai limité pour contester (vous trouverez ce délai dans les Conditions de Fonctionnement de votre carte).

On estime aujourd'hui qu'environ 90% des fraudes actuelles subies par nos clients sont liées à des techniques d'usurpation d'identité par un tiers qui se prétend « de confiance ».

LES TECHNIQUES

LE VOL D'INFORMATION PAR INGÉNIERIE SOCIALE

EXEMPLE

Une personne vous contacte par email, courrier, téléphone pour demander des informations (factures, loyers, coordonnées ...) :

« Dans le cadre de l'examen de votre déclaration de TVA, merci de me communiquer : les références de vos 2 plus importants fournisseurs, ainsi qu'un extrait de compte et un duplicata de facture pour chacun. »

https://youtu.be/z2lDrLzjX4c

À VOIR ÉGALEMENT
Dave le medium (en anglais)

LES INDICES QUI DOIVENT VOUS ALERTER

- **Toute personne inconnue** vous contactant sous un prétexte quelconque pour vous demander une information, même anodine.
- Une demande de factures, d'informations sur vos clients, vos loyers, etc. émanant d'un **prétendu client, commissaire aux comptes, inspecteur**...

SE PROTÉGER

Vérifiez l'identité de toute personne réclamant des informations

- Ne donnez pas d'informations à des **personnes inconnues** (chasseurs de tête, institut de sondage, collègue inconnu, impôts...).
- Méfiez-vous en particulier de toute personne réclamant des informations sur vos **factures, loyers, paiements, clients, fournisseurs**, procédures, outil de paiement, etc. (attention aux faux clients, commissaires aux comptes, administrations publiques...).
- Vérifiez l'identité de votre interlocuteur à ses **coordonnées habituelles** (et non celles communiquées par votre correspondant).

Limitez la diffusion d'information

- Limitez la **diffusion d'informations sur Internet** (réseaux sociaux, blogs, sites internet, site du comité d'entreprise ...).
- Ne diffusez pas de documents potentiellement sensibles (modèles de courrier, **signatures**...).
- Si possible, utilisez des **signatures différentes** pour vos mandats bancaires et pour vos actes publiques (statuts...).
- Soyez **discret à l'extérieur de votre entreprise** sur votre rôle (préparation des paiements, pouvoirs bancaires...).

Si possible, chiffrez vos données sensibles et utilisez TLS pour vos échanges d'emails avec l'extérieur.

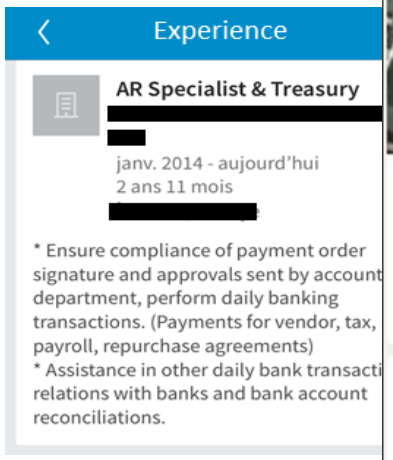
À SAVOIR

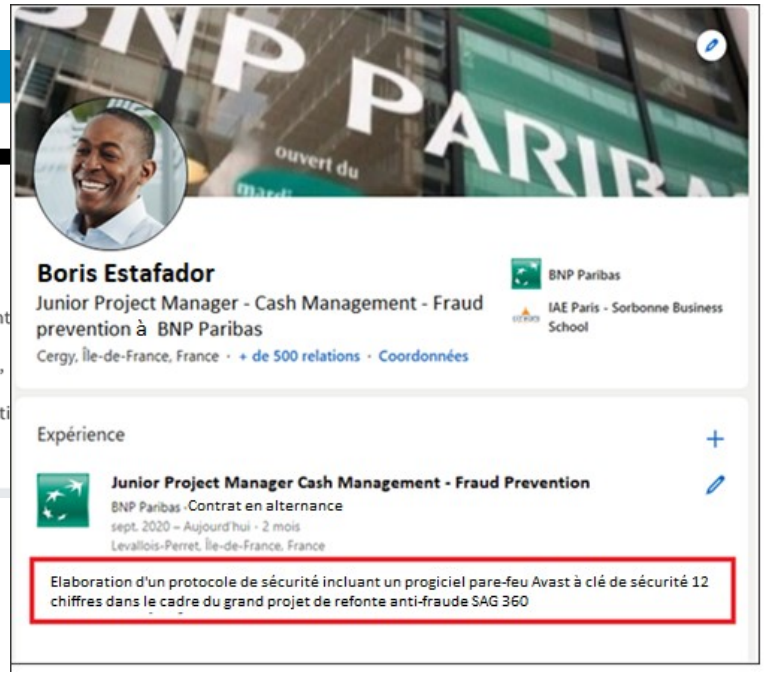
- **Toute information même anodine** peut avoir de la valeur pour un fraudeur (date de vacances, adresse email, noms des enfants, etc.).
- **« Internet n'oublie jamais »** : une fois qu'une information a été publiée sur Internet, il est extrêmement difficile de la supprimer.

LA COLLECTE DE DONNÉES PAR INGÉNIERIE SOCIALE

Méthodes de collecte de données utilisées par les hackers

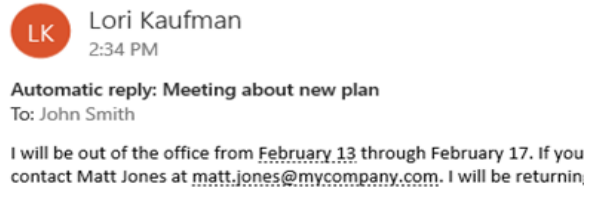
Collecte de données sur les réseaux sociaux, les registres des entreprises, les messages automatiques d'absence…





Companies House

KOMPASS



Appels de faux auditeurs, voyagistes, chasseurs de tête, administrations publiques, hotline…

Appels en "Voice over IP" simulant des numéros locaux, usurpation des numéros appelant, logiciels de changement de voix, déviation des lignes téléphoniques…

WhatsApp

voxbone
Local numbers, Global network

LE « SPOOFING » D'E-MAIL (USURPATION D'EMAIL)

EXEMPLE

Les fraudeurs utilisent souvent des adresses email qui ressemblent à celle de la personne dont ils usurpent l'identité : c'est le « spoofing » d'email, dont voici quelques recettes :

- Faux email dans l'alias : bill.gates@microsoft.com <fraud@gmail.com>
- Utilisation d'un sous-domaine: bill.gates@microsoft.presidency.com
- Autre adresse dans "Répondre à" :
- De: bill.gates@legit-company.com
- Répondre à: bill.gates@legit-company.presidency.com
- Utilisation d'un tiret ('-') : bill.gates@microsoft-corp.com
- Utilisation de caractères holographiques : remplacer 'O' par '0', 'l'' par 'i' capital, 'I' ou 'L' par '1', etc. : bill.gates@1egit-company.com
- Domaine avec une faute : bill.gates@nnicrosoft.com
- Domaine avec une extension peu courante : bill.gates@microsoft.top

Plus rarement, les fraudeurs falsifient les en-têtes d'email, ou même piratent l'accès à la messagerie de l'expéditeur.

LES INDICES QUI DOIVENT VOUS ALERTER

- La plupart des indices qui doivent alerter proviennent de **l'objet ou du contenu de l'e-mail** lui-même (demande d'information, virement urgent, changement de compte ...), ou de son expéditeur, inhabituel ou inconnu.
- En règle générale, soyez attentifs aux **adresses emails des expéditeurs**, et particulièrement lorsque l'objet ou le contenu d'un email est suspect.
- Un email aboutissant dans votre boîte de « **spams** » (ou indésirables) a plus de probabilité d'être un email usurpé.

SE PROTÉGER

Vigilance lors de la réception d'un email

- En cas de doute sur un email, le plus efficace est de procéder à un **contre-appel de l'expéditeur** à des coordonnées sûres.
- Apprenez à **vérifier attentivement les adresses email**, en cas de demande suspecte ou sensible, ou en cas d'expéditeur inhabituel. Pour ceci, apprenez à lire les **en-têtes détaillées** d'emails.

À LIRE ÉGALEMENT
Instructions pour lire les en-têtes

Filtres et authentification d'email

- Votre service informatique peut surveiller ou réserver les **noms de domaine** semblables au vôtre.
- Il peut aussi **filtrer les emails non authentifiés** par les protocoles standards : SPF, DKIM, DMARC. Il peut si besoin mettre en place des mécanismes de liste noire et/ou liste blanche de noms de domaine.
- Si possible, marquer 'EXTERNE' les emails issus de l'extérieur.

À SAVOIR

Le fraudeur peut usurper non seulement l'adresse de votre correspondant mais aussi la vôtre. Il vous transmet les réponses qu'il reçoit de votre interlocuteur, et vice-versa. **L'illusion est alors parfaite**.

Crédit : Shutterstock

LES CYBERRISQUES

LA FRAUDE PAR « PHISHING » (HAMEÇONNAGE)

EXEMPLE

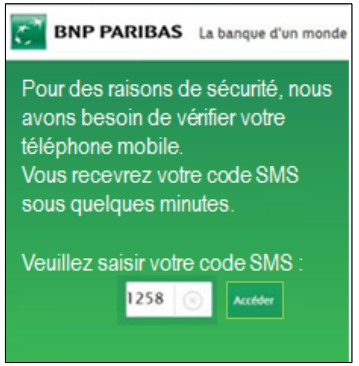
Vous recevez un email semblant provenir de votre banque. Si vous cliquez sur le lien, une **fausse page** de la banque s'ouvre, et vous demande des informations (mots de passe, numéro de carte bancaire, etc.). Parfois, le fraudeur parvient aussi à vous voler un code SMS envoyé par votre banque pour valider un compte ou un achat par carte.

Vous avez de nouveaux messages

J **john@bnpparibas.com** Hier à 12:02

À : kate@qwerty-analysis.com

Bonjour,
Vous avez (2) nouveaux message Sur Votre Messagerie.
Consulter Votre Messagerie, en cliquant Sur Le lien ci-dessous :
Votre Messagerie



Le phishing est très courant, et peut concerner **votre opérateur téléphonique, votre fournisseur d'électricité ou de gaz, l'administration, votre messagerie électronique en ligne, les réseaux sociaux, etc.**

À LIRE ÉGALEMENT
« Les dernières alertes » sur la page sécurité du site BNP Paribas

LES INDICES QUI DOIVENT VOUS ALERTER

- Tout email semblant provenir d'une institution (banque, fournisseur, client, Google, Facebook, LinkedIn…), avec un lien ou une pièce jointe.
- Une sollicitation inattendue semblant avoir une logique.
- Un objet alarmiste ou incitatif poussant à cliquer ou ouvrir un fichier.
- N'importe quelle inconsistance (fautes d'orthographe, logo ancien …).

SE PROTÉGER

- **Adoptez les bons reflexes !**
  - Vérifiez attentivement **l'objet** et le **contenu** ainsi que **l'adresse email** de l'expéditeur des emails que vous recevez.
  - En règle générale, n'ouvrez pas les pièces jointes et **ne cliquez sur aucun des liens** ou images cliquables contenus dans un email.
  - Pour ouvrir un site web, **ne cliquez pas sur un lien : utilisez l'application mobile, ou saisissez son adresse** dans votre navigateur. Vérifiez dans l'adresse la présence de **https://** et du **cadenas**.
  - Si par erreur, vous ouvrez un lien proposé dans un email, ne saisissez **ni mot de passe, ni code envoyé par SMS**.
  - **N'ouvrez pas et ne répondez pas aux emails douteux**, et n'appelez pas les numéros de téléphone qu'ils contiennent.
- **Utilisez l'authentification forte proposée par votre banque. Activez l'authentification à 2 facteurs sur Gmail, Hotmail, etc.**

À VOIR
7 conseils pour naviguer en sécurité

À SAVOIR

- Certains fraudeurs interceptent le **code à usage unique envoyé par SMS** par votre banque en se faisant envoyer une carte SIM par votre opérateur téléphonique. Si vous rencontrez une **anomalie avec votre téléphone mobile** (perte prolongée de réseau) vous pouvez contacter votre opérateur.
- On appelle « **harponnage** » ou « **spear phishing** » une attaque par phishing sophistiquée au cours de laquelle le fraudeur vous a spécifiquement ciblé et adapte son attaque à vos habitudes.
- Vous pouvez **vérifier un lien sans cliquer dessus** en le survolant avec la souris (l'adresse s'affiche en bas de votre navigateur).

L'INFECTION PAR UN LOGICIEL MALVEILLANT (« MALWARE »)

EXEMPLE

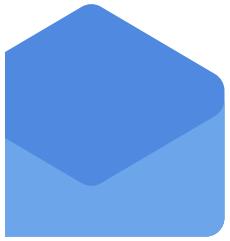
Un malware est un logiciel malveillant que vous installez à votre insu généralement en cliquant sur un lien ou en ouvrant un document.

Régularisation d'impayé – Facture F00012

SC **Service comptabilité** Hier à 12:02

À : kate@qwerty-analysis.com

L'examen de votre compte fait apparaitre qu'à ce jour, sauf erreur de notre part, le paiement de notre facture F00012 d'un montant de 372 € ne nous est pas parvenu.
Vous pouvez télécharger un duplicata de la facture à cette adresse : Télécharger ma facture
Nous vous prions de bien vouloir procéder à son règlement dans les meilleurs délais.



nptabilité Hier à 12:02

F00012.doc
29 Ko

Vous trouverez en pièce jointe la facture toujours en attente de règlement d'un montant de 1927.80 €.

LES INDICES QUI DOIVENT VOUS ALERTER

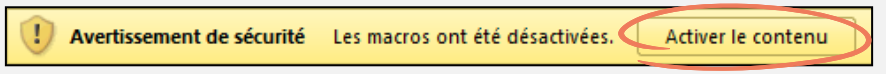
- Tout email d'un **expéditeur inconnu** avec un lien ou une pièce jointe.
- Tout email ayant un **objet ou un contenu inattendu**.
- Tout document envoyé par email ou téléchargé **contenant une macro**.

ATTENTION : nous pouvons tous être le vecteur d'une infection par un malware. Les conséquences peuvent être gravissimes : espionnage, vol massif de données, virements frauduleux, cryptage de toutes les données de l'entreprise (pertes d'exploitation)...

SE PROTÉGER

- Lors de la réception d'un email
  - Connaissez-vous l'expéditeur ? Son adresse paraît-elle habituelle ? Attendiez-vous cet email ? L'objet ou le message est-il inhabituel ?
  - En cas de doute, n'ouvrez **ni les pièces jointes ni les liens**.
  - Il peut arriver qu'un email frauduleux émane d'un de vos **contacts habituels** si son poste a été infecté. En cas de doute, contactez-le.
- Si vous ouvrez une pièce jointe reçue par email
  - Faites-le sur votre PC protégé par un antivirus, pas sur votre smartphone ou votre PC privé (souvent démunis d'antivirus).
  - Surtout, n'autorisez pas l'exécution des **macros** :

Ne pas cliquer !



- Protégez vos installations informatiques
  - Mettez à jour le système d'exploitation et l'antivirus **chaque jour**.
  - **Restreignez les droits d'installation** de logiciels aux administrateurs.
  - N'autorisez pas l'exécution automatique des macros.
  - **Bloquez les clés USB** et sites de partage de documents.
  - **Filtrez** les pièces jointes contenant du code Visual Basic (macros).
  - Vérifiez les **accès à distance RDP** (VPN ou mot de passe fort) et l'absence de faille sur vos sites web (ex : sur les formulaires Web).
  - Evitez de surfer sur des sites web inconnus (forum, blog, sites vitrines, marketplace etc.)
  - Si possible, **segmentez** votre réseau informatique.

À SAVOIR

- Les malwares ne sont souvent **pas détectés par les antivirus**.
- Les fraudeurs utilisent des **liens vers des fichiers** hébergés sur DropBox, Google Drive, ... ou sur des sites de PME piratés, pour déjouer les filtres.
- De plus en plus de malwares/trojans peuvent s'exécuter sur vos machines sans actions de votre part, uniquement en visitant un site web présentant des failles de sécurité.

LA FRAUDE PAR MALICIEL (MALWARE) BANCAIRE

EXEMPLE

Un malware peut créer un virement sur votre site bancaire. Il peut notamment afficher une fausse page de validation pour vous voler un code de validation :

Page de connexion normale

BNP PARIBAS

Accédez à vos comptes

Numéro d'abonné

12345678

Votre clé d'accès

******

Se connecter

Fraude : signature à la connexion

BNP PARIBAS

FRAUDE

Accédez à vos comptes

Pour procéder à la validation

1. Saisissez le challenge sur votre lecteur, et entrez le code PIN
2. Saisissez la réponse et confirmez

Challenge : 9876 5432

******

Confirmer

SE PROTÉGER

- Faites un bon usage de vos applications de paiement
  - Ne vous connectez pas en cas de suspicion de piratage ou malware. En cas de doute, contactez au plus vite votre **chargé d'affaires**.
  - **Déconnectez-vous** de votre application et débranchez votre moyen de validation après chaque session. Supprimez également les données de navigation présentes sur votre navigateur.
  - Ne communiquez jamais vos **identifiants, mots de passe, codes de validation**, etc. à qui que ce soit, et de quelque manière que ce soit.
  - Evitez de vous connecter depuis un **PC ou smartphone privé** ou depuis un **réseau Wi-Fi public**.
- Séparez les rôles
  - Evitez qu'une même personne dans votre entreprise puisse créer un compte tiers et valider un virement.
  - La séparation des rôles n'est pas sûre à 100% contre les malwares bancaires, mais elle est souvent efficace.
- Protégez vos installations informatiques
  - Mettez à jour le système d'exploitation et l'antivirus **chaque jour**.
  - Voir les autres conseils en page 18.

LES INDICES QUI DOIVENT VOUS ALERTER

- Une **page de validation inhabituelle**, ou apparaissant après une indisponibilité ou des lenteurs de l'outil bancaire.
- Des **échecs d'authentification** successifs et potentiellement anormaux.
- Des **lenteurs**, un **trafic du réseau** anormalement élevé, une **activité plus élevée du disque**, des **modifications de fichiers**, signes potentiels d'un piratage ou d'une infection de votre PC ou smartphone.

À SAVOIR

- Découvrez la solution **Flux Sécurisés** de BNP Paribas, protection efficace et personnalisée contre la fraude au virement (et particulièrement la fraude par malware).
- Votre **chargé d'affaires** est à votre disposition pour vous conseiller. Contactez-le !

UN RISQUE MAJEUR : LES RANÇONGICIELS (RANSOMWARES)

EXEMPLE

Un malware se répand dans votre réseau informatique, et y chiffre tous les fichiers. Il affiche un message exigeant le paiement d'une rançon, en échange d'une clé cryptographique pour décrypter vos données.

LES INDICES QUI DOIVENT VOUS ALERTER

- Un **soupçon d'infection** par un malware (par exemple : exécution d'une macro dans un document douteux par un employé ...).
- Une page vous annonçant que **vos données on été cryptées**.

SE PROTÉGER

- En cas d'attaque
  - **Déconnectez** tous les PC infectés du réseau pour stopper la propagation.
  - Les forces de l'ordre **déconseillent fortement de payer** la rançon.
- En prévention
  - Faites des **sauvegardes régulières** de vos données importantes.
  - **Limitez l'accès au répertoire de stockage** des sauvegardes (les ransomwares cherchent à crypter les sauvegardes).
  - Stockez régulièrement des **sauvegardes déconnectées**.
  - **Testez** régulièrement vos sauvegardes.
- Préparez un plan d'actions en cas d'attaque
  - Discutez à l'avance avec votre **responsable informatique**.
  - Prévoyez un **plan de secours** pour vos processus vitaux.
- Souscrivez une cyberassurance
  - Couverture des coûts d'expertise, de **perte d'exploitation**, etc.
  - Accès à une **assistance informatique** et à des actions d'expertise.

À SAVOIR

- Parfois, les escrocs menacent de **divulguer publiquement les données compromises** si l'entreprise ne paie pas la rançon.
- En général, le coût d'une attaque est au **minimum de 40.000 €**. Les préjudices les plus élevés atteignent des centaines de millions d'€.

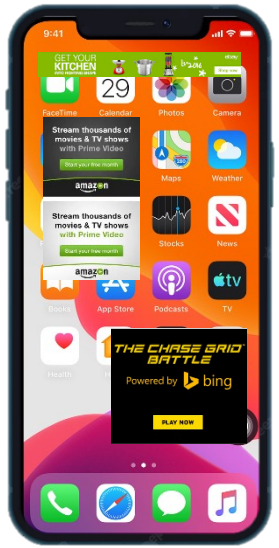
En 2020, l'ANSSI note ainsi une augmentation de 255% des signalements d'attaque par rançongiciel dans son périmètre par rapport à 2019. (source : État de la menace rançongiciels à l'encontre des entreprises et institutions – CERT-FR (ssi.gouv.fr))

LES SMARTPHONES : LA NOUVELLE CIBLE DES PIRATES

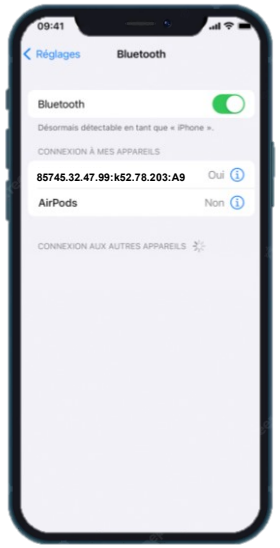
EXEMPLE

Android, IOS, WinPhone : aucun OS de smartphone n'échappe au piratage. Nos smartphones sont remplis d'informations confidentielles (SMS, Mail, Photo, Réseaux Sociaux etc.) et sont souvent sans défense, une mine d'or pour un pirate !

Exemple de ransomware



Exemple de Adwares



Exemple de Piratage via réseaux

LES INDICES QUI DOIVENT VOUS ALERTER

- **Des publicités omniprésentes** sur votre smartphone en dehors des applications
- Des appareils Bluetooth **non identifiés** enregistrés
- Des applications installées en dehors des **stores officiels**
- Des **appels ou messages** inhabituels dans vos historiques

SE PROTÉGER

- Evitez les pièges
  - Ne jamais télécharger d'application en dehors des magasins officiels (Apple Store, Play Store)
  - Ne jamais exécuter des fichiers : .apk, .ipa, .script etc... sur son smartphone
  - Désactivez après utilisation les fonctions NFC, Bluetooth et Infrarouge (pour les téléphones compatibles)
  - Ne rechargez pas votre smartphone sur les bornes USB en libre-service
  - Vérifiez la légitimité des accès aux données d'une application
  - Toujours activer l'authentification à deux facteurs (2FA) si possible
  - Ne débridez (jailbreakez) pas votre téléphone.
- En cas d'attaque
  - Prévenez toutes les personnes qui ont pu recevoir des messages frauduleux provenant de votre téléphone
  - Changez les mots de passes des applications sensibles
  - Contactez rapidement le support de la marque de votre téléphone
- En prévention
  - Faites des **sauvegardes régulières** de vos données importantes.
  - Ne stockez pas vos données sensibles ou mots de passe sur votre smartphone
  - Évitez au maximum les wifi publics ou réseaux internet non protégés (ou utiliser un VPN)

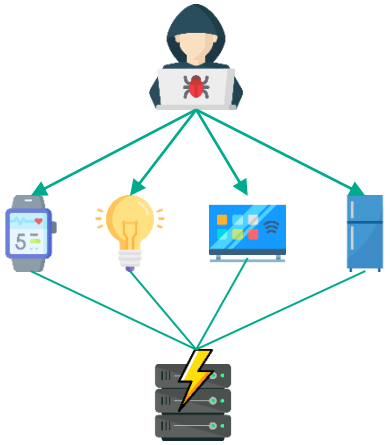
À SAVOIR

- 1 smartphone Android sur 36 a des applications à risque installées
- Début 2022, découverte des techniques de « Noreboot » sur iPhone qui permet à un pirate de contrôler à distance les caméras et microphones du smartphone sans être détecté

LES OBJETS CONNECTÉS, LA PORTE OUVERTE AUX PIRATES

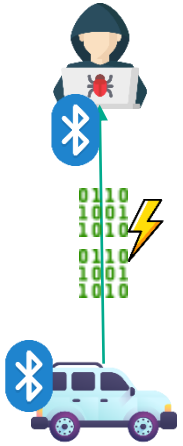
EXEMPLE

Depuis quelques années, les IOT (Internet of Things) ont envahi nos foyers. La particularité de ces appareils et d'être directement relié à Internet. Nous pouvons retrouver les : télévisions, montres, enceintes, caméras de sécurité, ampoules, réfrigérateurs, baby-phones etc. Cependant ces appareils sont trop souvent dépourvus de systèmes de sécurité, laissant le champs libre aux pirates...



Attaque DDoS

Écoute active



Vol de données (Blueborne)

LES INDICES QUI DOIVENT VOUS ALERTER

- Une utilisation intensive de vos appareils même quand ceux-ci ne sont pas utilisés (chaleur)
- Une activité anormale sur votre box internet (augmentation de la consommation internet)
- Un changement de comportement des objets connectés (changement de langue, erreur etc.)
- Des fichiers subitement cryptés marquants des dysfonctionnements de l'appareil

SE PROTÉGER

- Se prémunir des attaques
  - Désactivez les comptes démo ou invité de vos objets connectés
  - Modifiez les mots de passes d'origine des IOT pour des combinaisons plus fortes
  - Mettre en œuvre si possible des méthodes de chiffrement
  - Evitez de connecter votre ordinateur professionnel à un réseau disposant d'IOT, sinon utilisez le VPN fourni par votre entreprise
  - Mettez régulièrement à jour vos appareils pour corriger les vulnérabilités
- Lors d'une attaque
  - Déconnectez vos appareils d'internet pour interrompre l'attaque
  - Changez le mot de passe de vos appareils
  - Réalisez une recherche de mise à jour pour bénéficier des derniers patchs de sécurité

À SAVOIR

- Vos IOT disposent comme votre ordinateur d'une adresse IP visible par tous le monde sur le web. Un simple balayage d'adresse IP sur internet permet de trouver des millions d'objets connectés non protégés
- Le site *Shodan* permet de trouver tous les objets connectés ayant une adresse IP visible sur internet (donc non protégés)
- Le site *Insecam* permet d'accéder à des milliers de caméras de surveillance non protégées et de pouvoir les consulter à tout moment

Même les appareils connectés les moins risqués peuvent subir des attaques. C'est le cas en 2020 avec une vague de ransomware visant à infecter les machines à café connectées les rendant inutilisables si leurs propriétaires ne payaient pas la rançon

CONCLUSION

LES BONS RÉFLEXES : FAITES PREUVE DE BON SENS !

En cas de demande de virement inhabituel

- **Prévenez votre hiérarchie**.
- Ne cédez pas à l'urgence.
- Respectez la **séparation des pouvoirs** et les procédures.
- Vérifiez l'identité de votre interlocuteur à des **coordonnées sûres** ou en passant par le standard.

En cas de changement de compte fournisseur

- Vérifiez **dès réception de la demande** l'identité du demandeur à des **coordonnées sûres**.
- Vérifiez aussi les **changements de coordonnées téléphoniques**.
- Pour les **gros fournisseurs** et les **comptes étrangers**, soyez vigilants.

En cas d'appel d'un technicien

- Contactez votre **chargé d'affaires** (ou éditeur) à ses coordonnées.
- Refusez la **prise en main à distance** de votre PC.
- Ne réalisez **jamais de test** supérieur à 1€.
- Ne donnez jamais **aucun code** à personne, pas même à la banque.

En cas de demande d'information

- Ne donnez pas d'informations à des **personnes inconnues**.
- Méfiez-vous si l'on vous réclame des **informations comptables**.
- Vérifiez l'identité de votre interlocuteur à des **coordonnées sûres** ou en passant par le standard.

Sur les réseaux sociaux et en public

- Soyez discret sur les **réseaux sociaux** et en public sur vos fonctions et pouvoirs.
- Ne **publiez pas d'informations** utiles aux fraudeurs sur les sites web (organigrammes, actualités sur les déplacements du président, etc.).
- Si possible, utilisez une **signature distincte** pour les actes publics (statuts, etc.).

En cas de réception d'un email inhabituel

- Méfiez-vous des **emails inhabituels**, même s'ils proviennent d'un expéditeur que vous connaissez.
- **Ne touchez ni aux pièces jointes ni aux liens** : allez directement sur votre app ou votre site web sans cliquer sur un lien, ou appelez votre interlocuteur à des coordonnées sûres.
- **Si vous cliquez sur un lien dans un email, n'y saisissez rien**.
- Si vous ouvrez un document reçu par email, **n'autorisez pas l'exécution des macros**.

Lorsque vous utilisez vos outils de paiement

- **Séparez les rôles**, utilisez des plafonds, ne validez pas par fax.
- Ne vous connectez pas **sur un PC ou smartphone privé ou depuis un réseau Wi-Fi public**.
- **Débranchez** votre moyen de validation après chaque visite
- Vérifiez l'adresse du site, ainsi que la présence du **https://** et du **cadenas**.
- Méfiez-vous des **pages de validation inhabituelles**.
- En cas de doute, **contactez votre chargé d'affaires**.

Protégez votre système d'information

- **Mise à jour** système et antivirus.
- **Accès à distance RDP** : mots de passe forts ou VPN.
- Attention aux **failles des sites web** (ex. formulaires Web).
- Si possible **segmentation réseau**.
- **Blocage des clés USB** et des sites de partage de fichiers.
- **Sauvegardes** régulières testées.
- **Authentification des emails** (SPF, DKIM, DMARC) + usage de TLS.
- Filtres emails, liste blanche.
- Veille sur les noms de domaine.
- Si possible, chiffrement des données sensibles.

EN CAS DE VIREMENT FRAUDULEUX (OU SUSPICION)

1

Prévenez votre hiérarchie et préservez la preuve.

CONTACTS EN CAS D'URGENCE

2

Contactez immédiatement votre chargé d'affaires.

CONTACTS EN CAS D'URGENCE

3

Contactez immédiatement la police ou la gendarmerie en cas de fraude avérée

CONTACTS EN CAS D'URGENCE