Vous qui entrez ici abandonnez tout espoir

Dante , La Divine Comédie

Landes Esprit Micro

Rec Offensive

Les Cyberattaques

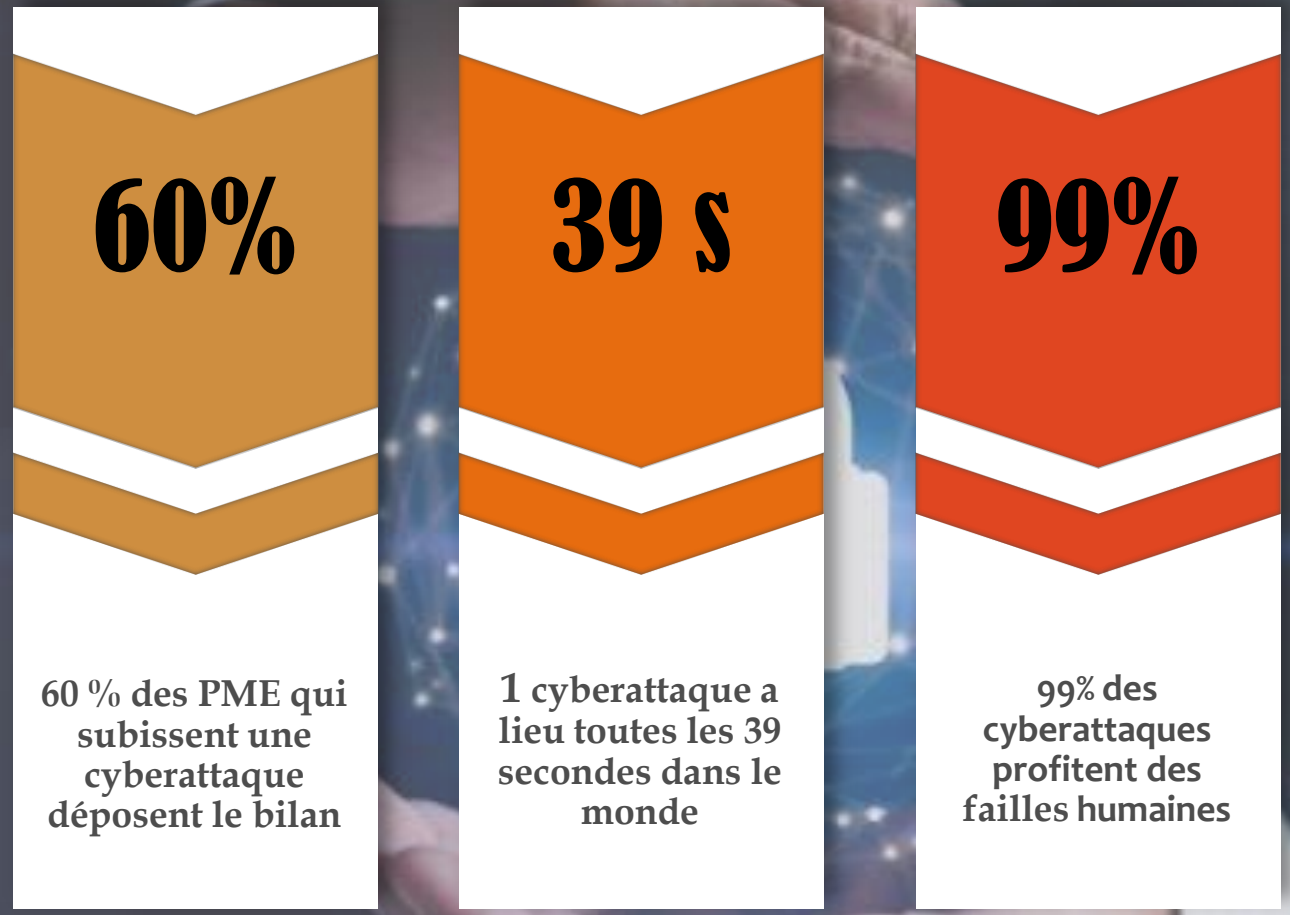
60% des entreprises qui subissent une cyberattaque déposent le bilan dans les **6 mois**.

80% auront déposé le bilan avant **1 an**.

Un risque qui ne pèse pas que sur les grandes entreprises : PME-TPE sont tout autant concernées.

Clairement la posture défensive dite de cybersécurité ne suffit plus. Les répercussions financières peuvent courir sur des mois, voire des années !

Aux entrepreneurs d'adopter désormais une démarche globale et pro-active : la cyber résilience et la sécurité Offensive.



QUELQUES CHIFFRES

Les cybercriminels créent en moyenne
11 500 nouveaux virus chaque jour.

25 sept. 2024

En 2024, **Kaspersky** a détecté
467 000 fichiers malveillants par jour

12 décembre 2024

Soit

170 455 000 ***de nouveaux fichiers malveillants***

détectés par an *(+14% par rapport à 2023)*

4 millions de nouveaux virus / an

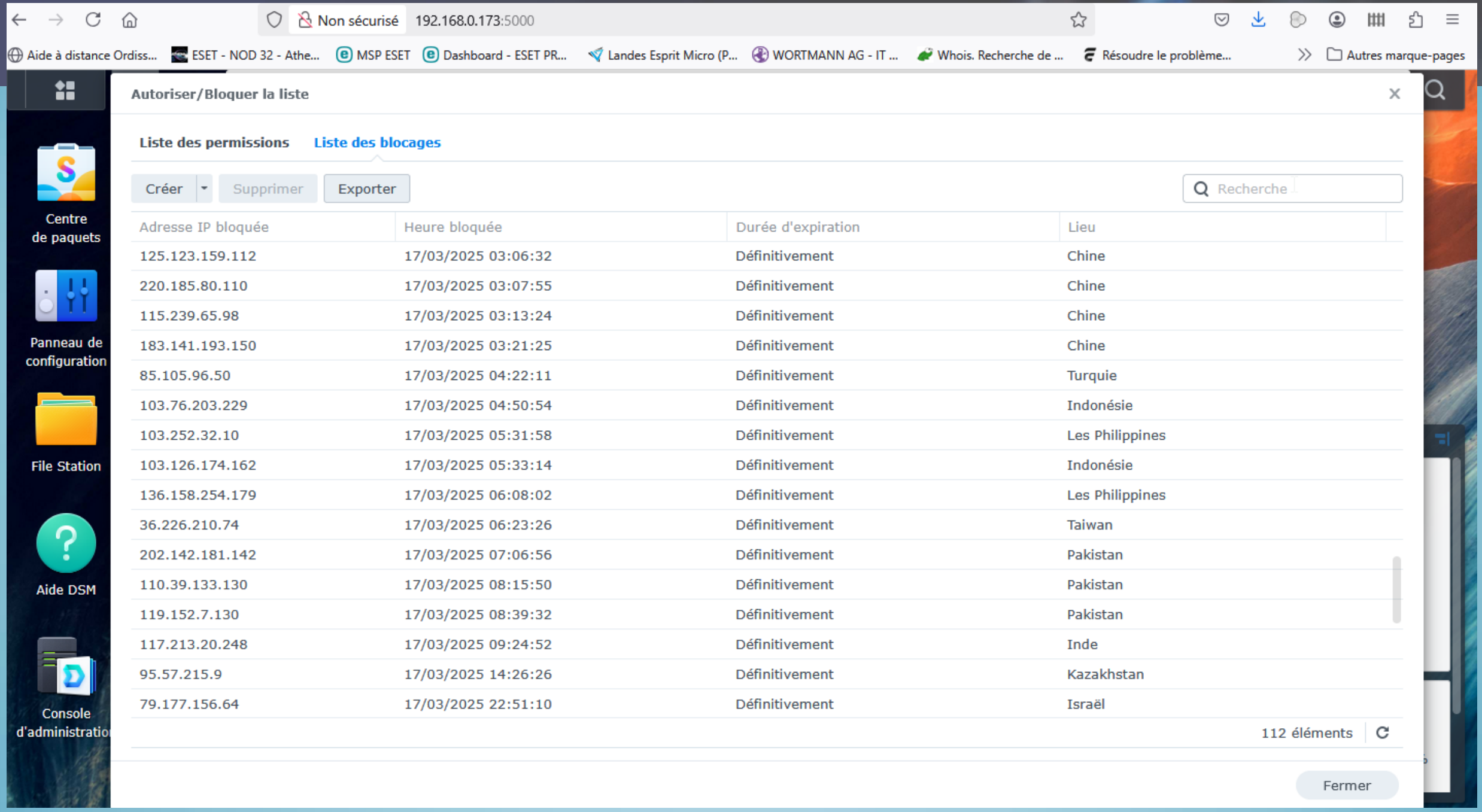
UN EXEMPLE

Selon vous combien de temps faut-il avant qu'un appareil connecté commence à se faire attaquer ?

Pas besoin d'attendre…

Les premières attaques arrivent le jour même

Nous avons mis en place un NAS pour un client le jour même, il a subi ses premières attaques et tentatives d'intrusion. En 5 jours, il a subi 112 attaques de partout dans le monde (le plus grand nombre en provenance de la chine)



A QUOI SERT UN TELEPHONE ?

Téléphoner

Envoyer des SMS et MMS

Prendre des Photos

Consulter ses mails

Consulter ses comptes bancaires

Passer des commandes

Effectuer des Paiements

OUI MAIS SUR LES TELEPHONES ?

33 ***millions d'applications dangereuses*** recensées par le laboratoire de recherche **AV-Test** en **2022**.

La plateforme macOS d'Apple est également visée par les cybercriminels, avec **900 000** variantes de malwares ciblant macOS la même année.

Android: *La probabilité d'attaque est passée de* ***34 %*** *en* ***2023*** *à* ***84 %*** *en* ***2024****.*

iOS: *La probabilité d'attaque est passée de* ***17 %*** *en* ***2023*** *à* ***29 %*** *en* ***2024****.*

1,3 million d'appareils sont infectés par ce malware sur Android : voici ce qu'il faut faire

16/09/2024 · 19:15

Des chercheurs ont identifié un virus touchant près de 1,3 [illegible] d'ag

ouest france en partenariat avec

androidmt

Malware Android : 1,5 millions d'utilisateurs espionnés, et vous ?

1 octobre 2024 par Alexis Lood

Un malware a été détecté sur Android, ayant touché plus de 1,5 million d'utilisateurs. Soupçonné de voler des données personnelles pour les envoyer vers la Chine, le logiciel malveillant est sous surveillance.

01net

Rechercher une news, produit, un logiciel, ...

Newsletter

ACTU TESTS ASTUCES TELECHARGER BONS PLANS

Produits Logiciels Gaming Technos Sécurité Société Télécoms Auto Médias Politique & Droits Sciences Cryptomonnaie Intelligence artificielle

01net · Actualités · Sécurité

Le malware Necro a piraté 11 millions de smartphones Android via le Play Store

24 septembre 2024 à 10:01

Kaspersky a découvert une nouvelle version du malware Necro sur le Google Play Store. Caché dans deux applications Android légitimes, il a infecté plus de 11 millions d'utilisateurs dans le monde. Le virus utilise des techniques sophistiquées pour dissimuler ses activités frauduleuses.

Une fuite massive : 70 millions de comptes français en vente sur le dark web

Posted On 04 Mar 2025 By : Damien Bancal Comment: 0

Une gigantesque **base de données comprenant 70 millions d'ad**
électroniques et de mots de passe appartenant à des Français
découverte par ZATAZ via son service commercial de veille, **ZATAZ**
Cette fuite colossale soulève des inquiétudes majeures quant à l'origine
informations et aux risques qu'elles représentent. Selon les pre
analyses, ces données semblent avoir été compilées avec des **inform**
datant de 2024/2025, ce qui renforce leur dangerosité.

PLANETE SCIENCES SANTE TECH MAISON CONSO DARK MODE JE M'ABONNE

ANDROID : JUDY, UN MAL...

Android : Judy, un malware caché dans Google Play, a peut-être infecté 36 millions de smartphones

SÉCURITÉ VIRUS SMARTPHONE ANDROID ANTIVIRUS

ACTUALITÉ · 7 MIN

lusieurs dizaines d'applications présentes dans le magasin officiel
oogle Play installaient un logiciel malveillant, le malware Judy, qui

PAR MARC ZAFFAGNI
JOURNALISTE

Publié le 16 avril 2024 à 14:31

01net

01net › Actualités › Sécurité

Cyberattaque massive sur le Play Store : plus de 300 apps Android criminelles veulent infiltrer votre smartphone

19 mars 2025 à 08:56

Une vaste campagne malveillante frappe le Google Play Store. Selon les chercheurs de Bitdefender, des pirates ont réussi à glisser plus de 300 applications Android frauduleuses sur la boutique, sans éveiller les soupçons de Google. Ces apps sont programmées pour vous bombarder de publicités intrusives et piller vos données personnelles, y compris vos numéros de carte de crédit.

Début du mois de mars 2025, les chercheurs de IAS Threat Lab ont découvert une vaste campagne malveillante sur

D'OÙ VIENNENT CES ATTAQUES ? QUELLES SONT LEURS MOTIVATIONS ?

Attaquants

Externes (94%), Internes (7%), Multiples (2%), Partenaires (1%)

Motivations

Financières (97%), Espionnage (1%), Commodité (1%), Représailles(1%)

Données compromises

Identifiants (54%), Données internes (37%), Données Personnelles (22%), Systèmes (11%)

Les Grandes attaques « à la mode »

que vous pourriez rencontrer…

Les attaques DDOS
Les Ransomwares
Le Phishing (hameçonnage).
L'arnaque au faux président ou au faux fournisseur.
L'arnaque au Faux Ordre de VIrement (FOVI)
L'arnaque au faux support technique
L'arnaque au faux conseiller bancaire

Les attaques DDOS

Le site que vous demandez n'est plus accessibles...

Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé

(pour cela on utilise des centaines ou des milliers de pc « zombies » qui attaquent une même « cible » au même moment)

LES RANSOMWARES

Comment tout perdre en quelques instants…

Un **ransomware** est un type de programme malveillant conçu pour crypter les données des utilisateurs et forcer les victimes à payer une rançon pour que leurs fichiers soient déchiffrés

Seules des sauvegardes à jour, externalisées et/ou déconnectées de tous vos équipements peuvent vous sauver…

LE PHISHING

1,76 milliard d'URL frauduleuses envoyées dans le monde

L'hameçonnage ou phishing en anglais est une **technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles** (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

L’arnaque au faux Président

La "fraude du président" consiste à convaincre un employé de l'entreprise d'effectuer d'urgence un transfert important d'argent à un tiers pour effectuer une tâche émanant de la direction, sous prétexte d'une dette à payer, d'un contrat à honorer, d'un nouveau partenaire...

- **Ne cédez pas à la pression.**
- **Vérifiez toujours l’origine d’un e-mail. Essayez de contacter la personne par d’autres moyens afin de vérifier la demande directement auprès de cette dernière.**
- **Respectez les processus internes pour les transactions financières.**
- **Faites-vous justifier par écrit chaque transaction demandée.**

L'arnaque au Faux Ordre de Virement (FOVI)

Souvent, vos coordonnées bancaires sont indiquées au bas de nos devis, commandes et factures… Ainsi, si le document est intercepté, un simple LOGICIEL de retouche d'image sera suffisant pour modifier l'IBAN…

Il est donc important de spécifier sur tous vos documents un rappel :

POUR LUTTER CONTRE LES ARNAQUES AUX ORDRES DE VIREMENT, avant d'intégrer nos coordonnées bancaires, nous vous invitons à nous appeler pour confirmer les coordonnées saisies dans ce document. Merci

IDEM sur les factures que vous recevez. En cas de changement d'IBAN, Appelez votre interlocuteur pour confirmer la véracité du RIB reçu …

La Procédure de RECALL bancaire

Lorsqu'une entreprise lance un ordre de virement, si une erreur est faite lors de la saisie des informations du bénéficiaire, du montant ou encore en cas de fraude, il existe la procédure de recall. Cette procédure consiste à rappeler les fonds auprès de la banque du bénéficiaire.

Attention dans les cas de virements dit « Immédiats », le RECALL est souvent plus difficile car les fonds sont virés immédiatement et dans la foulée vont être virés aussi rapidement sur d'autres comptes bancaires

Mais, les banques se heurtant à de plus en plus d'arnaque de ce type, essaient autant que possible de limiter la procédure de RECALL ou oublient de vous en parler et depuis début 2025 ont pu faire changer la loi : https://www.economiematin.fr/fraude-bancaire-remboursement-droit-refus-banque

L'arnaque au faux support technique

Votre système informatique bloque, un message de Microsoft, Google (ou autre) apparait vous informant que vous avez été piraté et qu'il faut appeler au numéro indiqué pour qu'ils puissent agir…

Que faut-il faire ?
Tout simplement…

ETEIGNEZ VOTR ORDINATEUR et REDEMARREZ

L’arnaque au faux conseiller bancaire

Cette escroquerie consiste à se faire passer pour un conseiller bancaire, l’alertant d’une possible attaque informatique sur son compte. A la demande de cette personne, qui indiquait procéder à des vérifications, le client a utilisé son code confidentiel pour supprimer puis réinscrire des bénéficiaires de virements.
Tout simplement…

NE DONNEZ AUCUNE INFORMATION. RACCROCHEZ ET RAPPELEZ VOTRE BANQUIER SUR SA LIGNE DIRECTE OU A L’AGENCE

Car plus les attaques sont invisibles, plus les virus peuvent rester dans l'appareil, plus ils vont pouvoir récolter des infos, s'insinuer dans le système et se préparer à agir au moment venu en faisant un maximum de dégâts…

Et d'ailleurs, amusons nous un peu à voir comment se passent certaines attaques…

LES KEYLOGGERS

« écoutent » tout ce que vous tapez...

Un keylogger est un "enregistreur de touches". Autrement dit, c'est un spyware (logiciel espion) capable de détecter les frappes sur le clavier de votre ordinateur et de mémoriser ou transmettre toutes les données que vous entrez.

ANDROID PAYLOAD

Les agents dormants...

Les payloads, ou charges utiles, sont les éléments de cyberattaques qui provoquent des dégâts. Les payloads malveillants peuvent rester en sommeil sur un ordinateur ou un réseau pendant plusieurs secondes, voire plusieurs mois, avant d'être déclenchés.

LE SPOOFING

vous avez un appel...

Un hackeur se fait passer pour une entité valide en falsifiant un numéro de téléphone ou une adresse IP. Le but est de tromper la victime pour obtenir des informations confidentielles ou infiltrer un réseau.

LE PAIEMENT SANS CONTACT

Risqué ou non selon vous ?

MasterCard nous certifie que non !

https://www.mastercard.com/news/europe/fr-be/points-de-vue/fr-be/2021/les-6-mythes-du-paiement-sans-contact/

Mais beaucoup d'autres ne semblent pas d'accord…

https://www.maaf.fr/fr/vie-quotidienne/paiement-sans-contact#chapitre1

https://www.journaldunet.com/patrimoine/finances-personnelles/1531943-hf1-arnaque-sans-contact-hausse/

SE CONNECTER N'IMPORTE OÙ

Les WIFI & QRcodes ne sont pas vos amis…

Le Réseau WIFI ou le QRCode sur lequel vous vous connectez n'est peut-être pas sur, il peut avoir été piraté très facilement (comme vous l'avez vu pendant la présentation).

Ne vous fiez qu'aux réseaux wifi dont vous pouvez être surs et surtout pas aux QRCodes.

« Pourtant ma connexion est sécurisée en HTTPS » !

Le protocole HTTPS est un protocole qui crypte les données transmises de votre poste au site internet concerné…

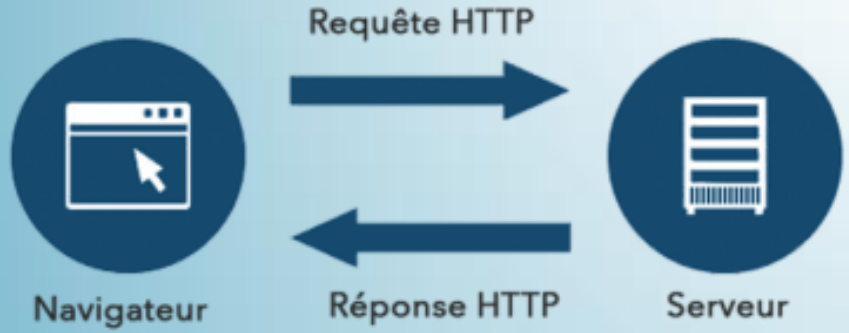
- Si le pirate / hacker a accès à votre machine, cela ne sert à rien… il récupère les infos avant qu'elles ne partent de votre ordinateur (virus, keylogger, …)

- Si le hacker pirate le site web à l'autre bout c'est pareil !

- Et si vous êtes dirigés vers un faux site, c'est encore pire !

« Pourtant ma connexion est sécurisée en HTTPS » !

Une requête HTTP classique



Une requête HTTPS classique

En cas d'attaque Cyber...
Que faire ? Et dans quel ordre ?

6 - Faire un Signalement sur Perceval (fraude bancaire)
5- Faire une déclaration sur cybermalveillance.gouv.fr
7 - Aller porter plainte (gendarmerie ou police)
2- Débrancher l'ordinateur d'Internet
1 - Eteindre complètement son ordinateur.
3- Prévenir sa banque (si fraude virement, CB, ...)
4 - Appeler son informaticien préféré
8- Faire vérifier son ordinateur / son parc informatique
9 - Installer un bon antivirus et mettre en place un système de sauveg.

Comment se protéger ?

- Analyse Préventive de votre Parc informatique (*Rec Offensive*)

- Avoir un Antivirus

- Installer un Pare-feu

- Utiliser un VPN

- Protégez vos mails

- Protégez vos téléphones

- Faire des Sauvegardes

- Gérer vos Mots de Passe

Et, surtout être **ATTENTIF** car 99% des attaques sont dues à …

des FAILLES HUMAINES

L'analyse preventive… Quelle difference ?

Offensive

VS

Défensive

La sécurité offensive, ou OffSec pour Offensive Security, est une approche proactive de la cybersécurité qui consiste à identifier les vulnérabilités des actifs numériques avant que les attaquants ne puissent les exploiter, améliorant ainsi la sécurité globale des organisations.

L'OffSec passe par l'utilisation de divers outils, techniques et méthodologies pour simuler des attaques sur un système cible, dans le but d'identifier et de signaler les éventuelles failles de sécurité.

La cybersécurité au sens classique du terme se concentre principalement sur la prévention et la détection des attaques, et comprend des mesures telles que :

- La mise en place de pare-feu
- Les antivirus
- Les systèmes de détection et de prévention des intrusions
- Les politiques et les procédures de sécurité

L'objectif principal de la cybersécurité "Défensive" est d'empêcher les attaques et de minimiser les dommages causés par celles qui aboutissent.

Comment se protéger ?

- Analyse Préventive de votre Parc informatique (*Rec Offensive*)

- Avoir un Antivirus

- Installer un Pare-feu

- Utiliser un VPN

- Protégez vos mails

- Protégez vos téléphones

- Faire des Sauvegardes

- Gérer vos Mots de Passe

Et, surtout être **ATTENTIF** car 99% des attaques sont dues à …

des FAILLES HUMAINES

Est-ce encore utile d'avoir un antivirus ?

Un antivirus est un outil qui est à même de protéger et d'analyser votre ordinateur pour repérer, supprimer ou mettre en quarantaine les fichiers dangereux, voire de réparer les fichiers infectés.
Actuellement, et contrairement à ce que l'on peut lire sur un certain nombre de sites webs ou dans certains magazines… Il est de plus en plus important de posséder un antivirus sur son ordinateur et sur son tel portable… et si possible performant… voire ultra performant !!!

Pour rappel, fin **2024** nous étions à **14** Millions de nouveaux malwares / mois)

Alors, vous pouvez ne pas en mettre !

(Et vous tirer une balle dans le pied tout en vous disant que la balle va passer à coté !)

Antivirus basique, Internet Security ou 360

Ces 3 versions de logiciels protègent l'utilisateur des virus, des programmes malveillants en les bloquant et en les supprimant. Il existe des similitudes et des différences entre eux.

L'une des principales différences est qu'un simple **Antivirus** protège l'ordinateur contre les virus, alors qu'une version **Internet Security** intègre souvent
- un pare-feu,
- un modules de protection de vos transactions bancaires
- tout en offrant une protection plus efficace contre les logiciels espions, les virus, le phishing, le courrier indésirable et les pièces jointes.

Et le 360 alors ? Lui, en plus il vous prépare le café !

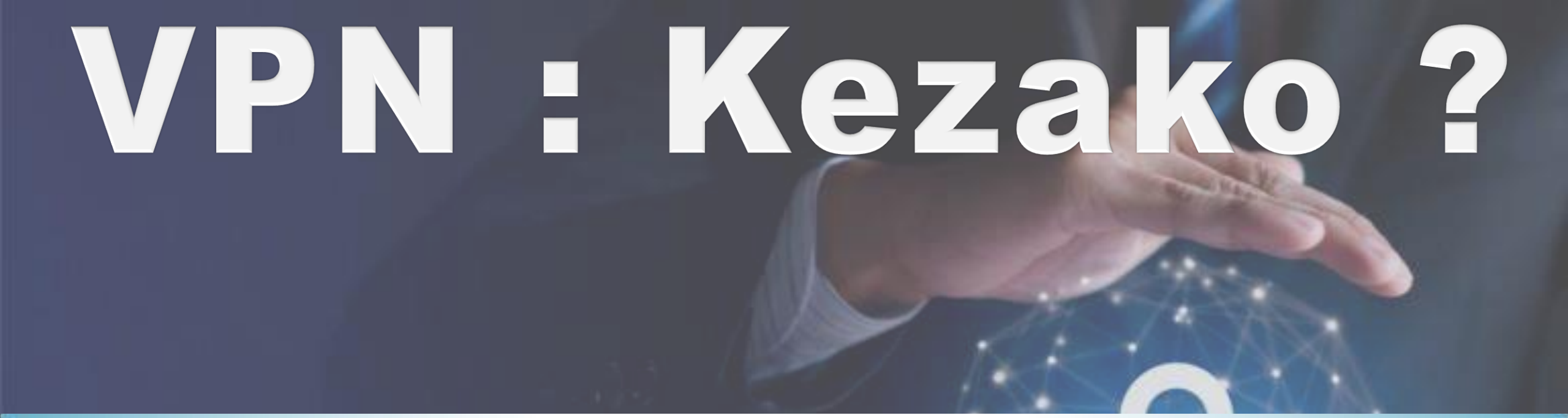
En fait le 360 est plutôt réservé pour les anxieux en rajoutant des Sandbox et des fonctionnalités supplémentaires mais souvent il est particulièrement lourd pour l'ordinateur et prend trop de cycles machines !!!

L’utilisation d’un Pare-feu

Un pare-feu est un système de protection (logiciel et/ou matériel) qui a pour mission de filtrer le trafic entrant et sortant sur votre réseau informatique. Autrement dit, il se pose en intermédiaire entre votre réseau interne d'entreprise et le réseau externe qu'est Internet et vérifie tout ce qui entre et sort.

Windows intègre un pare-feu par défaut et la plupart des antivirus avancés en intègrent également un autre…
Il est suffisant pour la majeure partie des utilisateurs qui ont un comportement prudent sur internet.
Mais ATTENTION : bien que le pare-feu Windows bloque bien le trafic entrant, il ne fait que surveiller (sans bloquer) le trafic sortant !

VPN : Kezako ?



Un VPN ou Réseau Privé Virtuel crée une connexion réseau privée entre des appareils via Internet. Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics.

Le VPN est donc un logiciel qui s'installe sur plusieurs appareils reliés à Internet. Une fois le VPN activé, un tunnel sécurisé se créer entre vous et le réseau Internet. De cette manière, les informations qui y transitent seront chiffrées. Aussi, précisons que l'activation s'effectue en se connectant à un serveur VPN distant. Ainsi, vous obtiendrez une nouvelle adresse IP d'emprunt et la vôtre sera masquée.

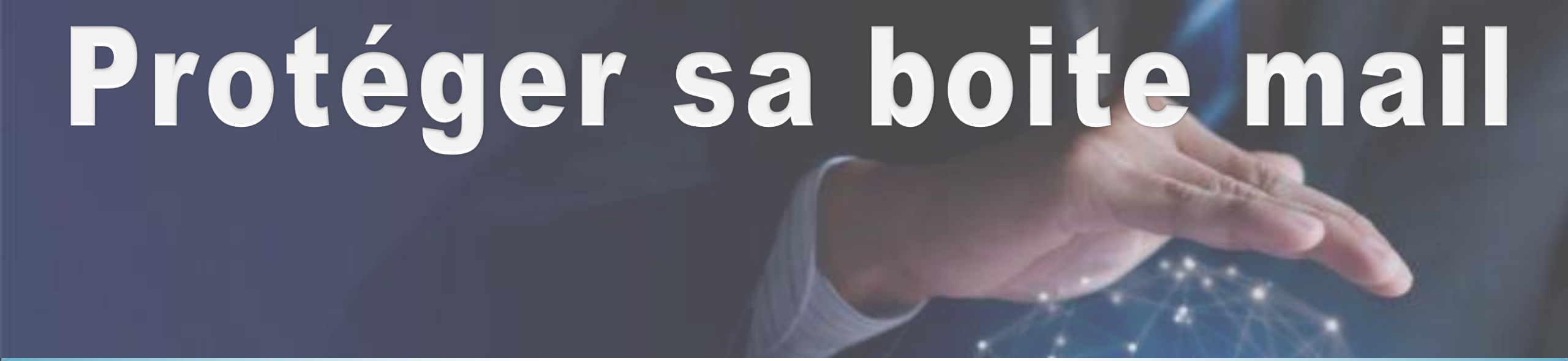
VPN : pour qui ? Pour quoi ?

Qui utilise les VPN ?

- Les sociétés ayant des filiales ou des agences distantes.
- Les personnes qui ont besoin de masquer certaines informations ou actions.
- Ceux qui ont besoin de débloquer l'accès à certains sites ou contourner la géo-restriction.
- Ceux qui veulent faire des economies…

-Parmi les VPN les plus connus, on trouve ExpressVPN, Cyberghost, NordVPN, …

Protéger sa boite mail



Tous les jours des mails importants sont mélangés à des mails sans intérêts ou potentiellement dangereux

Pour lutter contre les boites mails qui foisonnent de spams (pubs ou escroqueries diverses, …) il existe des solutions ANTISPAMS de 3 types :

- Activées (ou non…) par votre Fournisseur de messagerie.

- Intégrées sur votre pc ou votre client de messagerie : Spamfighter, modules liés à votre antivirus ou votre client de messagerie.

- Interface intermédiaire : Altospam, Mailinblack, solution payante mais TRES EFFICACES

Comment reconnaitre un faux mail ?

From : NOM AFFICHÉ EXPEDITEUR <e
To : NOM AFFICHÉ CLIENT<destinataire
Message-ID : <b079478f-66ca-40f4-a400-b5
Received : from opme11d2d04aub.bagnolet.francetelecc
LMTP id yMlCF0mcQGWTDgAA+elHag:T525:P1:P1 (e
+0100,from opme11ppr08aub.idf.fr.intraorange ([10.79.
yMlCF0mcQGWTDgAA+elHag:T525:P1 (envelope-fron
dQkbdlfnLVv9a+Titg/SJJJoRklMVunUtiSBwN/lO4g=>
opme11ppr08aub.idf.fr.intraorange with LMTP id yMlC
<expediteur@fournisseur.fr>) for <destinataire@fournis
([196.115.87.183]) by smtp.orange.fr with ESMTPA id xl
X-bcc : destinataire@fournisseur.fr
X-ME-User-Auth : thebaud85@orange.fr
X-ME-IP : 196.115.87.183
X-ME-Helo : [192.168.11.110]
X-ME-Date : Tue, 31 Oct 2023 11:00:13 +0100
Content-Language : fr
User-Agent : Mozilla Thunderbird
Reply-To : NOM AFFICHÉ EXPEDITEUI

De : cfparts.finance <espacebluetrackiine33000@alterway.fr>
Envoyé : mercredi 6 juin 2018 03:00
À : GERTRADE@HOTMAIL.FR
Objet : Vos impôts ont été revus à la baisse .

Voir la version en ligne

impots.gouv.fr
un site de la direction générale des finances publiques

Madame, Monsieur,
Suite aux derniers calculs annuels liés à l'exercice de votre activité, nous avons déterminé que vous êtes éligible à recevoir un remboursement de 197,39 euros sur les sommes versées en 2017.
Pour nous permettre de traiter le dossier dans un plus bref délai, veuillez nous soumettre une demande de remboursement en ligne.
Pour accéder au formulaire, cliquez ici.
(à titre indicatif, le délai de traitement de votre demande est de 10 jours ouvrés).
Attention, le remboursement peut être retardé pour diverses raisons telles que la soumission d'un dossier non-valide ou une saisie effectuée en ligne en dehors du délai légal.

Nous vous prions d'agréer l'expression de notre sincère considération.

Le comptable public

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

Est-ce utile de protéger vos téléphones ?

D'après les experts de TrendMicro, des millions de smartphones Android arrivent sur le marché avec des *malwares* préinstallés. Ces virus sont secrètement **placés par des développeurs tiers**, à l'insu des constructeurs, dès la sortie des appareils de l'usine.
De nombreuses marques, surtout des enseignes chinoises *low cost*, s'appuient en effet sur des sociétés externes pour développer une partie des logiciels de leurs systèmes d'exploitation.
Ces développeurs peu scrupuleux profitent du partenariat avec le fabricant pour gonfler leurs revenus en affichant **des publicités intrusives** ou en volant vos données personnelles.

Donc est-ce utile selon vous ?

Tout dépend de ce que vous faites avec votre téléphone…

Plus vous faites de choses importantes avec (accéder à des sites importants, à vos comptes bancaires, …),
plus c'est utile… !

Faire des Sauvegardes

Pour éviter de tout perdre, faire des sauvegardes est OBLIGATOIRE…
Pour cela, nous préconisons la mise en place d'une stratégie de sauvegardes dite 3 – 2 – 1

3 COPIES D'UN MÊME FICHIER

2 SUPPORTS DE SAUVEGARDE DIFFERENTS

1 SAUVEGARDE EXTERNALISEE

Une sauvegarde (type disque dur externe) déconnectée et externalisée est une des meilleures solutions pour la sécurité de vos données.

Et l'avenir de la sécurité ?

Là aussi, il n'y a pas beaucoup de raisons d'être optimiste !

- Le nombre d'intrusions et d'attaques augmente de manière exponentielle.

- De nouvelles techniques d'attaques apparaissent tous les jours

et surtout :

- L'arrivée de **l'I.A.** et de **l'I.O.** va encore amplifier les risques **CYBER**.

4 Octobre 2023 : Chantage à la fausse sextape, manipulations bancaires… En Chine, le développement de l'intelligence artificielle (IA) fait passer l'escroquerie en ligne à un niveau inédit. Dans une société où tout est enregistré, des caméras de surveillance à la reconnaissance faciale sur smartphone, les données relatives aux visages ou à la voix des individus se monnaient à vil prix sur Internet.

https://www.courrierinternational.com/article/cybercriminalite-la-chine-confrontee-au-trafic-des-visages-voles-de-l-intelligence-artificielle

Car, avec l'arrivée de l'IA ...

Cela fait plusieurs années que l'IA est utilisée à des fins de malveillance par les cybercriminels.
L'usage de l'intelligence artificielle permet d'améliorer des techniques d'attaques déjà utilisées telles que la personnification, le spearphishing, la target selection ou le persona building.
Connu de tous, l'hameçonnage (phishing) est aujourd'hui de plus en plus efficace grâce aux technologies d'IA disponibles pour générer de façon automatique de fausses informations telles que des vidéos, des articles, des messages ou encore des données personnelles.
Cela est possible grâce à une ingénierie sociale qui peut être automatisée en une veille pour identifier les cibles les plus vulnérables à l'aide des données issues des réseaux sociaux.

Pour Conclure…

5 REGLES A NE PAS OUBLIER

1 – FAIRE ATTENTION !

Rien ne remplace la réflexion et le fait de faire attention à tout ce qui peut être suspect !

2 – NE PAS CLIQUER OU TÉLÉCHARGER N'IMPORTE QUOI.

Ni depuis n'importe où…
Clubic, 01.net, Telecharger.com, lesnumeriques.com, xxx.softonic, …
Tous ne sont pas fiables !

3 – NE PAS SE CONNECTER N'IMPORTE OU.

4 – INSTALLER UN BON ANTIVIRUS.

5 – FAIRE DES SAUVEGARDE DE VOS DONNÉES.

Et comme je ne sais pas compter… je vais en rajouter une sixième…

6 – EN CAS DE DOUTE FAIRE APPEL A SON INFORMATICIEN

Si vous avez des questions…

N’hésitez pas à faire appel à …

Landes Esprit Micro

Eric Mussotte

09 53 059 987

contact@landesespritmicro.com

www.landesespritmicro.com

Rec Offensive

Marvin Descamps

06 51 36 90 65

contact@recoffensive.fr

Merci

Rec Offensive

lem
Landes Esprit Micro