SENSIBILISATION AUX
RISQUES CYBER

28 février 2023

Présentation des **Animateurs**

Direction Zonale de la Police
Judiciaire de Bordeaux
DZPJ Sud-Ouest
Hôtel de Police
23 rue François de Sourdis
33062 BORDEAUX

En cas de suspicion ou d'attaque le seul contact à retenir :

cybermenaces-bordeaux@interieur.gouv.fr

Pierre LABORDE

Réserviste Police Nationale

Commandant Divisionnaire

Gaël MANCEC

Réserviste Police Nationale

Juriste NTIC

Réseau des référents Cybermenaces

RCM

POLICE NATIONALE

- Dispositif lancé le 09 Mars 2018
- **But du RCM** : **sensibiliser** le tissu économique local aux risques cyber et apporter un **premier niveau d'assistance** aux victimes
- Composé **d'enquêteurs de PJ** et de **réservistes** du secteur privé ou public
- **Dans le Sud-Ouest :** 30 réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux

Point de contact pour les entreprises en Nouvelle-Aquitaine :

cybermenaces-bordeaux@interieur.gouv.fr

RCM
POLICE NATIONALE
DCPJ • RÉFÉRENT CYBER MENACE

RÉGION
Nouvelle-Aquitaine

POLICE NATIONALE

PLAN

1- Etat de la menace

2- Identification des différents types d'attaques

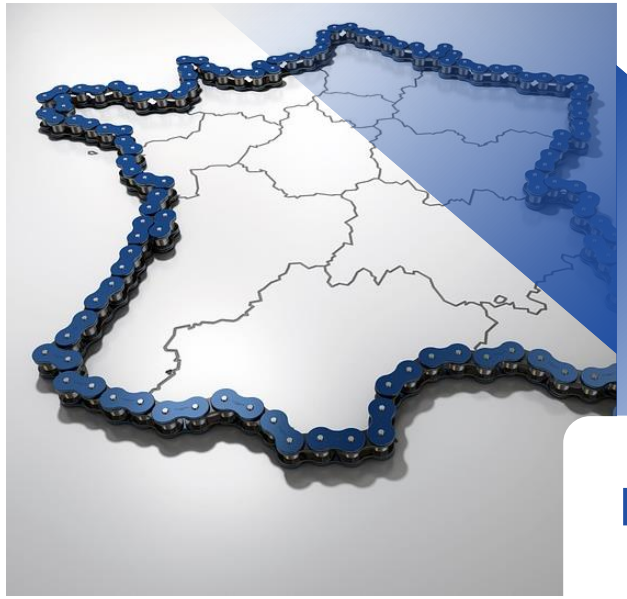
3- Présentation de cas réels

4- Bonnes pratiques

5- Signalement et dépôt de plainte

Évolution de la criminalité organisée **depuis 20 ans**

POLICE NATIONALE



Historique…

Evolution d'une délinquance en bande organisée au niveau national …

Actuel

… à une délinquance en Groupe Criminel Organisé (**GCO**) transnational

Il s'agit de **cybercriminalité** et de **vrais criminels** .

Les cybercriminels travaillent par spécialités

POLICE NATIONALE

Les concepteurs de malware

Programmateurs expérimentés trouvant des débouchés économiques plus importantes dans la criminalité

Conçoivent seul ou en équipe les souches ou les variants de virus, vers, cheveaux de Troie, Keylogger, etc.

Ces malwares sont ensuite revendus ou loués sur des plateformes de cybercriminels, avec leur notice d'utilisation et leur tutos. Les gains sont parfois partagés avec les exploiteurs.

Les ouvreurs de portes

Modes opératoires:

. E-mail frauduleux déclenchant un petit programme d'accès furtif

. Accès réseau compromis découvert par un balayage réseau accompagné de test de mot de passe

Ces accès sont ensuite revendus sur des plateformes à d'autres cybercriminels. Les gains sont parfois partagés avec les exploiteurs

Les exploiteurs ou « moissonneurs »

Disposent d'un panel de compétences (intrusion, élévation de privilèges, latéralisation pivot, déploiement de rançongiciel, captation de mémoire vive, ...)

Achètent ou louent les logiciels et les accès aux fins de monétisation. Ils peuvent de plus disposer d'informations financières afin d'ajuster le prix de la rançon dans le cas de rançongiciels. Ils diffusent même parfois quelques fichiers volés afin de d'accentuer la pression sur le paiement de la rançon.

Toutefois, il est difficile de définir qui se cachent derrière le vol massif de données

Les intentions Criminelles

Le profit

Phishing, Ransomware (rançogiciels) Jackpotting, ...

L'atteinte à l'image

DDoS, Défacement

L' espionnage

Attaque par point d'eau / Spearphishing

Le sabotage

Panne organisée

POLICE NATIONALE

Quelques **chiffres**

71%

Des cyber-attaques
sont motivées financièrement

Source : Verizon

POLICE NATIONALE

Quelques **chiffres**

POLICE NATIONALE

85%

Des incidents de sécurité sont causés par une erreur humaine

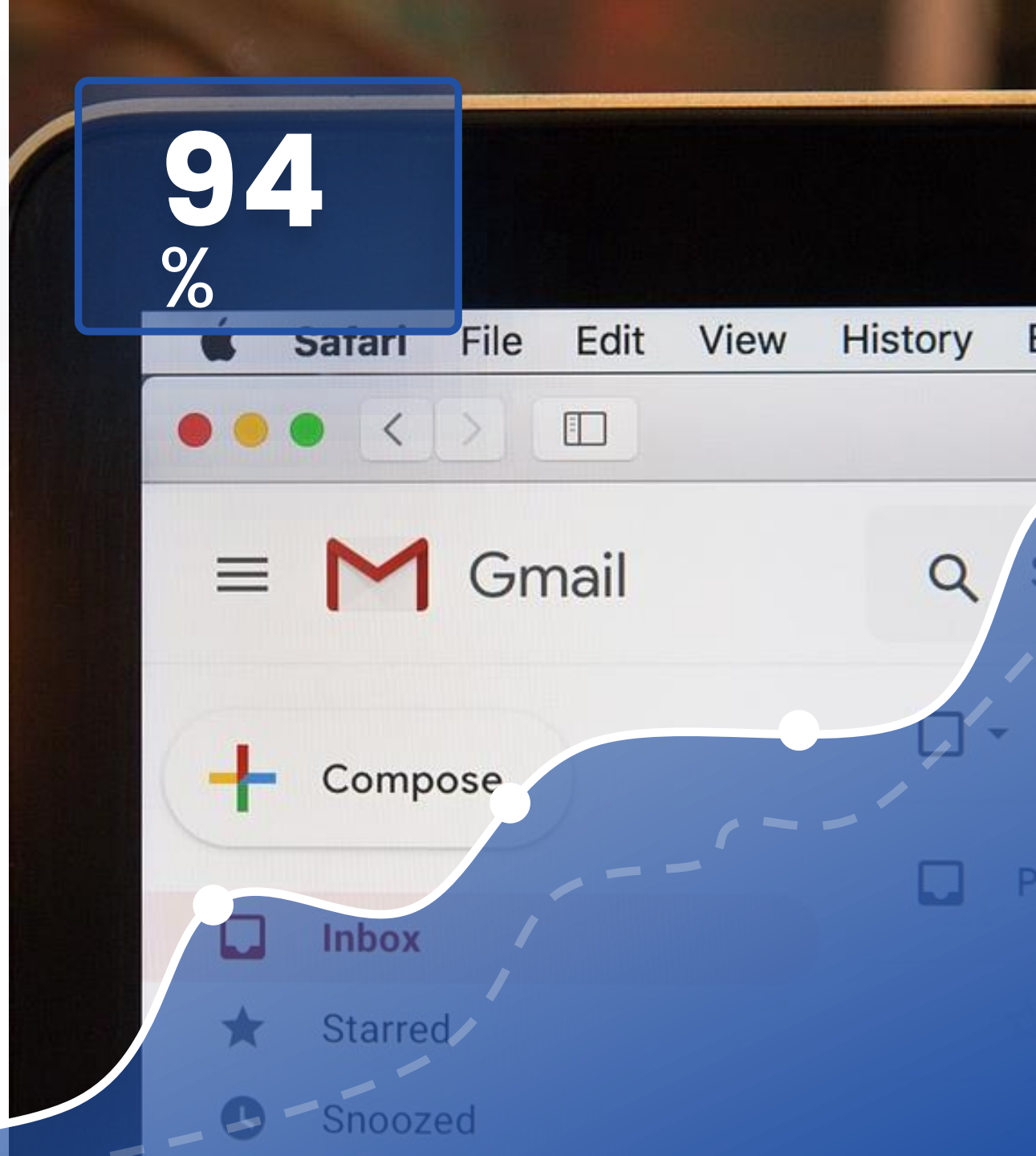
Source : Verizon

Quelques **chiffres**

94%

Des cyber-attaques
se déclenchent à partir d'un e-mail

Source : Verizon

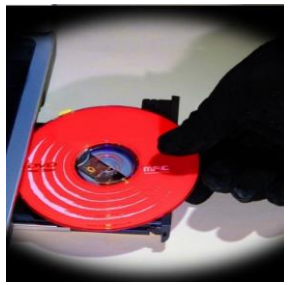


POLICE NATIONALE

Comprendre l’attaquant
Pour mieux s’en protéger

L'exploitation d'une **vulnérabilité humaine**
Ou « Ingénierie sociale »

POLICE NATIONALE



Manipulation psychologique

Exploite la

Vulnérabilité **humaine**

Dans un objectif

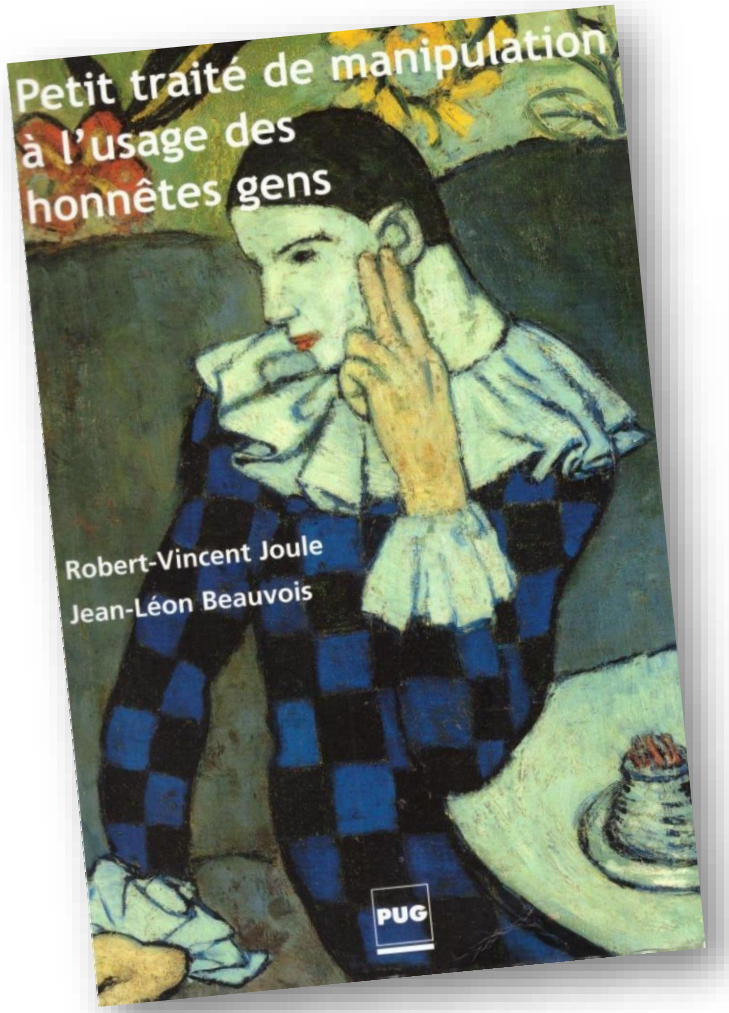
Escroquerie financière

Ou

Accès / Vol de **données**

L'ingénierie sociale :
les 2 principaux ingrédients

POLICE NATIONALE



Usurpation d'identité
Physique ou morale

Pression, émotion
sur la victime

L'ingénierie sociale : **Comment ça marche ?**

Le phishing

POLICE NATIONALE

Doctolib Pro

Sécurité de votre compte

Bonjour,

Votre compte Doctolib semble avoir été la cible d'une connexion suspicieuse.

Détails :

- Pays : Malaysia
- Date : 17 mars 2022 à 14h51
- Système : Windows 10.5.4

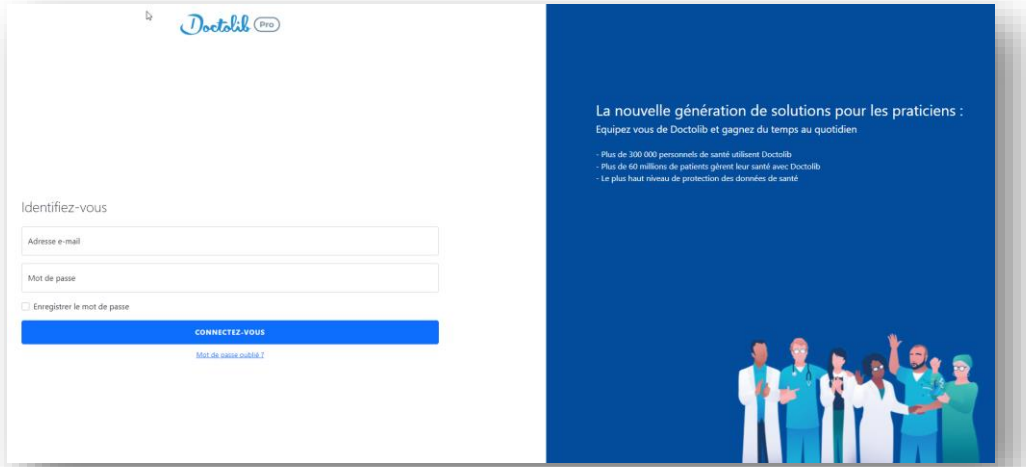
Pour des raisons de sécurité, votre compte est bloqué. Nous vous invitons à nous signaler si vous êtes à l'origine de cette action en cliquant sur l'un des bouton ci-dessous :

Il s'agit d'une connexion légitime

Je ne suis pas à l'origine de cette action

et e-mail vous a été envoyé pour vous informer de modifications importantes apportées à votre compte et aux services Google que vous utilisez.

© 2022 Doctolib



Usurpation **d'identité**

Homographe

http: // airfrance.com

POLICE NATIONALE

Usurpation **d'identité**

Phishing

POLICE NATIONALE

De [redacted] ☆

Sujet **Confirmation données personnelles !!!** 06:

Pou [redacted]

Cher client,

À la suite de notre dernière mise à jour du système, et pour des raisons de sécurité, nous vous informons qu'il est indispensable de confirmer vos données personnelles.

Pour votre sécurité, nous sommes amenés à revérifier les informations que vous nous avez transmises.

Aussi, nous vous remercions de nous adresser dans les plus brefs délais:

- une copie de votre pièce d'identité.
- votre dernier avis d'imposition sur revenu.

Nous vous remercions de nous transmettre ces éléments par mail sur : service@justificatif-ovh.com

A défaut de le recevoir dans un délai de 72 heures , c'est avec regret que nous procéderons à la fermeture de votre compte selon les dispositions prévues au titre de vos conditions générales.

Soyez assuré que toutes les informations que vous voudrez bien nous communiquer seront tenues pour strictement confidentielles

Usurpation **d'identité**

Phishing

POLICE NATIONALE

De Societe Generale <particuliers@societegnerale.fr>
Sujet **Confirmez votre Pass Sécurité**
Pour [redacted]

SOCIETE GENERALE

Cher(e) client(e),

Selon la nouvelle réglementation en vigueur relative à la sécurisation des données bancaire en France, nous somme dans le regret de vous annoncer, que si vous ne confirmez pas votre Pass Sécurité (1) auprès de nos services dans les plus bref délais, vous serez limité dans vos transactions.

Nous vous invitons à confirmer votre Pass Sécurité via notre service en ligne:

Confirmer mon Pass Sécurité

Nous nous excusons pour tout désagrément et vous remercions pour votre coopération.

Cordialement

Claude BAGNARD,
directeur de la relation Clients

Usurpation d'identité

POLICE NATIONALE

Hacking

Trend Micro fournit les détails suivants à *20 Minutes.* Entre la mi-mars et la mi-avril, des hackers russes **ont créé quatre noms de domaine ressemblant à ceux de l'équipe officielle d'En Marche** pour tenter de piéger des collaborateurs :

VIDEO. Présidentielle: Macron a bien été ciblé par les hackers russes de Fancy Bear

SECURITE La société de sécurité informatique Trend Micro confirme les soupçons de l'équipe de campagne d'En Marche! sur des attaques de hackers russes...

Philippe Berry | Publié le 25/04/17 à 00h08 — Mis à jour le 25/04/17 à 16h35

0 COMMENTAIRE 4,1k PARTAGES

À LIRE AUSSI

24/04/17 | PRESIDENTIELLE
Marine Le Pen se met «en congé de la présidence du FN»

31/12/16 | CYBER DÉFENSE
Comment Moscou a recruté une armée de hackers

30/12/16 | TECHNOLOGIE
Piratage russe: Le FBI accuse Moscou et le groupe de hackers Fancy Bear

D'ACTU 1 SUR 2

Le candidat à la présidentielle Emmanuel Macron sur sur iPhone, le 10 mars 2017, en gare de Bordeaux. — UGO AMEZ/SIPA

- onedrive-en-marche.fr (15 mars 2017)
- portal-office.fr (14 avril 2017)
- mail-en-marche.fr (12 avril 2017)
- accounts-office.fr (17 avril 2017)

Selon les chercheurs, « ces noms de domaine ont vraisemblablement été utilisés par Pawn Storm pour cibler la campagne de Macron », qui utilise le service email de Microsoft d'Office 365. La procédure est classique et vise en général **à se faire passer pour un courriel officiel afin de convaincre une personne** d'entrer son mot de passe lors d'une remise à zéro. Selon Trend Micro, les hackers ont également tenté d'infecter des ordinateurs avec un malware Javascript à la recherche d'éventuelles failles.

Escroquerie
Exemple d'atteinte

Faux recrutement

Scénario
D'attaque

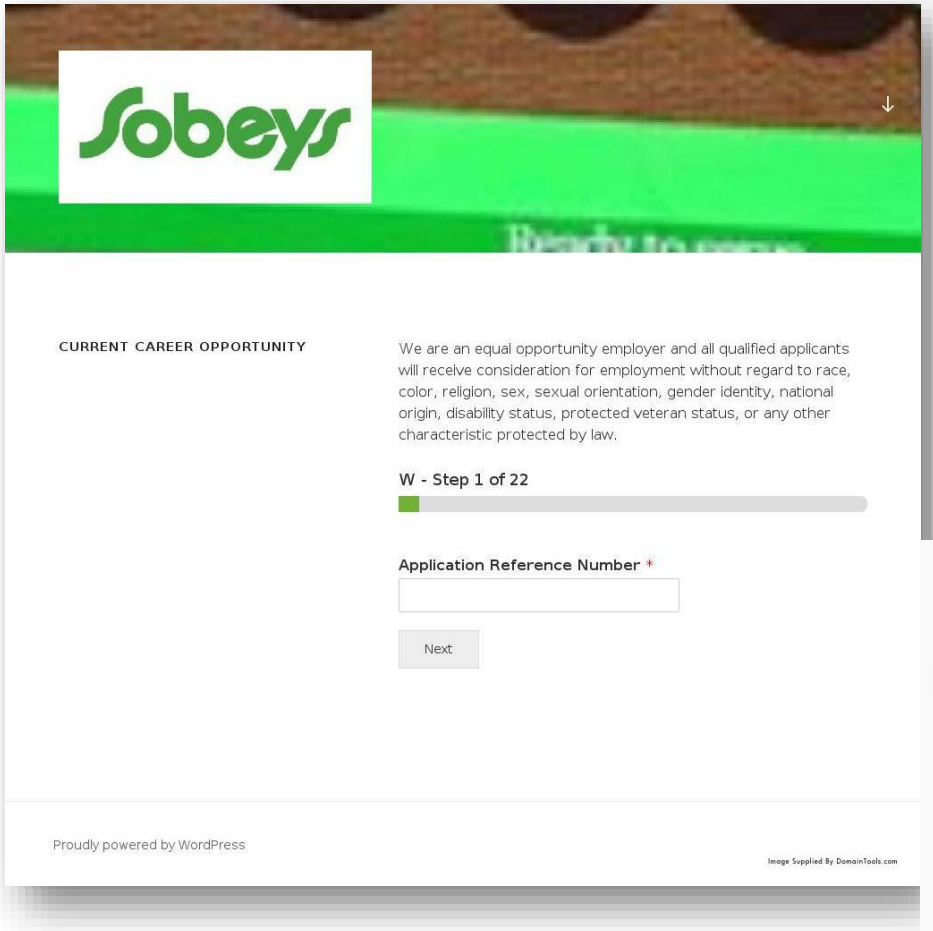
WIPO Arbitration and Mediation Center

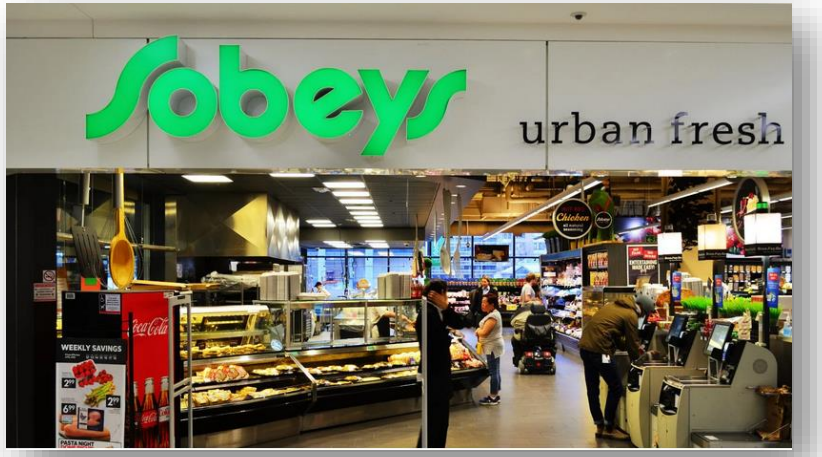
Sobeys Capital Incorporated v. Private By Design, LLC / Max Bill and Billi Max

Case No. D2020-1670

http://interview-Sobeys.com

POLICE NATIONALE





The Respondent registered the First Disputed Domain Name on May 29, 2020 and the Second Disputed Domain Name on May 6, 2020. The First Disputed Domain Name is used to direct users to a fake SOBEYS website, which prominently features the Complainant's Trademark, trade name, and other details about the Complainant, all without any authorization. This fake website is used to solicit "job applications" from prospective employees requiring the provision of confidential personal information.

Email addresses associated with the Disputed Domain Names have also been used to send third parties solicitation emails purporting to emanate from the Complainant and offering employment with the Complainant's business. These fraudulent emails represent that they are being sent by human resources personnel employed by the Complainant, and solicit confidential personal and financial information from the victims of the scam. Among other things, recipients are requested to sign an "Employment Contract" and to also provide confidential personal and financial information including copies of government documents, banking information, and postal addresses in order to "accept" the employment position offered by the Respondent posing as "Sobeys" after first submitting a "job application" through the fake website hosted at the First Disputed Domain Name. As with the fake website operated by the Respondent, the "Employment Contract" and other materials sent to recipients of these emails prominently feature the Complainant's Trademark and include references to the Complainant's actual activities.

Escroquerie
Exemple d'atteinte

Visant Pole Emploi

Scénario
D'attaque

https://pole-emploi.fr

http://poleemploifrance.fr

http://polle-emploi.fr

N° de dossier	Nom de domaine	Date de publication	Procédure
FR-2022-03066	poleemploifrance.fr	01/02/23 16:42:54	SYRELI
FR-2022-02885	polle-emploi.fr	29/08/22 09:46:13	SYRELI

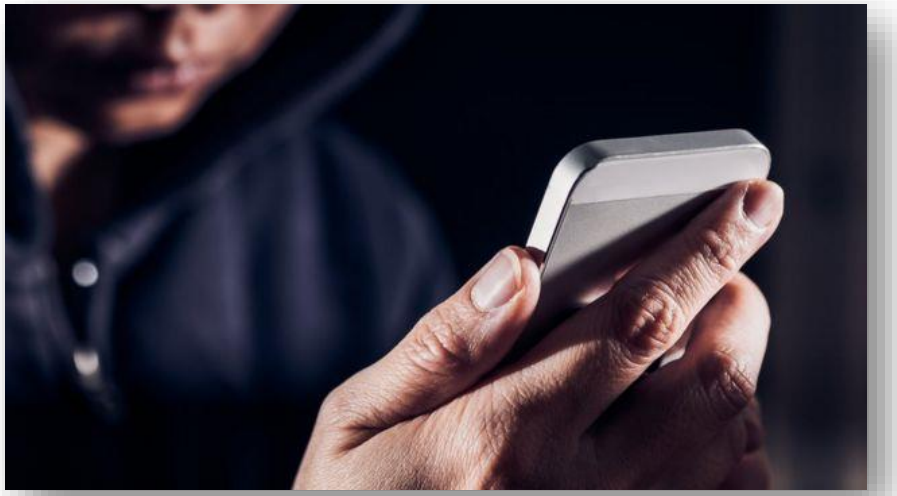
https://pajemploi.urssaf.fr

http://pajemploiurssaf.fr

N° de dossier	Nom de domaine	Date de publication	Procédure
FR-2022-02706	pajemploiurssaf.fr	19/04/22 12:18:25	SYRELI
FR-2021-02476	pajemploie.fr	11/10/21 09:44:01	SYRELI
FR-2021-02467	pajemploi.fr	11/10/21 09:44:24	SYRELI

L'ingénierie sociale : **Comment ça marche ?**

L'appel téléphonique



JUSTICE

"Arnaque au faux Le Drian" : l'avocate du ministre détaille le fonctionnement d'une escroquerie hors pair

Par Corinne Audouin

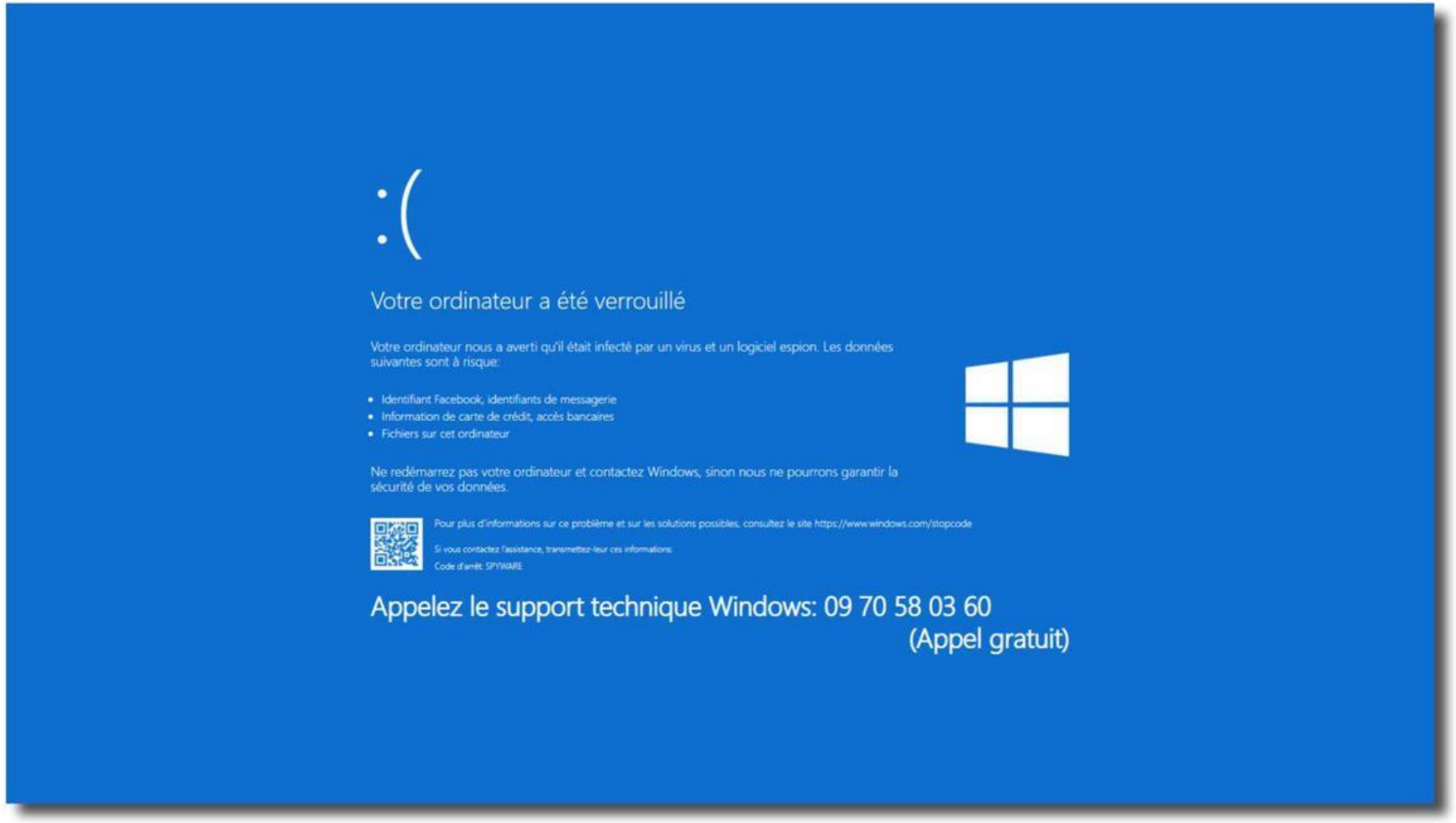
Publié le mardi 4 février 2020 à 06h05 | 3 min | PARTAGER

Voici le faux Le Drian que les victimes de l'arnaque ont vu lors d'une conversation via Skype

C'est le procès d'une incroyable escroquerie qui s'ouvre ce mardi 4 février devant le tribunal correctionnel de Paris : "l'arnaque au faux Le Drian", du nom de l'actuel ministre des Affaires étrangères. Sept prévenus sont jugés pour avoir escroqué plusieurs dizaines de millions d'euros entre 2015 et 2016. Entretien.

L'ingénierie sociale : **Comment ça marche ?**

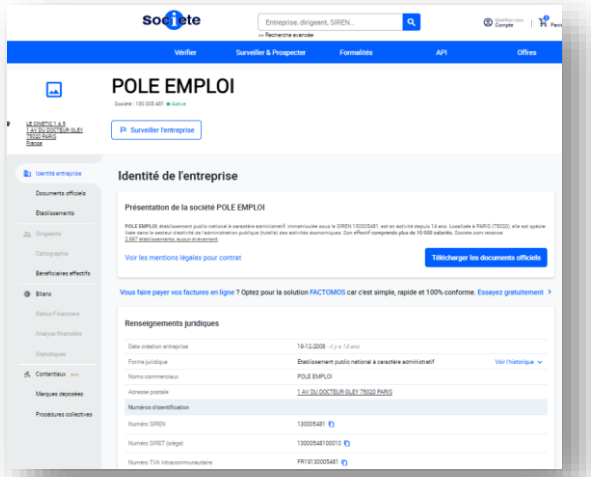
Le faux support technique



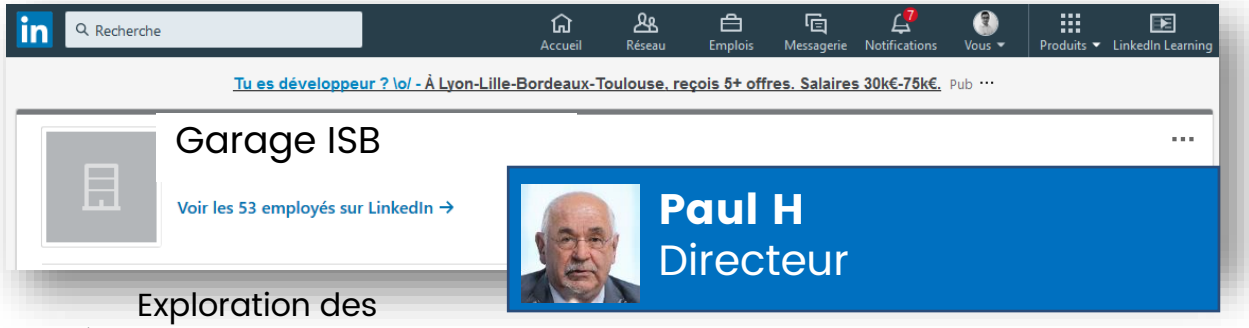
L'ingénierie sociale : **simple et efficace !**

Scénario D'attaque

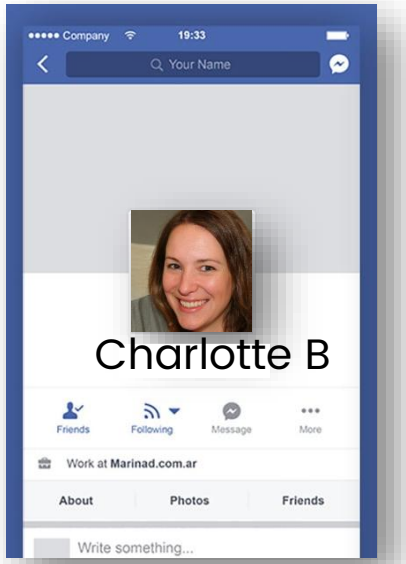
Les bases de **l'OSINT** (Open Source Intelligence) ou **ROSO** (renseignement d'origine sources ouvertes)



Exploration des **données publiques**



Exploration des **réseaux professionnels**

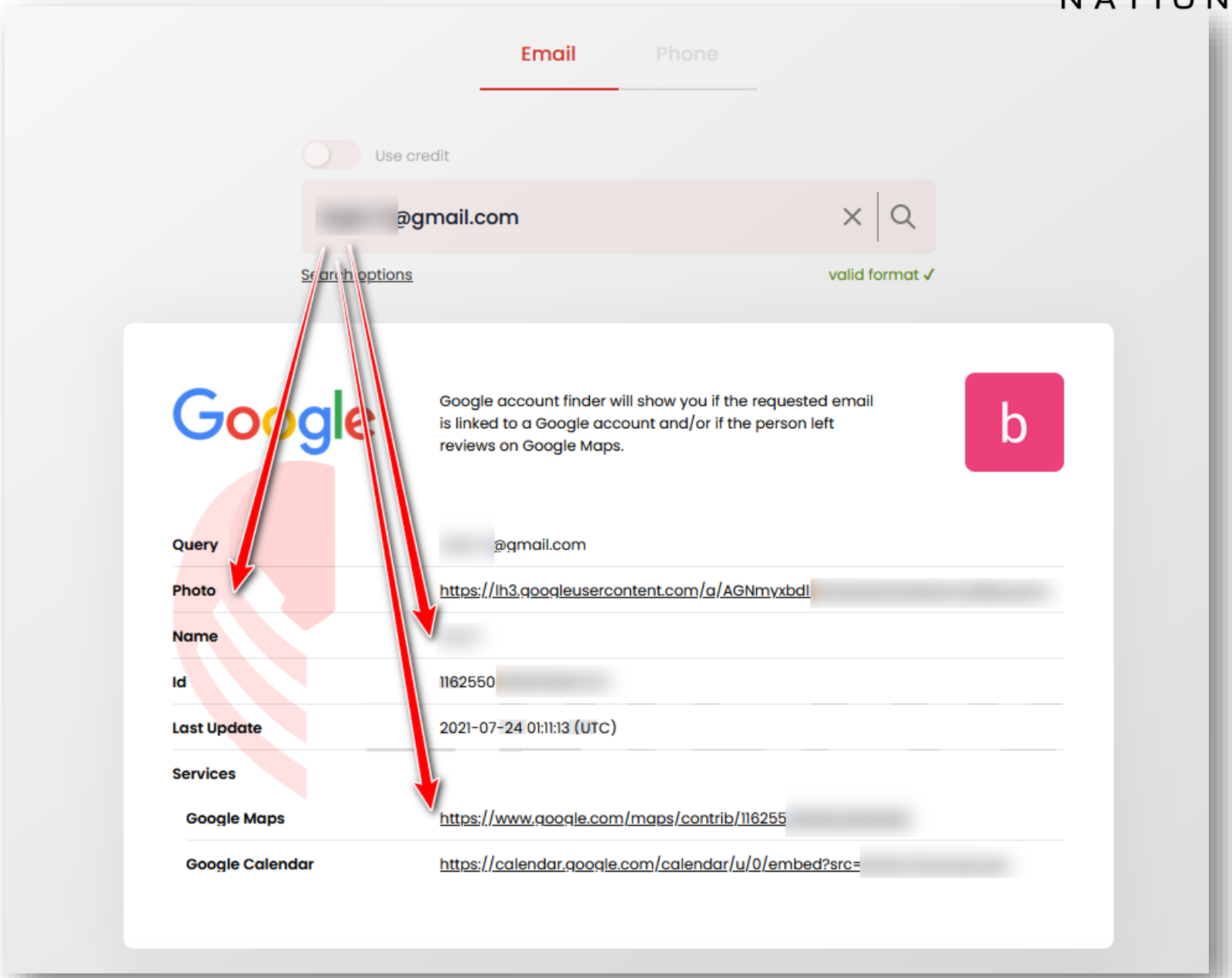


Exploration des **réseaux personnels**

L'ingénierie sociale : **simple et efficace !**

Scénario
D'attaque

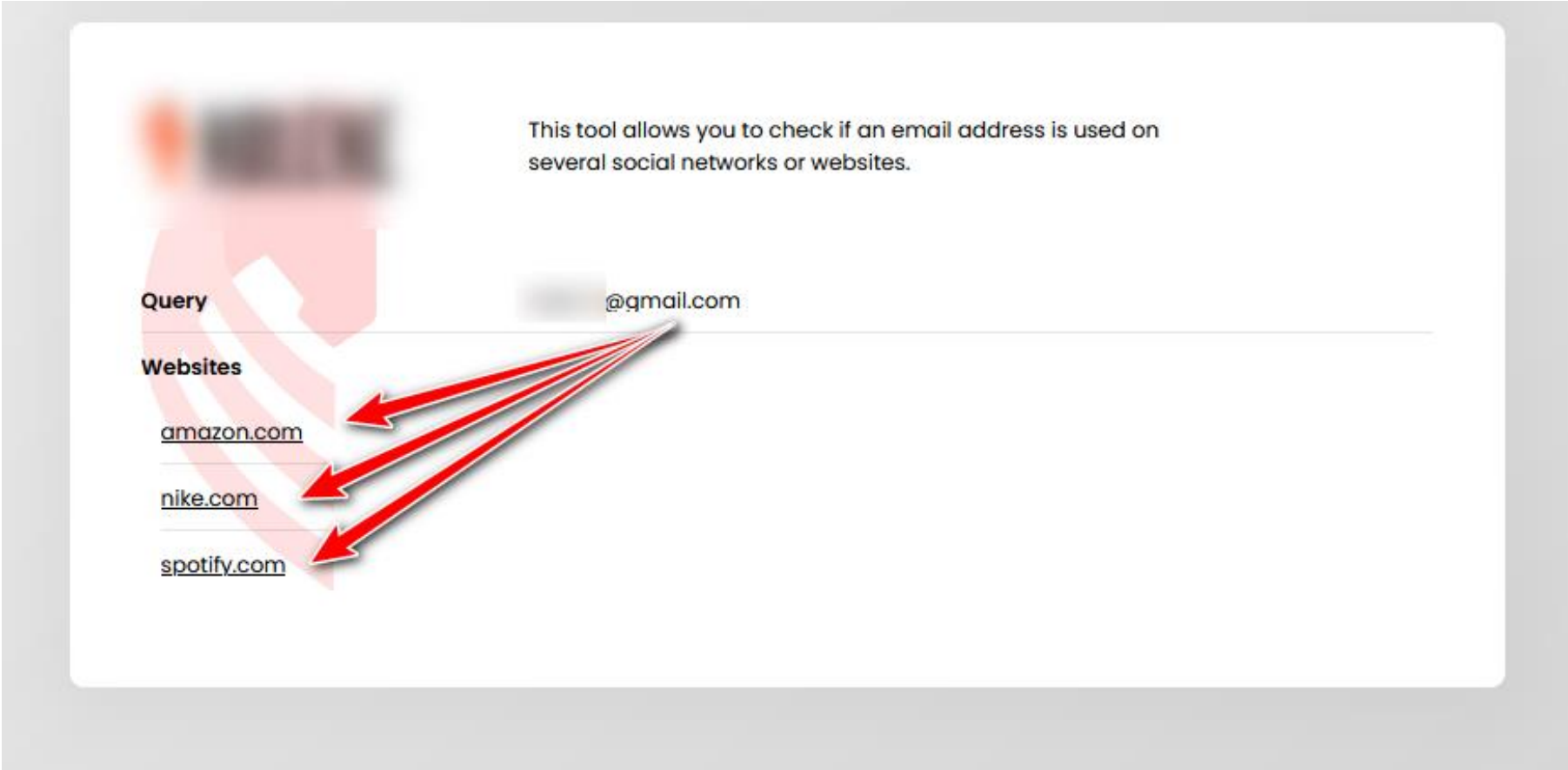
Exemple **d'OSINT** depuis
Une **adresse email**
-
Identification des **publications liées à son compte google** : avis, photos, calendrier



L'ingénierie sociale : **simple et efficace !**

Scénario
D'attaque

Exemple d'OSINT depuis
Une adresse email
-
Identification **des sites liées à l'adresse email** :
Possibilité de phishing personnalisé



L'exploitation d'une **vulnérabilité technique**

Les 3 principaux facteurs techniques d'attaques informatiques

L'absence des mises à jour
(Fonctionnelles et de sécurité)

L'absence de politique de mot de passe
(complexité, contrôle, renouvellement…)

La publication des outils sur internet et l'absence de contrôle des utilisateurs et des prestataires

Les **3 principaux facteurs** techniques d'attaques informatiques

2 exemples **de scénarios réels**

Scénario D'attaque

POLICE NATIONALE

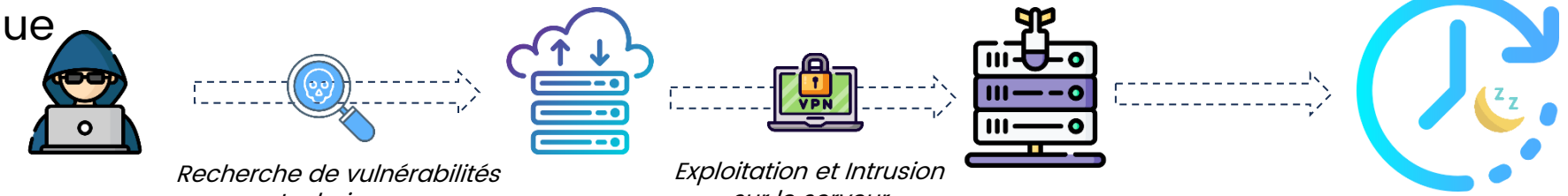
Ingénierie sociale

Envoi d'un mail piégé

Transmission d'informations sensibles (identifiant, mot de passe…)

Intrusion sur le serveur

Vulnérabilité technique



Recherche de vulnérabilités techniques

Exploitation et Intrusion sur le serveur

Les objectifs visés

Accéder et manipuler les données

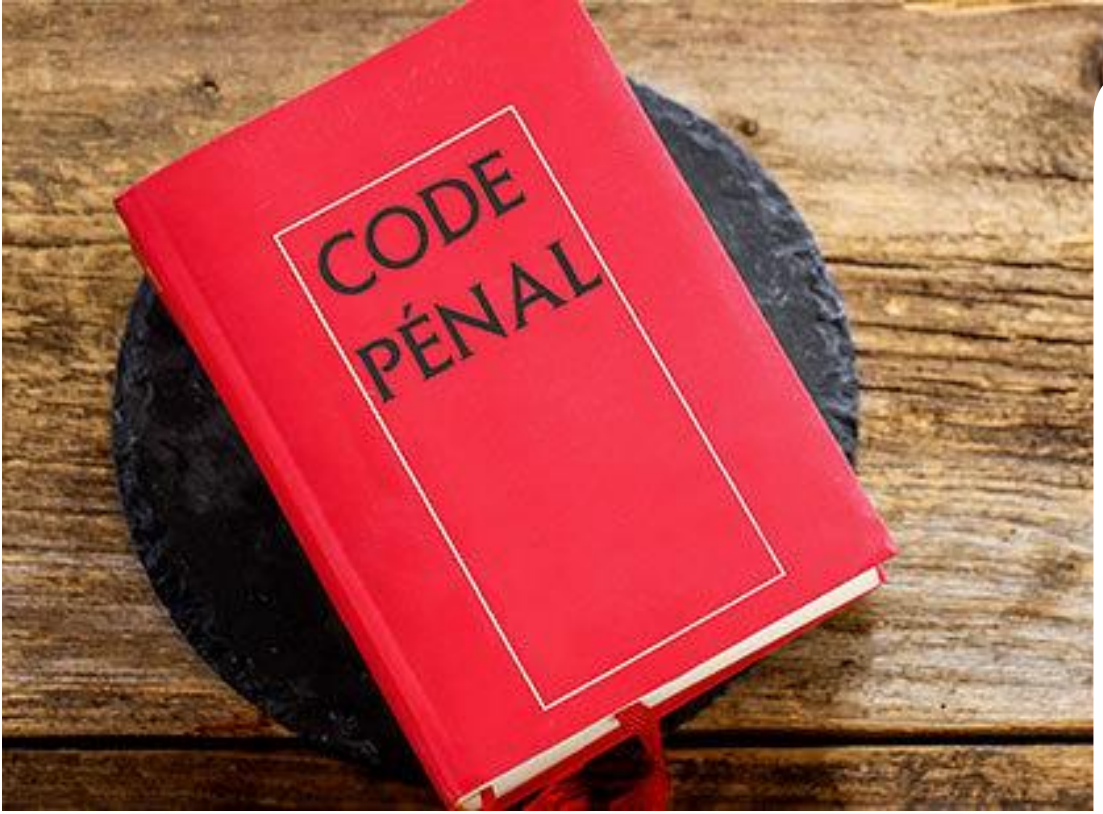
Télécharger les données

Chiffrer les données

Supprimer les données

POLICE NATIONALE

Les **escroqueries**



Article 313-1

L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- Escroqueries aux **faux virements étrangers**
- Escroqueries aux **faux investissements** sur le foreign exchange (FOREX)
- Escroqueries aux placements indexés sur les **cryptomonnaies**
- Escroqueries aux **faux supports techniques**
- Escroqueries à la **fausse amitié** (Scam romance)
- Escroquerie au **RGPD**
- Escroquerie au **faux RIB d'employé**
- Escroquerie au **CV**

Matrice d'influence en **escroquerie** et ingénierie sociale sur **les réseaux sociaux**

POLICE NATIONALE

Matrice **MICE**

Les piliers de la manipulation

\+

Money
Argent

Ideology (idéologie)
(convictions religieuses, politiques, etc.) ou intérêt (passe-droits)

Coercition
chantage, menaces, kompromat, torture, etc.

Ego
vanité, désir de se mettre en avant

Escroquerie
Les impacts

Scénario
D'attaque

POLICE NATIONALE

Arrêt des activités

Perte financière / Liquidation

Difficultés juridiques

Pression psychologique

Image de marque / Notoriété

Confidentialité / Secret

Comment se protéger ?

pour éviter **l'incident** ?

Comment se **protéger** ?

1) Protégez vous !

La **suite** de sécurité

Elle permet une protection contre :

- Les logiciels **malveillants**
- Les **comportements** suspicieux
- Les **pièce-jointes** malicieuses
- Les fichiers dangereux
- Les **sites** internet

Les conditions pour assurer votre sécurité :

- Installation sur **tous les appareils**
- L'outil doit être activé en **permanence**
- La base de données virale doit **être à jour**

Comment se **protéger** ?

2) Soyez vigilants aux mails !

POLICE NATIONALE

Règle n°1 : Contrôler TOUJOURS votre source

Ne vous fiez pas au lien présent sur l'e-mail mais à celui qui s'affiche dans votre navigateur : est-il vraiment celui de votre fournisseur ?

Règle n°2 : Vérifiez TOUJOURS si la communication est chiffrée

Le cadenas et la mention https sont indispensables pour garantir le chiffrement de la connexion avec le serveur web du destinataire.

Règle n°3 : Ayez TOUJOURS un doute !

Vous êtes surpris par le contenu d'un mail ?
On vous demande vos coordonnées bancaires ?
Vous n'avez jamais commandé sur le site en question ?

Le Phishing **comment s'en protéger ?**

STOP ! Il s'agit probablement d'une arnaque.
Contactez votre responsable informatique ou le fournisseur concerné !

Escroquerie –

Vérifier un
Nom de domaine

http://who.is
https://gwhois.org

WHOIS
DOMAIN
LOOKUP

Recherche d'information sur **un nom de domaine**

POLICE NATIONALE

https://pole-emploi.fr

```
domain:          pole-emploi.fr
status:          ACTIVE
Expiry Date:     2023-09-21T09:42:27Z
created:         2008-10-10T14:47:02Z
```

```
nic-hdl:         PEAD28-FRNIC
type:            ORGANIZATION
contact:         POLE-EMPLOI admin-domaines-internet
address:         POLE EMPLOI
address:         70 rue de Lagny
address:         93558 MONTREUIL
country:         FR
phone:           +33.155817000
fax-no:          +33.155817984
e-mail:          admin-domaines-internet@pole-emploi.fr
```

http://poleemploifrance.fr

```
domain:          poleemploifrance.fr
status:          FROZEN
Expiry Date:     2023-10-13T11:09:31.993649Z
created:         2022-10-13T11:09:32.017576Z
```

```
nic-hdl:         ANO00-FRNIC
type:            PERSON
contact:         Ano Nymous
registrar:       OVH
changed:         2020-03-27T09:04:06Z
anonymous:       YES
remarks:         ------------- WARNING -------------
remarks:         While the registrar knows him/her,
remarks:         this person chose to restrict access
remarks:         to his/her personal data. So PLEASE,
remarks:         don't send emails to Ano Nymous. This
remarks:         address is bogus and there is no hope
remarks:         of a reply.
remarks:         ------------- WARNING -------------
```

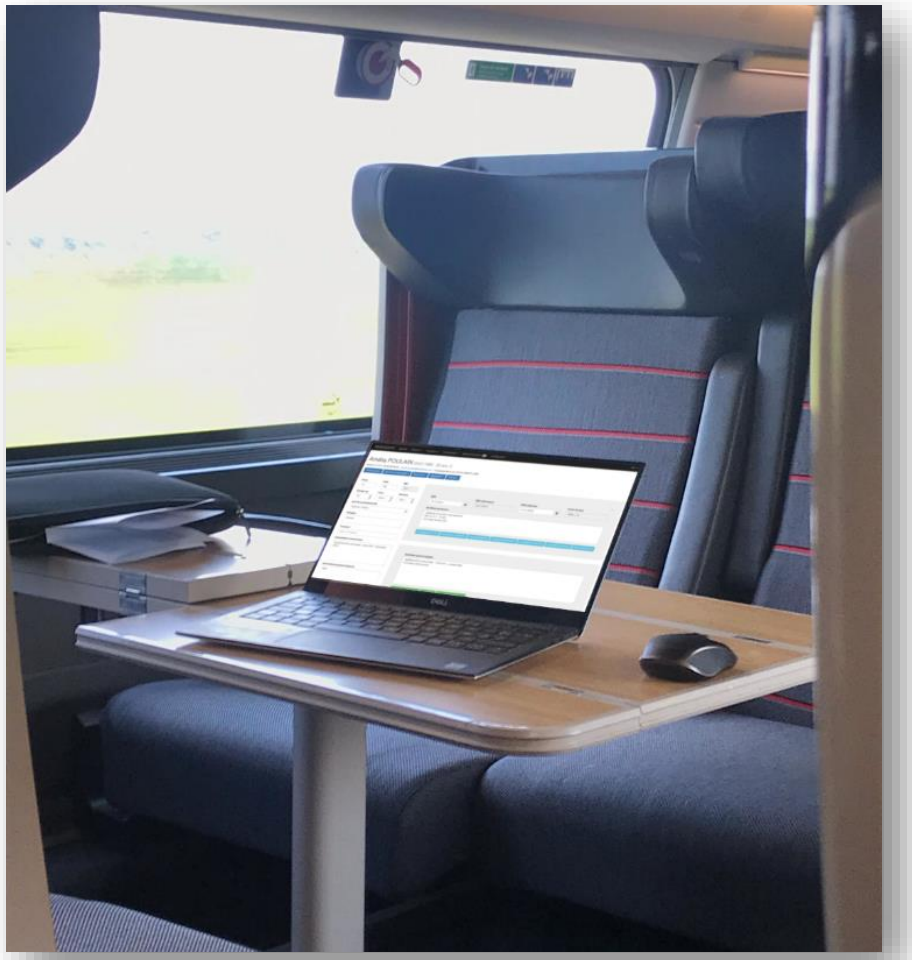
Comment se **protéger** ?

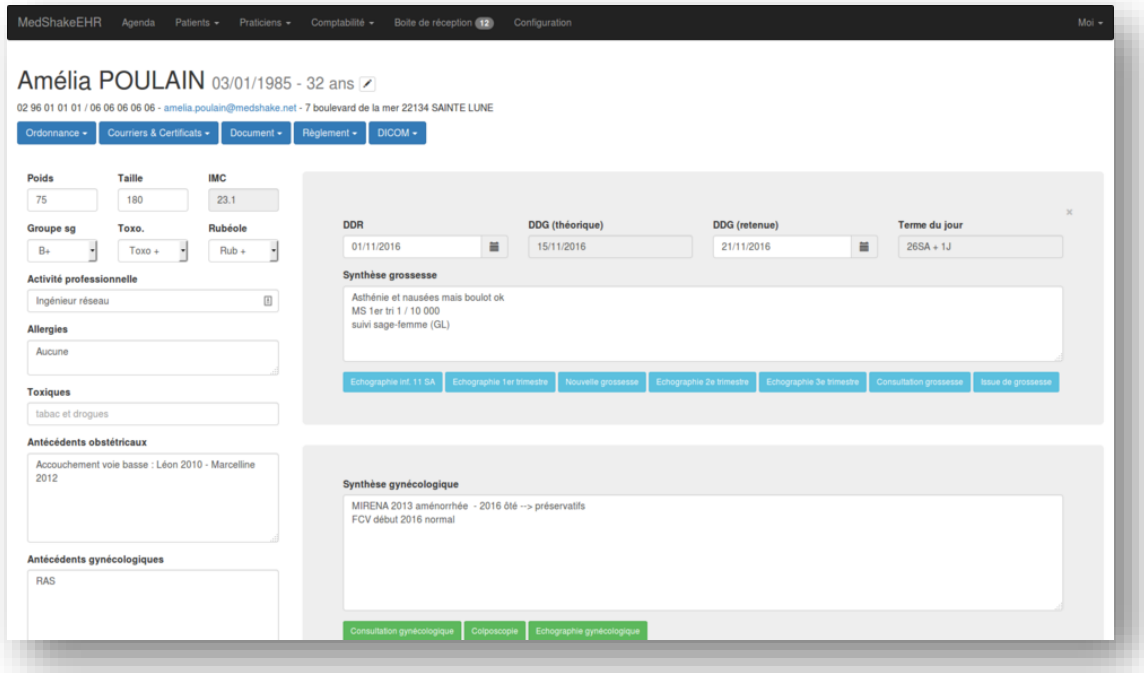
3) Sécurisez vos accès !

Le mot de passe : **votre clé privée !**

- Quelque soit le service que vous utilisez, **votre mot de passe est personnel !**
- **Ne transmettez jamais** votre mot de passe
- **Choisissez un mot de passe « complexe ».** C'est-à-dire « difficile à deviner » pour l'attaquant
- **N'utilisez pas le même** mot de passe pour deux services différents
- **N'enregistrez pas** vos mots de passe sur vos cahiers ou sur votre ordinateur

Comment se **protéger** ?
4) Surveillez votre matériel





POLICE NATIONALE

Comment se **protéger** ?
5) Sauvegardez vos données !

Vous hébergez votre logiciel métier chez un prestataire ?
Attention à votre contrat !

Vous hébergez vous-même vos données ?
Réfléchissez à la stratégie en fonction de la sensibilité !

Exemple de stratégie en 3 -2 - 1

- 3 **copies** des données
- 2 **supports** de sauvegardes
- 1 copie « **hors site** »

POLICE NATIONALE

Comment se **protéger** ?

6) Effectuez vos mises à jour !

La mise à jour corrige des **vulnérabilités** !

L'application des mises à jour est un **élément essentiel** pour assurer la sécurité de votre matériel.

Vous disposez d'un informaticien ?
Posez lui la question.

Comment se **protéger** ?
7) Sensibilisez au maximum

POLICE NATIONALE

Vos collaborateurs

- Intégration
- Contrat de travail
- Charte informatique
- Sensibilisation ponctuelle
- Surveillance…

Vos prestataires

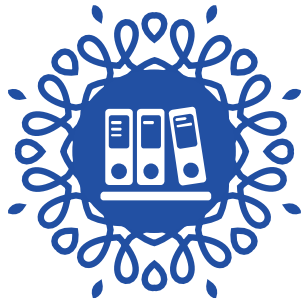
- Contrat de prestation
- Charte prestataire
- Accompagnement
- Surveillance…

Votre entourage

- Séparation des usages
- Confidentialité pro / perso
- Sensibilisation en famille
- …

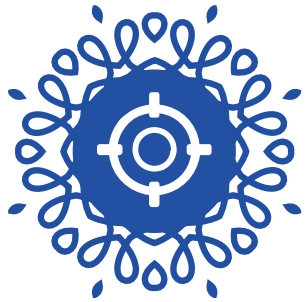
Comment **réagir**
En cas d'incident ?

Réactions face **à une cyber attaque**



Isoler

Ne pas éteindre les postes infectés mais **couper tous les accès réseaux**



Confiner

Mettre en **quarantaine** les postes infectés et les supports amovibles

Conserver

Les **journaux d'activité**, docs, **emails**, fichiers, trafic réseau + copie des supports / acquisition mémoire vive

Communiquer

Auprès des **collaborateurs**, des **fournisseurs**… pour éviter le surincident

Le dépôt **de plainte**

Pourquoi déposer plainte ?

Parce que vous êtes victime !

- Pour **comprendre les raisons** et/ou contexte de l'attaque
- Pour **identifier les modes opératoires** et les vulnérabilités
- Pour **récupérer les données métiers** et limiter leur diffusion
- Pour permettre (dans certains cas) le **blocage des fonds**
- Pour **se protéger** (ex. : usurpation d'identité)
- Pour **faire valoir ses droits** (auprès des banques, de l'assurance…)
- Pour **contribuer aux enquêtes** de Police

POLICE NATIONALE

Gendarmerie nationale

Le dépôt **de plainte**

Quand et comment déposer plainte ?

cybermenaces-bordeaux@interieur.gouv.fr

https://www.pre-plainte-en-ligne.gouv.fr

- La création **d'un point de contact unique et privilégié sur la Nouvelle-Aquitaine** avec une adresse mail dédiée en cas de doute ou d'attaque avérée : cybermenaces-bordeaux@interieur.gouv.fr
- Possibilité d'effectuer une **pré-plainte en ligne** : https://www.pre-plainte-en-ligne.gouv.fr
- Prise de plainte **sur rendez-vous**, avec les documents nécessaires, en présence (si possible) du responsable informatique

POLICE NATIONALE

Gendarmerie nationale

Ressources

https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

https://secnumacademie.gouv.fr/

CNIL.

https://www.cnil.fr/fr/cybersecurite

CYBER MALVEILLANCE .GOUV.FR

https://www.cybermalveillance.gouv.fr/cybermenaces

Merci pour votre attention

Vos questions ?

Pierre LABORDE
Commandant Divisionnaire
Réserviste Police Nationale
cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

RCM
POLICE NATIONALE
DCPJ • RÉFÉRENT CYBER MENACE

Gaël MANCEC
Juriste NTIC
Réserviste Police Nationale
cybermenaces-bordeaux@interieur.gouv.fr