SENSIBILISATION AUX RISQUES CYBER

Mise à jour : 24 Janvier 2023

Présentation des animateurs

Pierre LABORDE
Commandant Divisionnaire
Réserviste Police
Nationale

Charlotte VIALAT
Référente cybersécurité
Réserviste Police Nationale

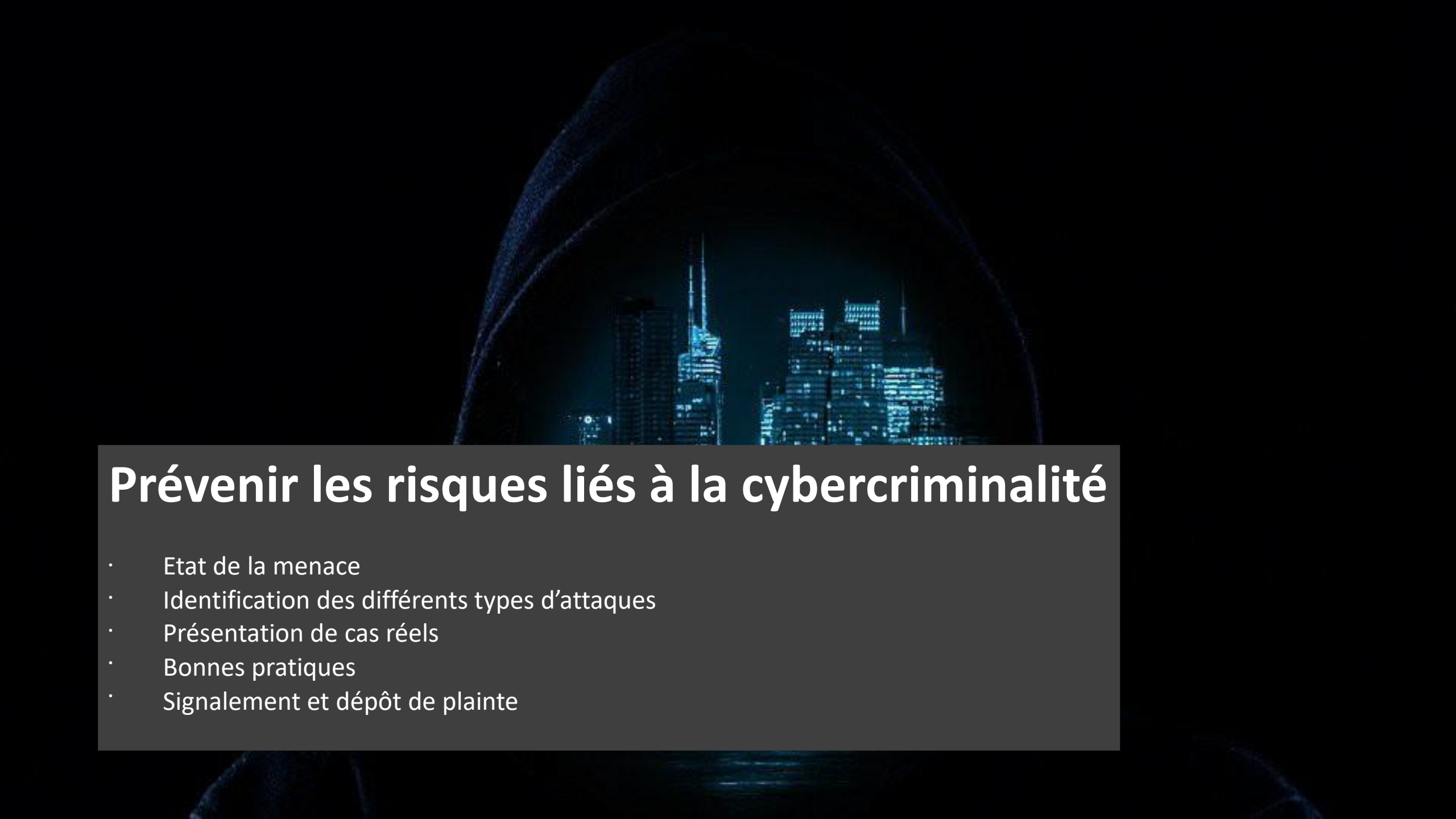
Direction Zonale de la Police Judiciaire de Bordeaux DZPJ Sud-Ouest
Hôtel de Police
23 rue François de Sourdis 33062 BORDEAUX

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

cybermenaces-bordeaux@interieur.gouv.fr

Réseau des référents Cybermenaces - RCM

- 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 :33 réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux
- Point de contact pour les entreprises en Nouvelle-Aquitaine :



Prévenir les risques liés à la cybercriminalité

- Etat de la menace
- Identification des différents types d’attaques
- Présentation de cas réels
- Bonnes pratiques
- Signalement et dépôt de plainte

Évolution de la criminalité organisée depuis 20 ans

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

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

Il s’agit de cybercriminalité et de vrais criminels !

Les cybercriminels travaillent par spécialités

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 (rançongiciels), Jackpotting…

L'atteinte à l'image :

DDos, Défacement

L'espionnage :

Attaque par point d'eau / Spearphishing

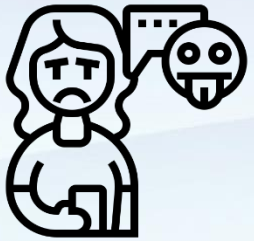
Le sabotage :

Panne organisée

Quelques chiffres

71 % Des cyber attaques sont motivées financièrement

85 % Des incidents de cybersécurité sont causés par une erreur humaine



94 % Des cyber attaques se déclenchent à partir d'un email

Source : Verizon

Comprendre l’attaquant

Pour mieux s’en protéger

L'exploitation d'une vulnérabilité humaine

Ou « Ingénierie sociale »

Manipulation psychologique

Exploite la

Vulnérabilité **humaine**

Dans un objectif

Escroquerie financière

Ou

Accès / Vol de **données**

L’ingénierie sociale : Comment ça marche ?

Le Phishing

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

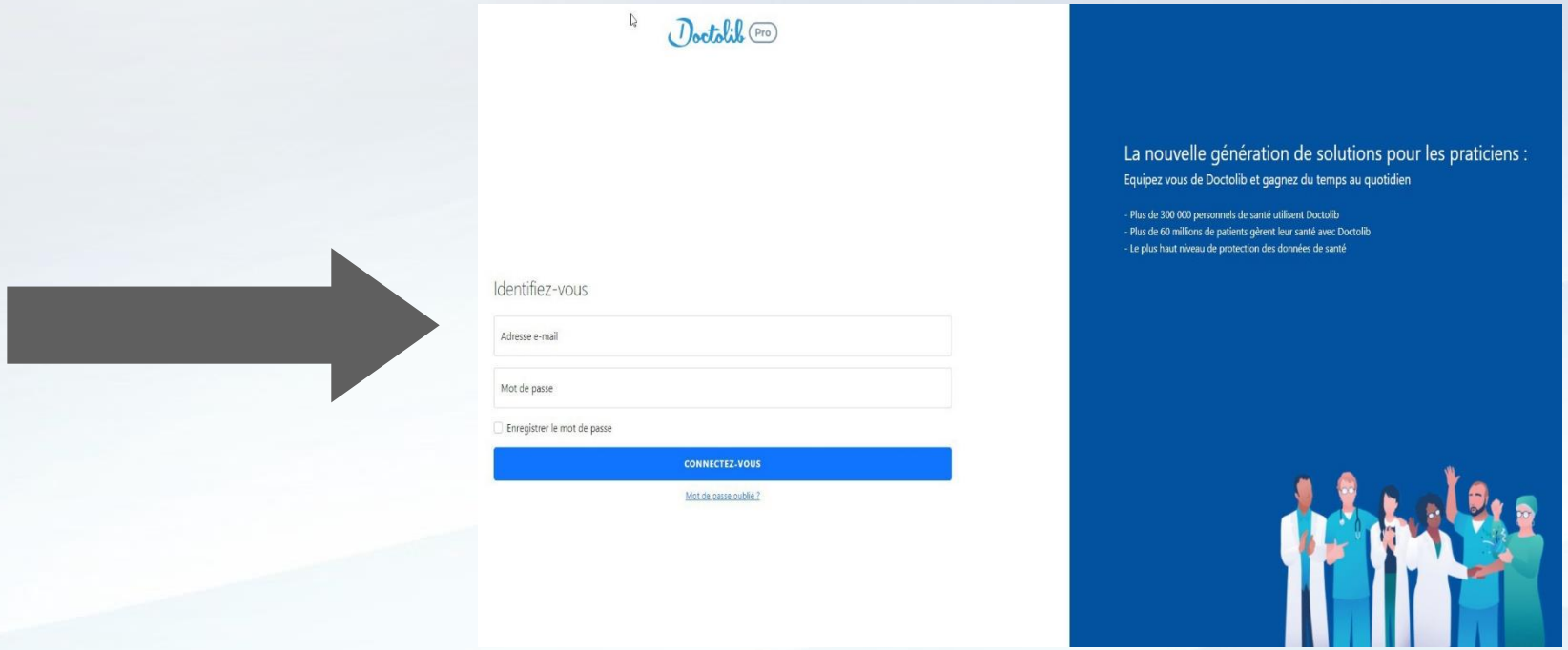
Pour des raisons de sécurité, votre compte est bloqué. Nous vous invitons à nous signaler si vous êtes à l'origine de cette action en cliquant sur l'un des bouton ci-dessous :

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



POLICE NATIONALE

Comment détecter un mail suspect ?

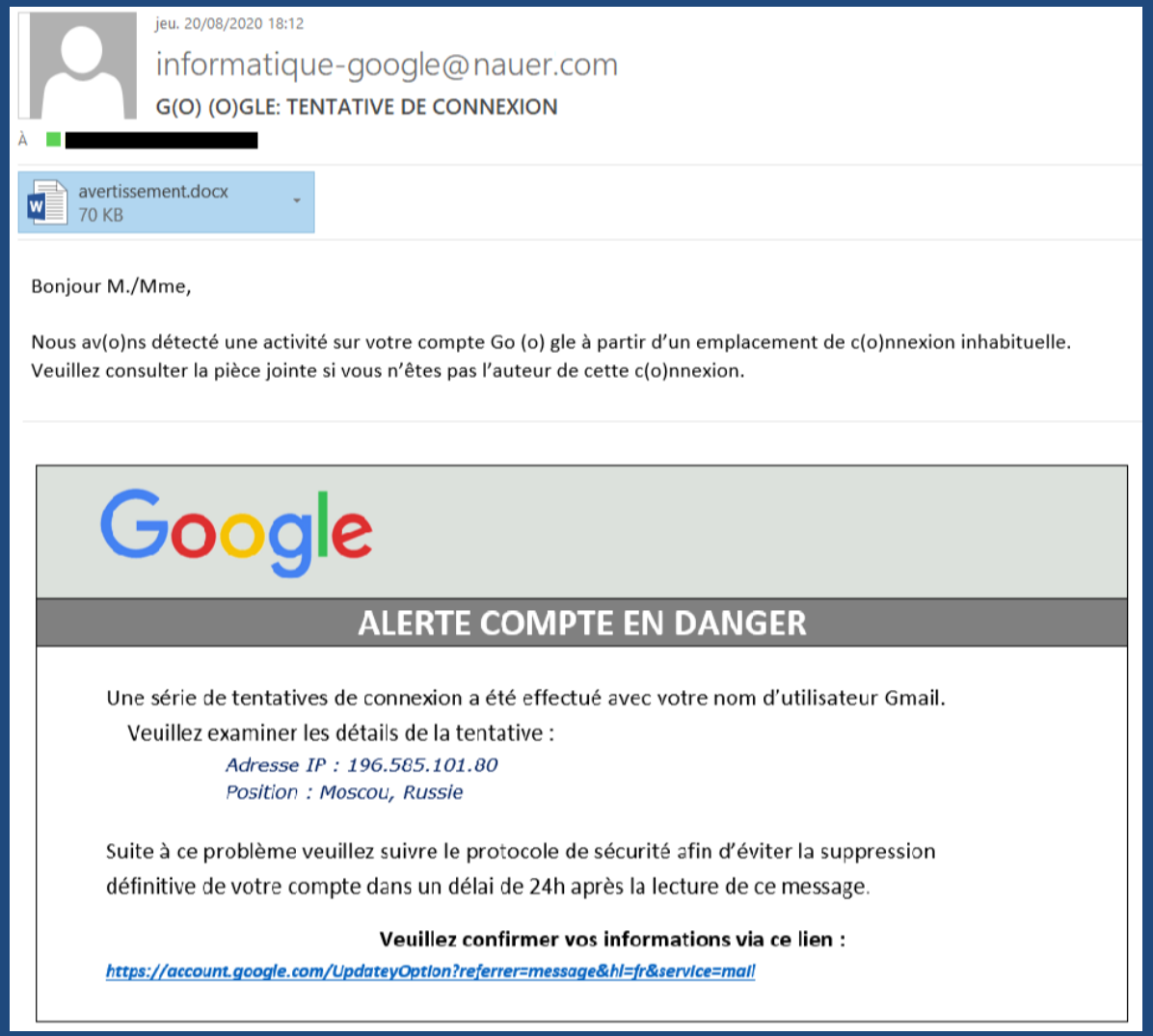
1. Est-ce logique que je reçoive ce mail ?
Est-ce que je connais l'expéditeur ? Suis-je le bon interlocuteur sur ce dossier ?

2. Ce mail est il cohérent ?
Contient-il des erreurs, des fautes d'orthographe ?

3. Les liens sont ils conformes ?
Passer la souris sur le lien, vérifier l'adresse mail et la signature

4. Données sensibles demandées et/ou urgence : arnaque
Contacter l'expéditeur par téléphone, vérifier auprès de sa hiérarchie

5. Attention aux pièces jointes
Archives Zip/Rar, demande d'exécution de macros



jeu. 20/08/2020 18:12

informatique-google@nauer.com

G(O) (O)GLE: TENTATIVE DE CONNEXION

À [redacted]

avertissement.docx
70 KB

Bonjour M./Mme,

Nous av(o)ns détecté une activité sur votre compte Go (o) gle à partir d'un emplacement de c(o)nnexion inhabituelle.
Veuillez consulter la pièce jointe si vous n'êtes pas l'auteur de cette c(o)nnexion.

Google

ALERTE COMPTE EN DANGER

Une série de tentatives de connexion a été effectué avec votre nom d'utilisateur Gmail.
Veuillez examiner les détails de la tentative :

Adresse IP : 196.585.101.80
Position : Moscou, Russie

Suite à ce problème veuillez suivre le protocole de sécurité afin d'éviter la suppression définitive de votre compte dans un délai de 24h après la lecture de ce message.

Veuillez confirmer vos informations via ce lien :

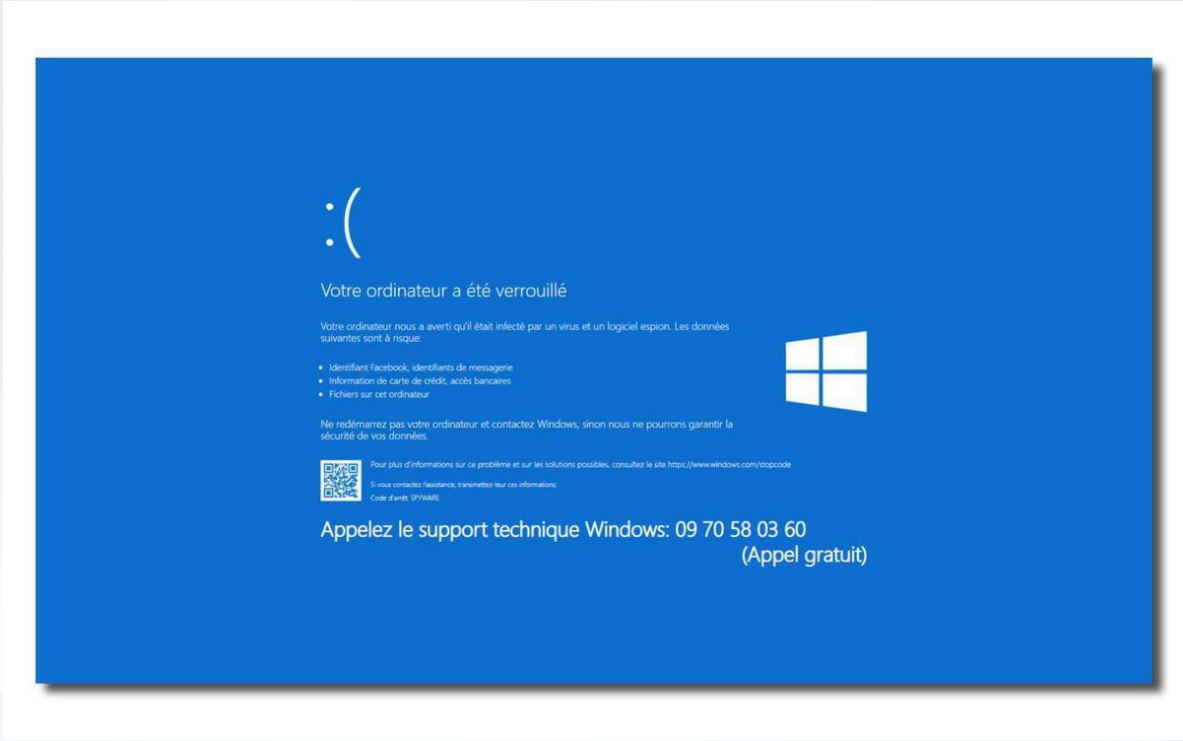
https://account.google.com/UpdateyOption?referrer=message&hl=fr&service=mail

L’ingénierie sociale : Comment ça marche ?

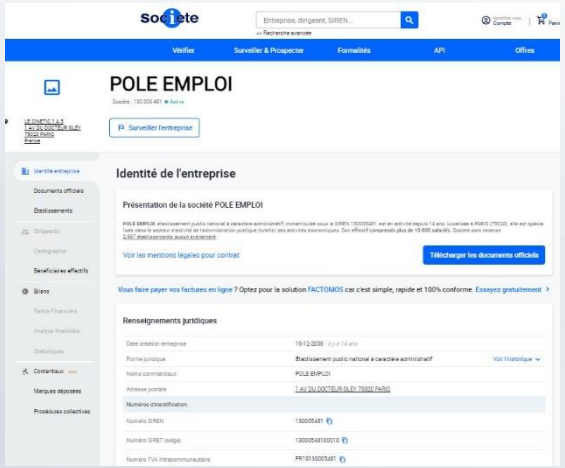
L’appel téléphonique

L’ingénierie sociale : Comment ça marche ?

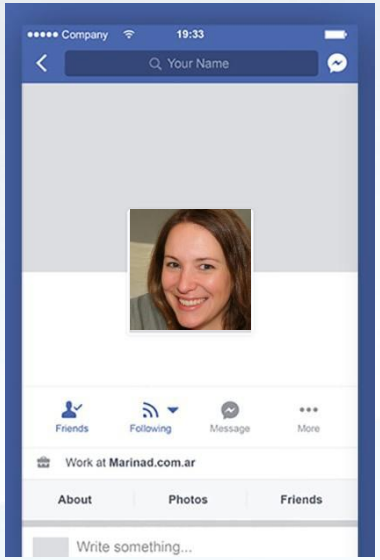
Le faux support technique



L’ingénierie sociale : simple et efficace !



Exploration des
données publiques



Exploration des
réseaux personnels

Exploration des
réseaux professionnels

Paul H

Directeur

Charlotte B

Secrétaire

Marie-Gaëlle S

Comptable

Les escroqueries

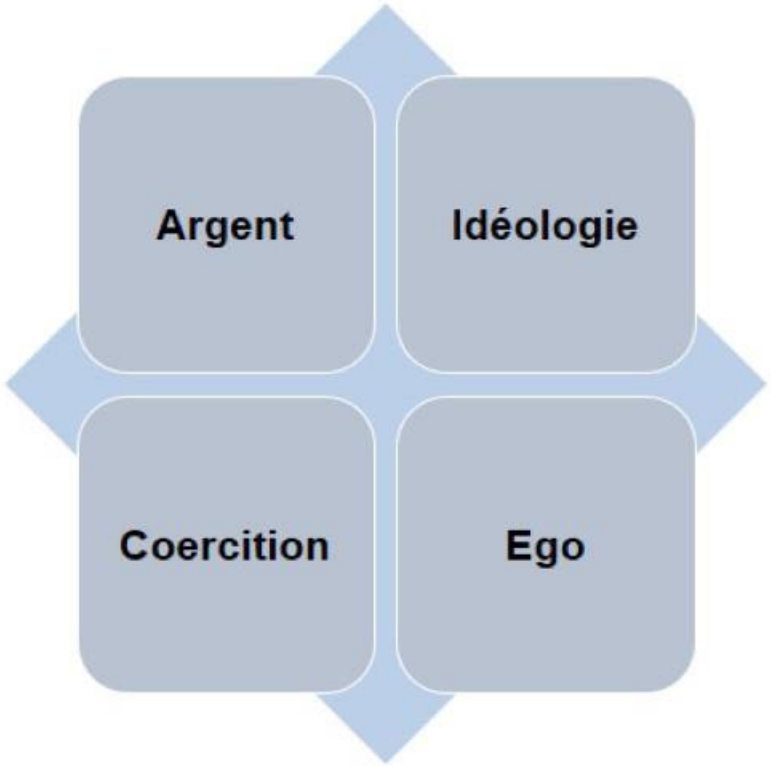
Art 313-1 CP:

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.

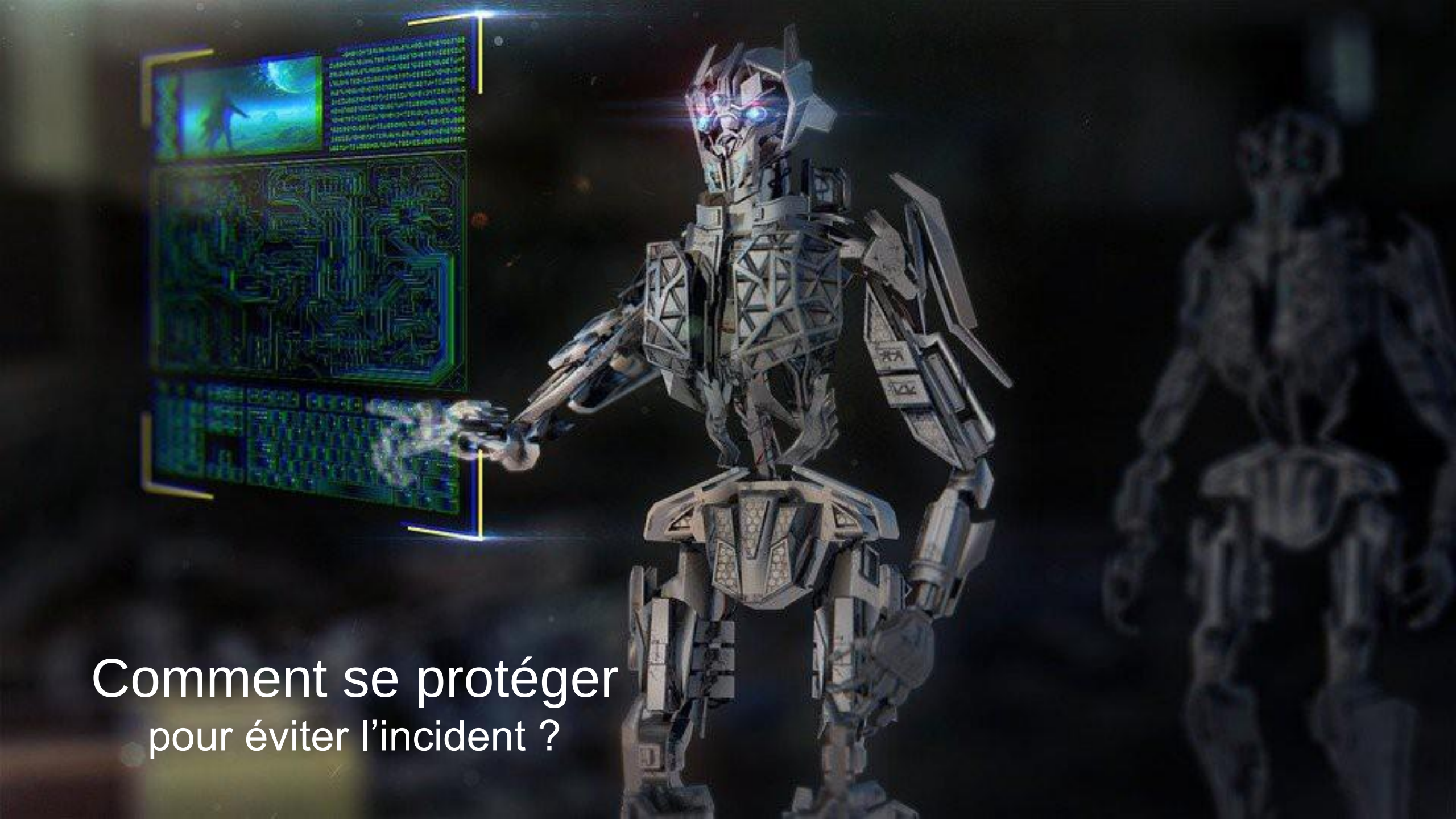
- Escroqueries aux faux virements étrangers
- Escroqueries aux faux investissements sur le foreign exchange (FOREX)
- Escroqueries aux placements indexés sur les cryptomonnaies
- Escroqueries aux faux supports techniques
- Escroqueries à la fausse amitié (Scam romance)
- Escroquerie au RGPD
- Escroquerie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

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

Matrice MICE + Réseaux sociaux



Facebook
Twitter
Instagram
Pinterest
viadeo
LinkedIn



Comment se protéger

pour éviter l’incident ?

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 vigilant vis-à-vis des mails !

Règle n°1 : **Contrôlez TOUJOURS** votre source

http://www.doct0lib.cf

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 ?

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

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 : utilisez un coffre-fort numérique (ex : Keepass)
- Activez la double authentification

Quelle est la durée de vie de ces mots de passe ?

1

020699

- 4 minutes
- 4 heures
- 4 jours

2

Max!$21

- 1 jour
- 1 mois
- 1 an

3

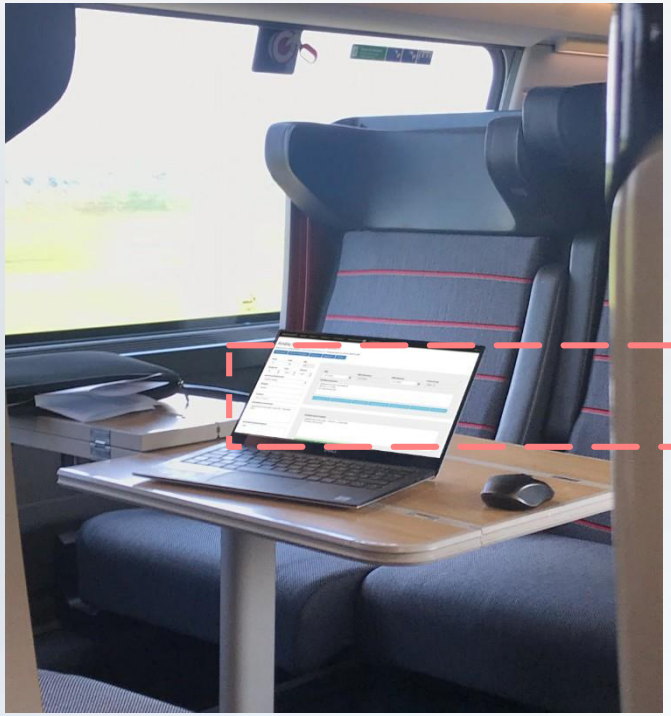
Max_&_Laura_2005

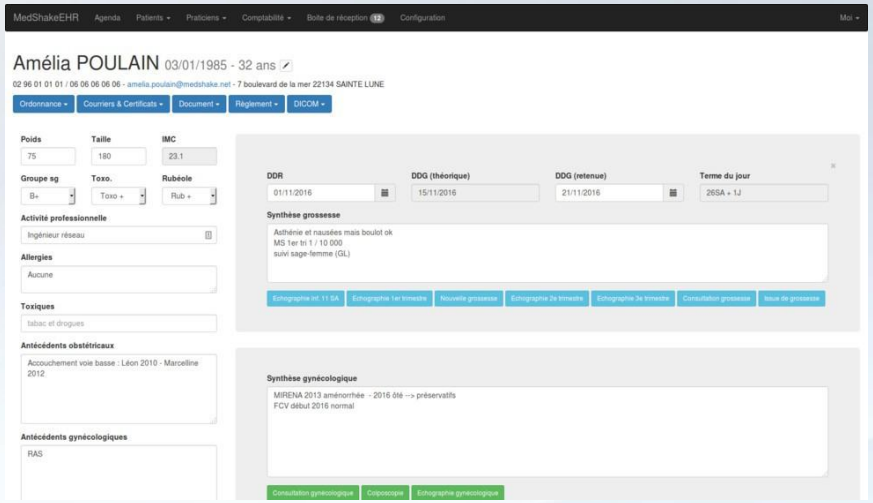
- 50 ans
- 500 ans
- 5+ millions ans

Un mot de passe LONG est un mot de passe FORT

Comment se protéger ?

4) Surveillez votre matériel





- Utilisez un filtre d’écran
- Verrouillez votre session
- Conservez vos équipements avec vous
- Évitez de vous connecter au Wifi public

5) Sauvegardez vos données !

La sauvegarde : votre dernier recours

Sauvegardez vos données importantes sur plusieurs supports

Mettez en place une sauvegarde automatique programmée

Chiffrez vos supports externes et les documents sensibles qu'ils contiennent

Utilisez uniquement des périphériques que vous maîtrisez

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 !

Comment réagir

en cas l’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

Le dépôt de plainte

Quand et comment déposer plainte ?

Il est primordial de déposer une plainte en cas de menaces, pour les mêmes raisons que nous portons plainte pour tout acte répréhensible dont nous sommes victime.

- 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

Des ressources

ttps://www.ss1.gouv.fr/entrepnse/bonnes-pra 1gues/

https://secnumacademie.gouv.fr/

CNIL.

https://www.Cnt .fr/fr/cybersec r e

https. /

,.. gouv.fr/cybermenaces ennalve·11an

Merci de votre attention

Vos questions