Les virus ? C'est démodé !!!

Nous sommes tous utilisateurs d'informatique et d'internet…
Nous ne vivons pas dans un monde de Bisounours qui nous veulent du bien…
Je vous parlerai aujourd'hui des menaces auxquelles nous sommes amenés à faire face, de la publicité ciblée, ainsi que de la manipulation des prix.
L'imagination des escrocs, influenceurs, vendeurs et publicitaires est sans limites et je suis certain de ne pas couvrir pas l'entièreté du sujet !!!

Un peu d'histoire

L'escroquerie n'est bien sûr pas une nouveauté : dès le XVIe siècle sont apparues des « lettres d'Espagne » qui proposaient une partie de la fortune des « prisonniers » en échange du paiement de leur rançon. Vidocq, dans son livre « Les voleurs » (1836), en présente une variante, avec les « lettres de Jérusalem » (envoyées par des bagnards de Cayenne). Des réunions « Tupperware » ont proposé des systèmes pyramidaux dès les années 50 (ventes pyramidales de savon, assurances, jeu de l'avion…) le but n'était pas le produit, mais l'organisation et le recrutement.

Social engineering (phishing, SMiShing, etc.)

On a tous reçu des messages publicitaires à la pelle, ciblés ou non, des e-mails étranges, etc. Tous les moyens de vous contacter sont utilisés ! En voici quelques exemples : vous avez gagné à une loterie à laquelle vous n'avez aucun souvenir d'avoir participé, une superbe femme est tombée raide dingue de vous, mais vous n'avez aucune idée de qui il s'agit, un notaire vous écrit pour vous offrir un héritage de quelqu'un dont vous ignorez l'existence, la police ou Interpol vous reproche une infraction grave, une banque vous

signale un compte piraté, une facture impayée, un remboursement, etc., votre compte Google vient de subir une tentative d'accès frauduleuse, vous avez soi-disant utilisé une image soumise à copyright sur votre site…

Tous ces mails ont un point commun : ils veulent vous faire réagir vite, et ce, afin que vous ne preniez pas le temps de réfléchir ou de vous renseigner.

C'est pourtant avec un minimum de sang-froid et de réflexion que vous pourrez détecter le problème.
La première chose à ne surtout pas faire, c'est de cliquer sur le lien qui vous est proposé dans le mail en question : il est fort probable que ce lien vous amènera sur un site falsifié ressemblant à votre banque, votre opérateur téléphonique ou autre…
Ces faux sites peuvent aussi exister indépendamment et utiliser une autre astuce pour apparaître à la place du vrai, parfois simplement en changeant une lettre ou une extension : un i remplacé par un l, un O par un 0, un. org par .net ou .com…

Heureusement, toujours actuellement, la plupart de ces tentatives sont faites par des script-kiddies. Donc un simple coup d'œil, la détection d'une adresse d'expéditeur fantaisiste et le réflexe de ne pas cliquer sur n'importe quoi sans se méfier peuvent déjà suffire. La majorité des techniques utilisées est bien connue, car souvent élémentaire et utilisée jusqu'à plus soif.

La fonction « afficher la source » de votre programme mail permet en outre de mieux repérer certains détails inquiétants.

Concernant l'orthographe ou les tournures douteuses, dans certains cas, c'est voulu !!! Sur un phishing type « *prisonnier espagnol* », cela permet de passer pour un non-francophone ou de ne pas perdre son temps avec les gens plus instruits qui relèveraient le problème immédiatement.
Sur un courrier de prétendus notaires ou avocats (héritage, copyright troll) ce serait évidemment se tirer une balle dans le pied.
Certains sont de plus en plus futés, innovent, utilisent l'AI, masquent mieux les adresses ou sites frauduleux, qui apparaissent plus vrais que les vrais.
Le black friday, avec son flot de pubs et spam, est une occasion de passer des scams (escroquerie, arnaque) noyés dans la masse…

C'est ici que la seconde ligne de défense que vous allez mettre en place intervient :

JAMAIS une banque ou un site légal ne vous demandera de communiquer des informations sensibles par mail ou téléphone ! Récemment certains se sont même déplacés physiquement chez des personnes âgées ou fragiles, prétendant être leur banquier pour pouvoir leur faire faire des validations d'opération en ligne
N'ouvrez jamais un lien proposé dans un mail, si tentant soit-il, et connectez-vous plutôt

d'une autre manière (celle que vous utilisez habituellement et qui est fiable) pour vérifier si le mail provient bien de qui de droit.
Certains escrocs auront pu collecter des détails plus précis sur vous : liste d'adresses, mails d'amis, détails et photos sur FB, LinkedIn…
J'ai reçu un prétendu mail d'une amie : « *je suis à Paris victime d'un accident avec mon compagnon » (appelé par son vrai nom) « fais-moi parvenir de l'argent pour payer l'hôpital »*… Ayant du temps à perdre (et surtout, envie de leur faire perdre le leur), j'ai inventé qu'un ami commun était justement sur place et qu'il allait les rejoindre de suite…

Amusant échange de mails, de plus en plus surréalistes, avec l'escroc qui cherchait à éviter la rencontre et juste recevoir de l'argent. Il a fini par abandonner… 🙄
Le père d'une amie a perdu 4000 € lors d'une vente de jantes sur marketplace : tellement embobiné par le scammer au téléphone, il a ignoré ses proches, à côté de lui, qui essayaient de le faire raccrocher pour ne pas aller plus loin ! Trop tard…

Il n'y a donc pas que les e-mails qui sont ciblés : SMS et téléphone le sont aussi (spoofing : usurpation d'identité) : un Espagnol a utilisé la technique avec de vraies lettres papier ! Retour au XVIII^{e} siècle ! Ce sont les faux timbres qui l'ont trahi. Son taux de return était de plusieurs pour cent contre 1 pour 1000 ou moins par mail !
On reçoit de plus en plus de notifications par SMS et un lien qui permet d'y répondre (par ex. via un N° surtaxé) ou d'être recontacté par téléphone par une personne qui, bien entendu, n'a rien à voir avec votre banque et vous fera utiliser votre Digipass à son bénéfice. Encore une fois, s'il y a un doute ou que c'est trop beau (ou catastrophique) pour être vrai, c'est que ce n'est pas vrai !

N'oubliez pas que le moindre document ou information peut valoir de l'or pour qui sait s'en servir, même votre simple numéro de compte.

Ce dont je viens de parler porte le nom de social engineering. Le social engineering, ou ingénierie sociale, est un ensemble de techniques utilisées pour manipuler psychologiquement la victime afin d'obtenir des informations sensibles ou de les inciter à effectuer des actions compromettantes, financièrement dangereuses ou stupides.

Techniques courantes :

1. Phishing : envoi de faux e-mails imitant des sources légitimes ou habituelles pour obtenir des informations confidentielles.
2. Spear phishing : idem, mais le mail est personnalisé par des informations plus précises (collectées sur les réseaux sociaux par exemple).

3. Vishing et SMiShing : Utilisation d'appels téléphoniques (vishing) ou de SMS (SMiShing) pour tromper les victimes et soutirer des infos bancaires.
4. Pretexting : création de scénarios plausibles pour convaincre les victimes de partager des données sensibles (par téléphone, mail, ou même en personne).
5. Baiting : utilisation d'offres alléchantes pour inciter les victimes à révéler des informations ou à installer des logiciels malveillants.
6. Piggyback :
   *suivre une personne autorisée pour pénétrer dans une zone d'accès restreint avant que la porte ne se referme ;
   *observer un mot de passe par-dessus l'épaule (distributeur bancaire par exemple) ;
   *copie à la volée d'un badge d'accès (flipper zéro)keylogger (mini boîtier sur hardware ou programme sur pc) : enregistrement des frappes clavier ;
   *man in the middle.
7. Whaling ou arnaque au président : l'escroc, après avoir collecté suffisamment d'infos se fait passer pour un directeur et demande (par mail, SMS…) aux comptabilités d'effectuer des opérations bancaires. Une variante existe également pour les particuliers…

Le social engineering repose sur l'exploitation des faiblesses humaines plutôt que sur des vulnérabilités techniques
Les attaquants utilisent souvent les 3 étapes suivantes :

1. Collecte d'informations sur la cible.
2. Etablissement de la confiance.
3. Exploitation de la relation établie.

Prévention

Pour se protéger du social engineering en entreprise, il est recommandé de :

- mettre en place des campagnes de sensibilisation régulières ;
- former le personnel à reconnaître les tentatives de manipulation ;
- implémenter des politiques de sécurité stricte ;
- utiliser des technologies de contrôle d'accès appropriées.

La meilleure défense contre le social engineering reste la vigilance et le bon sens des utilisateurs, qui pourront dès lors se protéger également dans la vie courante.

Chevaux de Troie et autres logiciels malveillants

Beaucoup d'entre nous échangent photos, PDF, jeux gratuits, vidéos amusantes… Il est possible que la vidéo de chat mignon qu'on vous envoie n'en soit pas une, mais autre chose, à savoir un exécutable, qui se lancera de façon non visible. En effet, particulièrement sous Windows, les extensions connues sont masquées par défaut : par exemple, « videodechat.avi.exe » apparaîtra comme « videodechat.avi ».

Cet exécutable installera un malware sur votre pc sans que vous vous en aperceviez. Cette technique s'appelle **le cheval de Troie**…

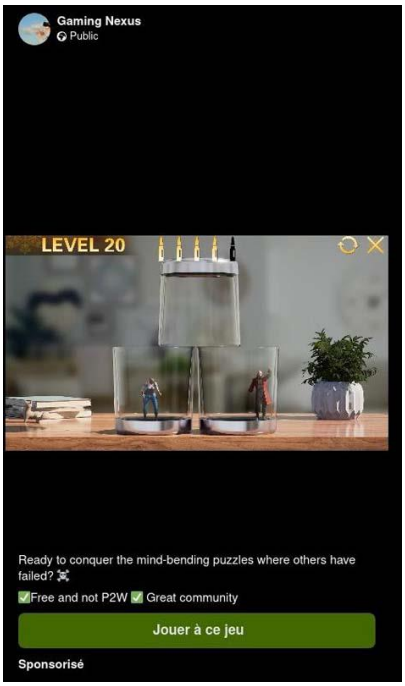
Cet exécutable installera un malware sur votre pc sans que vous vous en aperceviez. Cette technique s'appelle le cheval de Troie…

Dans le même genre, des pages web peuvent se faire passer pour un antivirus.
Ça m'amuse beaucoup quand ma vieille mère me téléphone parce qu'une page web dit que l'antivirus de Windows a détecté une menace alors que sa machine est en LINUX !
Il vous signale gentiment que vous avez été infecté… et qu'il suffit de téléphoner au N° en question pour qu'un gentil monsieur de « Miro-soft » ou de « gogole » vous aide… et vous fera faire quelques manipulations « **pour votre bien** » qui, à votre insu, lui donneront la main sur votre machine pour son propre bénéfice !

Autres exemples de trojan (ou troyen) :

- il installe un programme de minage bitcoin sur votre pc, utilisant vos ressources pour miner au bénéfice d'autres ;
- PC zombies : votre pc, en même temps que des milliers d'autres, servira à lancer des attaques DDOS et ce, sur commande du pirate. Technique imparable puisque provenant de milliers de machines différentes…

Gamethief



Les casinos et pokers en ligne sont hébergés à Malte ou dans d'autres paradis à l'abri des lois. Les procédures de récupération des gains sont tellement complexes qu'elles vous inciteront à rejouer vos gains jusqu'à les avoir finalement perdus. C'est toujours le casino qui gagne à la fin !

Des tas de jeux ou programmes gratuits fleurissent (envoyé par mail ou sur Facebook, etc.) et une bonne partie vous fait, par exemple, charger un .exe sur le PC… Oserez-vous l'exécuter sans vous méfier, maintenant que vous savez ce qu'est un cheval de Troie ?

Idem sur smartphone : si vous voulez un jeu gratuit (donc avec de la pub…), l'App Store ou le playstore ont en principe un minimum de sécurité, mais méfiance si vous allez le chercher ailleurs.

Ne croyez pas non plus que l'antivirus, même acheté très cher, va détecter des malveillants ! Il n'est tout simplement pas fait pour ça : il repère des virus, et pas autre chose !

Le virus serait donc presque une espèce en voie de disparition par rapport à toutes les méthodes plus récentes et efficaces !

Cookies, tracking de l'ip, de la signature PC, etc.

Vous voulez réserver un billet d'avion et vous cherchez le meilleur prix. Vous le trouvez mais ne réservez pas tout de suite. Le lendemain, lors de la réservation, le prix a augmenté !

En effet, le site de la compagnie aérienne vous a reconnu, a retenu que vous vous étiez connecté hier et sait que vous avez déjà effectué cette recherche (tracking via un cookie, votre historique de navigation, l'adresse ip, la signature hardware de votre PC, etc.). Il ne vous propose alors plus le prix plancher ! L'avion n'est pourtant pas plus rempli qu'hier…
Pour retrouver le prix du jour d'avant, vous pouvez faire la recherche à partir d'une autre machine (le pc d'un voisin par exemple).
Faire une recherche en navigation privée pourrait ne pas suffire, car beaucoup de compagnies sont capables de reconnaître votre pc (la compagnie irlandaise est loin d'être la seule à en abuser).

De plus, le pays depuis lequel vous réservez fera aussi varier le prix, d'où l'utilité de l'utilisation d'un VPN (gratuit) pour réserver en navigation privée depuis l'endroit où le billet est le moins cher… c'est pousser la tarification dynamique à son paroxysme.

Ce tracking sert aussi aux publicitaires pour vous bombarder de publicités ciblées. Les sites d'E-commerce le pratiquent assidûment !

Facebook, TikTok, Cambridge Analytica, Brexit et élections américaines

L'algorithme de Facebook et des réseaux sociaux en général joue un rôle crucial dans la personnalisation du contenu affiché, il varie régulièrement et de façon opaque.
Son but est de vous présenter des « informations » qui vont dans votre sens pour vous inciter à rester très longtemps (le modèle économique est notamment basé sur la pub).
Tiktok et son infinité scrolling de vidéos courtes est très addictif. Les contenus ne sont pas non modérés ni vérifiés et contiennent désinformation, publicité déguisée et influenceurs en tout genre !

- Cambridge Analytica a obtenu les données de 87 millions d'utilisateurs Facebook sans leur consentement. D'autres, moins connus, font toujours de même.
- Ces données ont été utilisées pour du microciblage politique, notamment lors de la campagne présidentielle américaine de 2016 et du référendum sur le Brexit
- d'autre nuisibles utilisent Facebook ou tik tok de la même façon (influenceurs, Qanon, organisations « religieuses », djihadistes, sectes, pseudo médecines new age, antivax…

Usurpation d'identité et arnaques

Les techniques courantes d'usurpation d'identité incluent :

1. L'**usurpation d'identité** en ligne, qui consiste à créer de faux profils ou à utiliser les informations personnelles d'une victime pour nuire à sa réputation ou commettre des actes frauduleux.
2. Le **Phishing**, où l'usurpateur se fait passer pour un organisme connu afin de récupérer des informations personnelles via de faux sites ou courriels.
3. Le **vol de documents** physiques, portefeuilles, sacs à main, courrier, poubelles ! pour obtenir des informations confidentielles.
4. L'**usurpation d'adresse IP**, N° de téléphone, permet aux cybercriminels de dissimuler leur identité et leur emplacement réels.
5. L'**usurpation de DNS** (DNS spoofing), qui redirige le trafic d'une adresse IP légitime vers une fausse adresse…
   Les providers comme Proximus, Voo, orange, etc. utilisent également des DNS menteurs pour vous empêcher d'accéder facilement à des sites qui sont « interdits » comme Piratebay, les sites de Peer to peer, etc.
   Ils affichent dans ce cas une page de la police fédérale qui dit que le site que vous essayez de visiter est « illégal ».
6. L'**usurpation de l'identité** de l'appelant, utilisant des numéros de téléphone apparemment locaux pour tromper les victimes.

L'arnaque à la webcam et ses variantes

L'arnaque à la webcam est une forme d'extorsion où les cybercriminels prétendent avoir enregistré la victime dans des situations compromettantes via sa webcam. Les variantes incluent :

1. Le **chantage à la vidéo** : Les escrocs affirment avoir capturé des images embarrassantes et menacent de les diffuser. (en fait ils n'ont rien…).
2. L'a**rnaque à la vidéo en direct** : Les criminels utilisent des vidéos préenregistrées pour simuler une interaction en temps réel. (vous croyez discuter avec la fille de vos rêves, mais c'est un Camerounais au cybercafé !) L'AI va pouvoir les aider très efficacement quand ils sauront mieux s'en servir !
3. Le **piratage de webcam réel** : Dans de très rares cas, les cybercriminels peuvent effectivement prendre le contrôle de la webcam d'une victime.

Risques liés aux réseaux sociaux

Les réseaux sociaux présentent plusieurs risques en matière d'usurpation d'identité :

1. **Surexposition d'informations personnelles** : Les utilisateurs partagent souvent trop de détails personnels, facilitant le vol d'identité.
2. **Création de faux profils** : Les escrocs peuvent créer des profils imitant ceux de personnes réelles pour tromper leurs contacts.

3. Phishing ciblé : Les informations partagées sur les réseaux sociaux permettent aux cybercriminels de personnaliser leurs attaques.
4. Exploitation des photos : Les images publiées peuvent être utilisées pour l'usurpation par reconnaissance faciale.
5. Manipulation sociale : Les escrocs peuvent exploiter les relations en ligne pour gagner la confiance des victimes.

Pour se protéger, il est crucial de limiter les informations partagées publiquement, d'utiliser des paramètres de confidentialité stricts et de rester vigilant face aux demandes suspectes ou aux interactions inhabituelles sur les réseaux sociaux.
Il est possible de limiter un peu le traçage que Facebook effectue sur vos visites de sites internet tiers par l'utilisation d'une extension de navigateur comme Facebook container pour Firefox ou brave.

Protection des données personnelles, limitation des traces numériques

Pour réduire le partage de données personnelles en ligne, voici quelques techniques efficaces :

1. Limiter les informations partagées sur les réseaux sociaux.
2. Utiliser des paramètres de confidentialité stricts sur les plateformes en ligne.
3. Se désabonner des newsletters inutiles et supprimer les e-mails contenant des informations personnelles.
4. Chaque fois que c'est possible ou utile, utiliser des mails jetables ou des boîtes mail poubelle.

5. Privilégier les clés USB ou disques durs externes plutôt que le stockage cloud pour les données sensibles (sans oublier les backups !).
6. Télécharger uniquement les applications nécessaires et vérifier leurs autorisations d'accès.
7. Privilégier l'open source !

Concernant l'utilisation de VPN et de navigateurs privés : Les VPN (Virtuel Private Networks) permettent de chiffrer les données échangées en ligne et de masquer l'adresse IP de l'utilisateur, offrant ainsi une meilleure protection de la vie privée.

Les navigateurs privés, quant à eux, ne conservent pas l'historique de navigation, les cookies ou les données de formulaires après la fermeture de la session. Bien que ces outils améliorent la confidentialité en ligne, il est important de noter qu'ils peuvent avoir un impact sur l'empreinte numérique : Les VPN peuvent ralentir la connexion internet (goulet d'étranglement). L'utilisation de navigateurs privés peut nécessiter plus de ressources système, car ils ne conservent pas les données en cache. Il y a

suffisamment de VPN gratuits et open source pour ne pas payer cher et méchant ! Non, ni Nord VPN ni les autres ne sont pas la panacée !!! On laissera toujours des traces !

- Privilégier les extensions de navigateur et les navigateurs qui bloquent les publicités, cookies et traceurs (brave, Firefox, opéra…) un programme de mail permettant de voir directement l'adresse vraie de l'expéditeur du message est un plus pour visualiser les adresses fantaisie qui vous indiqueront un problème (Thunderbird).
- Windows est l'operating system préféré des pirates, tant de portes ouvertes ou mal fermées, vulnérabilités en tout genre non patchées par la paresse ou la non-connaissance de l'utilisateur… c'est le plus répandu, installé par défaut sur les PC il est donc le plus intéressant pour ratisser large ! Encore une fois privilégiez libre et open source !

Savoir si une de vos adresses mail est compromise et susceptible d'être spammée https://haveibeenpwned.com/, bitwarden.com…

Les Cookies

Ces délicieux petits gâteaux peuvent avoir un goût amer pour l'utilisateur : on a vu plus haut (billets d'avion) que ceux cis servent à savoir si vous avez visité un site et éventuellement quelle page de celui-ci… mais les cookies tiers peut aussi informer d'autres sites qui n'ont rien à voir et que vous n'avez pas visités de vos intérêts, pour en faire quoi ? Allez savoir, mais pas pour votre bien à vous, c'est sur ! Si c'était si innocent, pourquoi vous les impose-t-on avec tant de force malgré la loi ?

Le nettoyage des cookies à l'arrêt du navigateur est une bonne option. Il n'y a pas de cookie strictement nécessaire c'est un abus fréquent !

La mise en place d'un « cookie wall » — est une pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à l'installation de cookies « non strictement nécessaires » — n'est pas conforme au RGPD.
Cette pratique empêche, en effet, de recueillir votre consentement libre, puisque vous êtes obligé de consentir à l'installation et/ou à la lecture de cookies pour pouvoir accéder au site web ou à l'application mobile.

Utilisation de mails jetables

Les adresses e-mail temporaires, également appelées jetables ou éphémères, sont des adresses créées pour un usage unique ou à court terme. Elles offrent plusieurs avantages :

1. Protection contre le spam : Elles évitent que votre adresse principale ne soit inondée de courriers indésirables.
2. Confidentialité accrue : Elles limitent l'exposition de vos données personnelles en ligne.

3. Contournement des restrictions : Elles permettent de créer plusieurs comptes sans limites d'adresse IP : couplées à un germinateur de N° de carte visa permettra de prolonger indéfiniment des essais gratuits…
4. Sécurité renforcée : Étant temporaires, elles réduisent les risques de piratage.

Comment créer et utiliser des mails jetables

1. Choisissez un service d'e-mail temporaire comme Temp Mail, yopmail, 10 minutes mail.
2. Générez une adresse aléatoire ou sélectionnez-en une.
3. Utilisez cette adresse pour vous inscrire ou recevoir des messages.
4. Consultez les e-mails reçus directement sur la plateforme.
5. L'adresse s'autodétruira après un certain temps ou manuellement.

Situations recommandées pour l'utilisation

1. Inscriptions à des services en ligne pour des essais gratuits.
2. Participation à des forums ou téléchargements nécessitant une inscription.
3. Tests d'applications ou de sites web en développement.
4. Création de comptes secondaires pour certains services.
5. Protection lors d'achats en ligne ou d'inscriptions à des programmes de fidélité.

Il est important de choisir un service fiable, gratuit, sans processus d'inscription complexe et respectueux de la vie privée.

L'utilisation d'adresses e-mail temporaires permet de garder le contrôle sur sa présence en ligne tout en profitant des services numériques. Il est important d'avoir des mots de passe forts et uniques, l'utilisation des gestionnaires de mots de passe, une authentification à deux facteurs et de penser aux mises à jour et sauvegardes.

Sécurité des réseaux Wi-Fi

Les réseaux Wi-Fi publics présentent plusieurs risques pour la sécurité de vos données :

1. Interception des données : Un attaquant peut facilement intercepter le trafic non chiffré sur un réseau public.
2. Attaques de l'homme du milieu (man in the middle) : Un pirate peut se positionner entre vous et le point d'accès pour intercepter vos communications (point d'accès dupliqué).
3. Réseaux malveillants : Des réseaux Wi-Fi malveillants peuvent être créés pour attirer les utilisateurs et voler leurs informations.
4. Propagation de logiciels malveillants : Les réseaux publics non sécurisés faciliteraient la propagation de virus et malwares.

SCRIBD

Accaparateurs de contenu :

Certains sites web accaparent du contenu gratuit, entre autres des publications universitaires, pour les rendre payants. Ce phénomène est particulièrement problématique dans le domaine de la recherche académique.

- Accès restreint à la connaissance : Les publications scientifiques, souvent financées par des fonds publics, se retrouvent derrière des paywalls, limitant leur accessibilité.
- Ils tirent profit de la recherche sans en supporter les coûts de production.
- Impact sur la diffusion du savoir : Cette pratique freine la circulation des connaissances et peut ralentir le progrès scientifique.
- De plus en plus de chercheurs et d'institutions militent pour un accès libre aux publications scientifiques.

Plateformes alternatives :

Des initiatives comme les archives ouvertes et les revues en libre accès émergent pour contrer ce phénomène d'accaparement de contenu qui doit être gratuit.

Des solutions partielles existent pour passer derrière un paywall ou retrouver d'anciennes publications disparues (sci-hub, wayback machine, 13ft ladder, scholar.google…).
Pour trouver des pages non référencées d'un site spécifique sur Google, vous pouvez utiliser la syntaxe suivante dans la barre de recherche Google : site : *nomdedomaine.com*.

Cette commande affichera toutes les pages indexées par Google pour le domaine spécifié.
Si certaines pages importantes de votre site n'apparaissent pas dans les résultats, cela peut indiquer qu'elles ne sont pas indexées.
Pour vérifier si une page spécifique est indexée, vous pouvez utiliser la même commande en ajoutant l'URL complète de la page : Site : nomdedomaine.com/page-spécifique un lien en annexe vous montre la syntaxe des commandes du moteur de recherche Google. Utilisez aussi https://scribd.vpdfs.com/ qui bypasse le paywall.

De nombreuses universités et organismes de financement exigent désormais que les recherches qu'ils soutiennent soient publiées en libre accès.
Cette situation soulève des questions importantes sur l'accès démocratique à l'information.

Copyright et patent troll

L'attaque d'un copyright troll sur le site du club est à l'origine de cette présentation, à la suggestion de Morgan ON4MOD :
Un copyright troll est une entreprise qui exploite les droits d'auteur uniquement à des fins lucratives, en utilisant des menaces de poursuites judiciaires pour obtenir des compensations financières, sans véritable intention de protéger la création originale. Son objectif principal est de générer des revenus par le biais de réclamations juridiques.

La Méthode est de recherche systématique de violations des droits d'auteur, souvent à l'aide de technologies algorithmiques.
Et la cible, principalement les utilisations non autorisées de contenus en ligne, notamment des photographies.

Ces entités se distinguent des organismes légitimes de protection des droits d'auteur par leur motivation purement financière, qui dénature l'esprit initial de la protection des créateurs.
Ces sociétés utilisent des méthodes qui flirtent avec la limite de la légalité et collaborent avec des huissiers (eos-contentia, eos-ksi). Depuis que les victimes ont réalisé que verser un paiement en Suisse (hors Europe) était manifestement une solution douteuse, elles ont pris conscience de cette réalité.

La violation du droit d'auteur est une chose réelle, MAIS Picrights (et d'autres) ne poursuit pas de véritables réclamations en matière de droit d'auteur. Picrights est une entreprise frauduleuse dont le modèle commercial contraire à l'éthique consiste à harceler et à contrarier les petits blogueurs jusqu'à ce qu'ils paient des frais exorbitants pour une utilisation abusive généralement involontaire de photos génériques.

Picrights menace les particuliers et les petites entreprises de poursuites judiciaires extrêmes concernant des images génériques qui ont souvent été correctement obtenues, mais même si elles ne l'étaient pas, la licence et l'utilisation ne coûteraient qu'entre 10 et 50 dollars.

Pour poursuivre correctement une violation du droit d'auteur, un agent tiers doit établir que - L'image en question a fait l'objet d'un droit d'auteur (y compris la date et par qui) et cela - l'agent est habilité à négocier une réclamation au nom du titulaire du droit d'auteur. Sans ces deux éléments dans la communication, la réclamation n'a aucune validité juridique.

Picrights n'inclut jamais d'informations réelles sur les droits d'auteur, car il n'y en a pas. Les images qu'ils recherchent sont des photos d'archives (pas des événements cinématographiques Hindenburg/Zapruder une fois dans une vie) comme un gros plan d'une pièce d'euro. Aucun photographe ou entreprise ne protège ces photos générales/génériques, car le coût est prohibitif.

Cela ne signifie pas que les blogueurs et les entreprises doivent utiliser l'image de leur choix, quand ils le souhaitent. Ils ne devraient pas être payés pour leur travail.
Cependant, Picrights est une société dont les tactiques commerciales sont contraires à l'éthique et peut-être illégales. Picright est dans un petit bureau en suisse au-dessus d'une pizzeria minable !
L'extension Tineye permet de faire une recherche d'image sur le net, en déterminer la première occurrence ou de repérer des photos usurpées sur de faux profils.

Pollution publicitaire et influenceurs

La publicité sur internet en général est une plaie ! de moins en moins rentable, elle tente de nous matraquer de plus en plus… l'avenir est aux influenceurs qui aux yeux de certains seraient des modèles sympathiques à suivre ! Les plus jeunes sont à peine conscients des sommes qu'ils touchent pour simplement parler d'un produit. Quand ceux cis ne vous proposent pas de vous escroquer financièrement par des « investissement » ou des pyramides de Ponzi.
Souvent réfugiés à Dubaï pour des raisons fiscales, ils échappent à toute réglementation contrairement aux annonceurs en Europe, ils pratiquent aussi le dropshipping.

Le dropshipping est une méthode où des produits sont achetés à bas prix sur des sites comme AliExpress et revendus à un prix élevé. Les influenceurs, notamment ceux de la téléréalité, utilisent leur notoriété pour promouvoir ces produits, ce qui peut poser des problèmes.

- Qualité médiocre : Produits souvent de mauvaises qualités.
- Absence de garantie : Peu ou pas de service après-vente.
- Informations trompeuses : Caractéristiques du produit souvent exagérées.
- Comparez les prix sur des sites comme AliExpress.
- Vérifiez les avis et la réputation du vendeur.
- Soyez vigilant face aux offres trop alléchantes.

Les influenceurs doivent indiquer clairement le contenu sponsorisé. En cas de problème, contactez le vendeur, car l'influenceur n'est pas le vendeur direct. Restez vigilant et faites vos recherches avant d'acheter en ligne !
Nous avons un certain nombre de possibilités pour échapper à la pollution publicitaire, comme des extensions de navigateur qui les font disparaître et qui peuvent aussi brouiller les cartes des traqueurs.

Cela vous évitera de payer pour un YouTube premium, accélérera le chargement d'une page en empêchant les pubs de vous envahir ou d'exécuter du code plus ou moins malveillant pour vous identifier (ad nauseam, ublock origin…) Une procédure particulière existe pour installer ad nauseam sur des navigateurs à base chrome ou IE, ni google ni Windows n'aiment cette extension qui leur ferait perdre de l'argent !
Pas de solution ultime qui tuera tout malheureusement, mais une bonne réduction en perspective quand même. Firefox supporte ces extensions sans problème en natif. Il existe malheureusement des bloqueurs de pub qui laissent passer les annonceurs qui les ont payés !!!

Bitcoin, Shitcoin, pyramides de Ponzi

Bitcoin ou Ethereum ne sont pas forcément des choses nuisibles, j'en ai moi-même profité.
Par contre l'instabilité inhérente au système peut vous faire perdre la majeure partie de votre mise de fonds… ça apparaît grimpe puis s'évapore subitement… le minage demandant de plus en plus de ressources devient de plus en plus l'apanage de fermes de plus en plus énormes, loin est le temps minage avec la carte vidéo du pc de la maison : il y a eu des chevaux de Troie qui faisaient miner votre pc à votre insu au bénéfice d'autres, régulièrement le halving diminue la rémunération pour avoir miné du bitcoin. Le halving participe aux variations extrêmement brutales du cours. Les possesseurs de Bitcoin et particulièrement de shitcoins qui ne suivent pas le cours à la minute sont bien sûr les dindons de la farce.
Récemment un teenager a créé et mis en ligne un shitcoin, le cours s'est envolé en quelques minutes, il a revendu la totalité moins de 1 h après (carpet pulling) provoquant l'effondrement… bénéfice pour le gamin 50 000 $ (Wired dec24)
Les pyramides de Ponzi (une variante, le jeu de l'avion, qui s'est pratiquée en réunion genre tupperware chez des particuliers avant l'ère internet).

Le principe sont de payer des dividendes élevés et rapides aux sortants avec l'argent des nouveaux arrivants.
Les sortants qui ont gagné de l'argent facilement trouvent opportun de repartir pour un tour…

Cela provoque une croissance exponentielle de la quantité d'investisseurs jusqu'à la saturation qui provoque l'effondrement de la pyramide et fait perdre leur mise de fonds aux derniers entrés.

Si vous voulez jouer, faites-le avec de l'argent que vous ne regretterez pas d'avoir perdu !

Conclusion

Les principales choses à retenir, je n'ai évidemment pas pu vous exposer la totalité des techniques utilisées ni les nouvelles qui sont encore à inventer, sont :

- Pas de panique, on se pose et on réfléchit.
- Si on vous pousse à agir vite, c'est pour vous empêcher de réfléchir et de vous informer !
- Encore maintenant, en étant attentif on repérera des choses étranges (adresse de retour, orthographe, différence avec le vrai site…)
- Ça ne durera pas éternellement, les escrocs aussi utiliseront l'AI !
- Quand c'est trop beau ou catastrophique pour être vrai, ça ne l'est jamais !
- On ne clique JAMAIS un lien qui est dans un mail, il risque de vous amener où vous ne voulez pas et vous faire des choses que vous ne voulez pas non plus.
- Si vous devez contacter votre banque, fournisseur, effectuer un virement, etc. n'utilisez jamais les liens ou N° qui figurent dans un mail.

- Utilisez plutôt un moyen sûr qui n'est pas lié au mail reçu.
- Idem pour des sites qui peuvent être des copies frauduleuses.
- Si vous avez été victime d'escroquerie, consultez https://economie.fgov.be/fr/signaler-une-infraction il vous indiquera la marche à suivre, comment déposer plainte systématiquement.
- Transférer les mails douteux à l'adresse suspect@safeonweb.be.
- pour alimenter la base de données qui permettra de poursuivre les escrocs.

*Définitions

Phishing : 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.
SMiShing : Le smishing est une attaque de cybersécurité par phishing menée par le biais de la messagerie texte mobile, également connue sous le nom de phishing par SMS. Il s'agit d'une variante du phishing, qui consiste à tromper les victimes en les poussant à communiquer des informations confidentielles à un pirate déguisé.
Script-kiddies : ou lamer est un terme péjoratif d'origine anglaise désignant les néophytes qui, dépourvus des principales compétences en sécurité informatique, essaient d'infiltrer des systèmes en se servant de programmes efficaces — souvent des scripts —, simples d'utilisation, mais qu'ils ne comprennent pas.
Scammer : escroc, arnaqueur.
Social engineering : L'ingénierie sociale est *une technique de manipulation qui exploite l'erreur humaine* dans le but d'obtenir des informations confidentielles.
Cheval de Troie ou Trojan horse en anglais est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur. *(Wikipédia)*
Gamethief : ce type de programme malveillant est conçu pour voler les informations de compte d'utilisateur pour les jeux en ligne.
Cambridge Analytica LTD (ou « CA ») est une société britannique de « Conseil en gestion autre que la gestion financière » combinant des outils d'exploration et d'analyse des données. *(Wikipédia)*
The Pirate Bay est un site web créé en 2003 en Suède, indexant des liens Magnets de fichiers numériques, permettant le partage de fichiers en pair à pair (de manière mutualisée) à l'aide du protocole de communication BitTorrent.
Le pair-à-pair, peer-to-peer ou P2P (les trois termes désignent la même chose), définit un modèle de réseau informatique d'égal à égal entre ordinateurs, qui distribuent et reçoivent des données ou des fichiers.
Cookie wall : L'expression « mur de traceur » désigne le fait de conditionner l'accès à un service à l'acceptation, par l'internaute, du dépôt de certains traceurs sur son terminal (ordinateur, smartphone, etc.).
Un patent troll (en français « troll des brevets », ou plus rarement « chasseur de brevets ») est, dans le domaine de la propriété intellectuelle et plus précisément dans

celui de la concession de licences (licensing), une société ou une personne physique qui utilise la concession de licence et le litige de brevets comme principale activité économique.
Drop shipping, ou dropshipping (en français « expédition directe », « livraison directe » selon le contexte) est un système tripartite, où le vendeur accepte la commande du client sans avoir le moindre stock du produit vendu. Il transfère alors les commandes et les détails d'expédition soit au fabricant, soit à un grossiste, soit encore à un autre détaillant, voire à une société de traitement des commandes, qui expédie ensuite les marchandises directement au client.
Halving du bitcoin (parfois appelé « halvening ») consiste à diviser la prime de minage de nouveaux blocs en deux, ce qui signifie que les mineurs reçoivent 50 % de bitcoins en moins pour vérifier les transactions.
Shitcoins : Si vous parlez un petit peu anglais, vous avez déjà saisi le sens de ce néologisme. En effet, ce mot-valise se compose des mots « shit », qui signifient littéralement « merde », et « coin ». En somme, on peut le traduire par « pièce de monnaie de merde ».
Carpet pulling : pour une équipe de développement, abandonner un projet soudainement en prenant tout l'argent de ses fonds de liquidité, sans rien laisser aux investisseurs.
Pyramides de Ponzi : est un montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants.

Tous les liens utiles

Vous trouverez ici une série de liens utiles en rapport avec les sujets évoqués.

https://on5vl.org/securite-numerique/

https://www.mozilla.org/fr/firefox/new

https://www.mozilla.org/fr/firefox/facebookcontainer

https://adnauseam.io

https://haveibeenpwned.com/tps://vienumeriqueprivee.fr/ad-nauseam-ou-comment-combattre-les-algorithmes-publicitaires

https://ublockorigin.com/fr

https://haveibeenpwned.com

https://tineye.com

https://temp-mail.org/fr

https://yopmail.com/fr

https://internxt.com/fr/temporary-email

https://10minemail.com/fr

https://adguard.com/fr/adguard-temp-mail/overview.html

https://www.cookieyes.com/fr/analyseur-de-cookies

https://www.vccgenerator.org

https://dnschecker.org/credit-card-generator.php

https://www.akto.io/tools/credit-card-generator

https://neapay.com/online-tools/credit-card-number-generator-validator.html

https://ccardgenerator.com

https://www.cookieyes.com/fr/analyseur-de-cookies

https://tempsmss.com/country/belgium-temporary-phone-number

https://quackr.io/temporary-numbers

https://temp-number.com

https://receive-smss.com

https://quackr.io/ (payant mais imparable)

https://play.google.com/store/apps/details?id=com.alabididev.tempnumbersms&hl=fr (smartphone)

https://fr.mytempsms.com

https://temporary-phone-number.com

https://www.jubel.be/fr/le-phishing-le-nouveau-cambriolage-en-2021

https://alternativeto.net/software/13-fe

https://alternativeto.net/software/smry/about/et-ladder/about

https://alternativeto.net/software/bypass-paywalls/about

http://web.archive.org/

https://chromewebstore.google.com/detail/wayback-machine/fpnmgdkabkmnadcjpehmlllkndpkmiak?pli=1

https://sci-hub.se

https://scholar.google.com

https://www.student.be/fr/student-life/ou-trouver-des-articles-scientifiques-pour-un-travail-academique

https://cursus.edu/fr/12714/7-solutions-innovantes-facilitant-lacces-libre-et-gratuit-aux-savoirs-scientifiques-payants

https://www.ionos.fr/digitalguide/serveur/configuration/changer-de-serveur-dns-sur-windows-11

https://support.google.com/android/answer/9654714?hl=fr

https://www.liligo.fr/magazine-voyage/billets-davion-lastuce-pour-ne-plus-se-faire-pigeonner-par-les-variations-de-prix-13811.html

https://www.noiise.com/ressources/seo/recherche-avancee-google-astuces-conseils

https://www.unite.ai/fr/best-open-source-intelligence-osint-tools

https://www.portail-ie.fr/univers/droit-et-intelligence-juridique/2024/copyright-trolling-strategies-limites-juridiques-et-appel-a-lethique

https://rorypecktrust.org/fr/how-we-help/freelance-resources/digital-security/social-media-trolling-and-doxxinghttp://Copyright trolling : stratégies, limites juridiques et appel à l'éthique

https://avocat-chamfeuil.fr/actualites/copyright-troll

https://isern.com/fr/les-trolls-des-brevets-ce-quils-sont-et-comment-les-combattre

https://www.intotheminds.com/blog/picrights-afp

https://www.bfmtv.com/tech/actualites/reseaux-sociaux/arnaques-produits-dangereux-la-liste-des-14-influenceurs-epingles-par-la-dgccrf-au-cours-de-l-ete_AV-202309040561.html

https://www.stormshield.com/fr/actus/petite-histoire-du-phishing

https://www.wikiwand.com/fr/articles/Escroquerie

https://fr.scamdoc.com

https://economie.fgov.be/fr/signaler-une-infraction

suspect@safeonweb,be

https://www.blick.ch/fr/opinion/nicolas-capt-petite-histoire-des-arnaques-a-lheure-o-le-phishing-nexistait-pas-id17815248.html

https://www.dnsbelgium.be/fr/naviguer-sagement/phishing

A propos de l'auteur

Jean-François Mussen

Depuis mon plus jeune âge, je suis animé par une passion profonde pour l'électronique, l'aviation et la plongée. À 14 ans, j'ai conçu mon premier émetteur, posant ainsi les bases d'un parcours riche en expériences techniques. Durant mes études en électronique, je passais mes fins d'après-midi dans l'atelier de Servais Penay, perfectionnant mes compétences. Un emploi d'été chez ICEM à Liège m'a permis, en 1979, de constituer mon propre laboratoire. J'ai obtenu ma licence ON1 en 1981.

Après une période d'inactivité depuis le milieu des années 90, où je travaillais sur l'instrumentation de bancs d'essai moteur chez Safran, j'ai renoué avec la radio grâce à l'acquisition d'un analyseur HP E4411b. Cet appareil a ravivé ma passion et m'a poussé à reprendre contact avec mes amis radioamateurs. L'électronique radio a toujours fait partie de moi, et j'ai même réalisé quelques projets commerciaux dans ce domaine. Toutefois, je reste peu actif sur les ondes, privilégiant la technique au trafic.