Sécurité numérique

Réseau Volontaires Solidaris - Depaz Jean-Marc - version 1.1

Table des matières

Introduction

Notre société se construit de plus en plus autour d'ordinateurs et d'intelligences artificielles. Aujourd'hui, nous effectuons nos paiements en ligne ou sans contact. Nous pouvons consulter nos données médicales sur internet. Les réseaux sociaux nous donnent accès à tous nos contacts et à nos conversations privées. Etc. Il faut donc bien connaître les systèmes et être attentif pour ne pas faire de bêtises.

C'est la raison pour laquelle il est important de se tenir informé des nouvelles technologies lorsqu'on suit les actualités quotidiennes. Il est aussi primordial d'avoir une attitude proactive concernant leurs nouvelles implications. Les médias traditionnels ne s'y intéressent pas assez. Cela ne concerne plus seulement les geeks qui boivent des sodas, mangent des chips et qui sont pleins de boutons. Oubliez les stéréotypes. La technologie concerne désormais tout le monde.

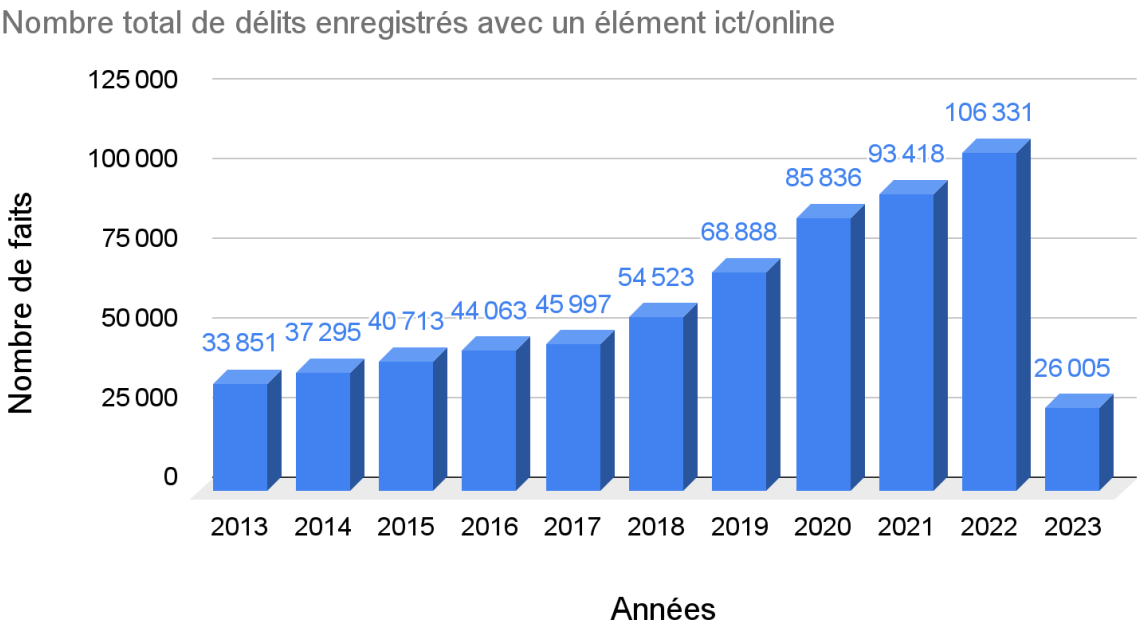
Parlez-en également autour de vous, avec votre famille, vos amis, les communautés dont vous faites partie, lors d'activités que vous partagez en groupe,...

Cet ouvrage a trois objectifs principaux. Premièrement, il vous sensibilise à l'importance de bien vous protéger. Deuxièmement, il vous informe sur les différentes menaces actuelles. Troisièmement, il vous montre comment vous protéger et protéger vos appareils.

Afin de suivre avec aisance les différents conseils mentionnés, il est recommandé d'avoir un niveau de base et d'utiliser régulièrement un ordinateur, une tablette ou un smartphone. Par niveau de base, j'entends ceci : savoir ce qu'est un téléchargement, une pièce jointe, un mail, une application, un lien de site web, un compte en ligne,...

Chaque thème abordé peut être approfondi. Si un sujet vous intéresse ou vous concerne, n'hésitez pas à prendre note sur le côté pour effectuer vos propres recherches par la suite.

Pourquoi s’intéresser à la sécurité numérique ?



Voici le graphique du rapport de police concernant l’ict (technologies de l’information et de la communication) disponible sur le site officiel de la police belge. Cette version s’arrête à la fin du premier trimestre 2023.

Il présente le nombre total de délits enregistrés par les forces de l’ordre avec un élément ict ou en ligne (notamment par internet). Le nombre réel est plus élevé car tout le monde ne signale pas toujours les faits à la police.

Depuis 2013, les chiffres augmentent. On peut l’expliquer, entre autres, par le fait que nous soyons de plus en plus connectés.

À partir de 2019, on observe une croissance exponentielle due au confinement, le nombre de communications par internet ayant explosé.

Acteurs numériques hors la loi : profils et motivations

On retrouve plein de profils différents. Voici une liste non exhaustive :

- Des groupes s'organisant sur le dark web pour vendre toutes sortes de biens : des données d'identité, des données bancaires, de la drogue, des armes, de faux billets,... Leur motivation est principalement l'argent. Ils se font payer à l'aide de cryptomonnaies. Ce sont des monnaies non gérées par l'État. Ils communiquent à l'aide d'outils cryptés pour rester anonymes. La pauvreté est l'une des raisons qui peut pousser les gens à franchir le pas. D'autres personnes moins scrupuleuses veulent simplement s'acheter un téléphone dernier cri.

- Des entreprises aux méthodes commerciales douteuses. Elles peuvent tenter de vous forcer un peu la main, par des pressions psychologiques ou en se basant sur la relation qu'elles ont établie avec vous.

- Des groupes extrémistes ou non recrutant sur les réseaux sociaux ou faisant de la propagande idéologique pour manipuler les élections, les opinions.

- Des individus isolés (un ex-petit ami, un gendre ou une belle-fille malveillants, un pervers narcissique,...) cherchant à se venger, harceler sur les réseaux sociaux, nuire à la réputation de quelqu'un,...

- Des individus aimant les défis et cherchant de la reconnaissance pour la réussite de leur attaque / arnaque. Passer par la case prison peut être un plus dans le milieu de la cybersécurité.

- Des pédophiles voulant obtenir un rendez-vous avec vos enfants ou petits-enfants. Ils entrent en contact avec ceux-ci via des sites de rencontres dédiés aux plus jeunes ou, plus classiquement, via les réseaux sociaux.

  Les grosses plateformes mettent en place des moyens pour modérer leurs interactions. Mais, créer un site de rencontres n'est pas coûteux et pas illégal. Tout le monde peut le faire. Si certaines pratiques peuvent être surveillées sur de gros sites, alors d'autres plateformes, avec moins de moyens, seront exploitées.

  De plus, la loi n'impose pas encore de s'identifier avec une carte d'identité pour s'enregistrer sur un site. Et du point de vue légal et technique, il est très compliqué d'imposer des contrôles, mais des discussions sont en cours.

  C'est pourquoi il est très important de bien encadrer l'utilisation d'internet des plus jeunes, notamment en les informant. Pour ce faire, vous pouvez vous rendre sur le site de Child Focus. Il fournit plein de conseils utiles. Par exemple, comment gérer le contact avec des inconnus ou comment parler du porno à vos enfants etc.

  Par ailleurs, il est possible d'installer un contrôle parental sur vos appareils par le biais d'une suite de sécurité (un antivirus).

Les conséquences d'une cyberattaque

Le malware

L'ordinateur peut être infecté par un malware. "Malware" est le terme général correct. Dans le langage commun, il est remplacé par le terme "virus".

Ces infections passent souvent inaperçues mais il est parfois possible de constater un ralentissement du système ou une altération de son fonctionnement comme :

- une fenêtre publicitaire qui apparaît,
- une nouvelle barre de favoris,
- une nouvelle page d'accueil sur votre navigateur internet,
- un nouveau programme qui se lance automatiquement,
- un plantage du système,
- …

Une infection destinée à espionner sera plus efficace si on ne se doute pas de sa présence. Elle pourra ainsi voler vos mots de passe, vos cookies ou votre historique de navigation sur internet etc.

Un ransomware, quant à lui, vous indiquera qu'il débloquera vos données si vous payez. Dans ce cas-ci, l'infection se déclare.

Pour remédier à une infection, vous pouvez lancer une analyse antivirus. Ça ne garantit pas que la menace sera trouvée et supprimée mais c'est un bon premier réflexe. Vous pouvez aussi réinitialiser votre système d'exploitation. Dans ce cas-ci, vos données et vos applications seront supprimées. Ce n'est pas une garantie totale, mais la plupart des menaces seront effacées.

La fuite de données

Elle peut être due :

- aux infections sur vos appareils,
- aux entreprises sur lesquelles vous avez un compte qui se font hacker. Ici, vous n'y êtes pour rien. Ce sont les machines de l'entreprise qui ont été attaquées.
- aux informations que vous donnez volontairement aux commerciaux que ce soit par téléphone, dans des galeries commerciales ou en utilisant des applications peu scrupuleuses ou mal sécurisées. Attention à ne pas donner trop souvent vos informations, à ne pas accepter trop souvent des politiques de confidentialité sans les lire. Idéalement, il faudrait les lire. Toutes les entreprises ne sont pas forcément bienveillantes ou très sécurisées. Vous pouvez éventuellement donner quelques informations aux entreprises / applications réputées qui vous intéressent.

  Lorsque votre adresse mail a tellement servi qu'elle se retrouve envahie par des spams et fait l'objet de tentatives de piratage, pensez à la désactiver en tant que méthode d'authentification. De cette façon, les escrocs ne sauraient plus utiliser votre adresse pour vous attaquer.

- …

La perte financière

Dans le cas d'une fraude à la carte bancaire principalement. Soyez sûrs d'être en contact avec le site web officiel ou l'application officielle d'une entreprise réputée avant de fournir vos coordonnées bancaires (ainsi que le code pin ou la réponse du lecteur de cartes).
L'une des méthodes les plus courantes pour vous soutirer ce genre d'informations s'appelle le hameçonnage. Concrètement, on vous fait croire toutes sortes de scénarios, qu'il faut mettre à jour vos coordonnées bancaires pour poursuivre votre abonnement à tel ou tel service, par exemple, que ce soit par SMS, par mail, voire même par téléphone ou d'autres moyens de communications. Ne fournissez jamais d'informations sensibles par ces canaux.

Comment faire la distinction entre un mail / SMS malveillant et un mail / SMS légitime ? Ne cliquez pas sur le lien fourni dans le mail / SMS, mais rendez-vous sur le site officiel via un moteur de recherche (comme Google) ou sur l'application officielle et vérifiez là-bas.

Le malaise psychologique

On se sent bête. On a honte. Ces méthodes ont été étudiées soigneusement pour fonctionner. Ça arrive donc à beaucoup de monde, même à ceux qui sont bien conscients des arnaques. Ne vous jugez pas trop sévèrement. Tirez-en les leçons dont vous avez besoin et essayez de tourner la page. Bien entendu, je parle uniquement de l'aspect psychologique. N'hésitez pas à entamer des démarches pour vous défendre et signaler ces arnaques.

Les vecteurs d'attaque

Les sites web malveillants

Que ce soit dans un moteur de recherche, un mail, un SMS, une conversation privée ou ailleurs, ne cliquez jamais sur les liens, les images, du texte ou tout autre élément susceptible de vous diriger vers un site web malveillant, surtout si vous hésitez. En effet, ces sites pourraient infecter votre ordinateur par un malware ou se faire passer pour des sites officiels dans le but de vous soutirer des informations confidentielles (identifiants de connexion, coordonnées bancaires,...).

Mais quels sont les sites web de confiance ? Je pense qu'on peut partir du principe que ceux des grandes entreprises réputées ne devraient pas être malveillants.

Pour vous assurer que vous accédez bien aux sites officiels, effectuez toujours une recherche via un moteur de recherche et mettez les sites en favoris ou téléchargez leur application officielle.

Pour vérifier l'adresse des sites auxquels vous accédez sur ordinateur, vous pouvez survoler (sans cliquer) l'élément de redirection avec votre souris. Vous voyez, ensuite, son adresse en bas à gauche de votre navigateur internet. Sur tablette et smartphone, vous pouvez parfois maintenir appuyé sur l'élément pour voir l'adresse mais une erreur de manipulation est plus vite arrivée. Idéalement, vérifiez donc via un ordinateur. Si l'adresse correspond exactement à l'adresse officielle, qu'il ne manque aucun caractère ou qu'il n'y en a pas en trop, c'est bon. Toutefois… sur les réseaux sociaux, il se peut que le lien d'une publicité commence en mentionnant le nom du réseau social mais vous dirige en dehors de celui-ci. Lisez bien toute la publication. Vous pourrez y voir "sponsorisé", "publicité", "annonce", "collaboration commerciale" ou quelque chose du genre s'il s'agit d'une publicité qui veut vous emmener sur son site. Néanmoins, si le produit vous intéresse, essayez de le trouver auprès d'une entreprise réputée.

Pour vous inciter à cliquer sur un site malveillant, les arnaqueurs peuvent choisir d'utiliser la technique du hameçonnage. Voici un exemple : "Votre abonnement Netflix va expirer dans 24 heures, cliquez ici pour mettre à jour vos coordonnées bancaires". L'urgence de la situation vous poussera à cliquer au lieu de réfléchir. Si vous cliquez sur le lien, vous verrez un site web ressemblant au site officiel, mais ce sera seulement pour vous tromper. Un autre exemple pourrait être une invitation à payer une amende, des frais de transport, etc ou à prendre connaissance d'un document dans lequel figure une plainte à votre encontre. Tout cela donne envie de cliquer pour aller voir. C'est fait exprès. Dans mon exemple, si vous souhaitez vérifier que votre abonnement est toujours actif, rendez-vous sur Netflix via un moteur de recherche (et mettez-le en favori) ou via l'application officielle.

Le fait qu'un site commence par https n'est pas un critère de sécurité si le propriétaire a de mauvaises intentions.

Aussi, consultez les paramètres de votre navigateur pour voir comment il peut vous protéger face aux menaces d'internet. Par exemple : que faire si un site web veut télécharger un

fichier sur votre appareil ? Faut-il ouvrir directement le fichier, simplement le télécharger ou vous demander de choisir au cas par cas ? Pour ma part, j'utilise l'option me permettant de choisir au cas par cas. Ainsi, je peux télécharger et ranger directement mon fichier à la bonne place ou je peux l'ouvrir directement. C'est dans les paramètres aussi que vous pouvez consulter vos cookies, gérer la prévention du suivi, personnaliser votre expérience,...

Lorsque vous avez un doute concernant les intentions d'un site, vous pouvez le vérifier via VirusTotal. Il s'agit d'un site pouvant analyser les intentions d'un fichier ou d'une URL. Cependant, ce n'est pas une garantie totale. Aussi, les sites de hameçonnage ne seront pas nécessairement détectés comme malveillants. C'est, en effet, le propriétaire qui est malveillant et non le code.

Dans la catégorie des liens, on retrouve aussi les QR codes malveillants. On pourrait notamment coller un QR code par dessus un autre pour détourner un paiement, vous renvoyer vers un mauvais site web ou vous faire télécharger un virus. Exemple : une fausse contravention qui vous invite à payer via un QR code. En réalité, les pirates vont récupérer vos informations bancaires et votre paiement.

Les téléchargements

Téléchargez uniquement des applications provenant d'entreprises fiables, soit à partir de leur site officiel, soit à partir de magasins officiels (Play Store, Apple Store, Microsoft Store, Galaxy Store,...). Comment savoir lesquelles sont fiables ? On ne peut jamais être complètement sûr mais vous pourrez vous faire une opinion en consultant différents avis sur internet.

Si vous téléchargez les applications à partir des stores, vérifiez deux fois qu'il s'agit bien de votre application et de la bonne entreprise. Ces informations sont souvent l'une à côté de l'autre. Pourquoi cette vérification ? Parce que certaines applications ressemblent à celles que vous voulez télécharger mais proviennent d'autres entités.

C'est la même chose pour les pièces jointes provenant de vos messages (SMS, mails, conversations privées,...). Soyez sûrs qu'elles proviennent bien d'expéditeurs de confiance, et même dans ce cas, il vaut mieux être au courant que l'on va recevoir quelque chose avant de le recevoir. Aussi, désactivez bien le téléchargement automatique des pièces jointes dans vos applications.

La vente en ligne

Attention aux arnaques sur les plateformes de vente en ligne.
Quelques exemples :

- L'arnaque à la location. Louer un appartement qui n'existe pas.
- L'arnaque aux voyages organisés. Les organisateurs partent à l'étranger quand ils sont payés avant que le voyage ait lieu.
- Vous voulez acheter une nouvelle table ? Est-ce une table que vous achetez ou seulement sa photo ?

Pour éviter ce type d'arnaque, n'achetez, ne louez ou ne réservez que par le biais

d'entreprises réputées et à des vendeurs réputés. Certains sites permettent aux consommateurs d'attribuer une note aux vendeurs en fonction de leur expérience.

Parlez-en aussi autour de vous, à votre famille, vos amis, lors de vos activités,... L'expérience d'un groupe / d'une communauté est souvent très enrichissante !

Vos comptes en ligne

Un compte en ligne peut être piraté facilement si la sécurité pour y accéder est trop faible. Suivant le compte, cela peut signifier :

- Accéder à vos messages privés,
- Modifier vos publications,
- Supprimer vos contacts,
- Publier du contenu inapproprié en votre nom,
- Accéder à vos informations sensibles (nom, prénom, numéro de téléphone, coordonnées bancaires, adresse,...) pour usurper votre identité ou pour les vendre.

Le mot de passe doit être difficilement trouvable par une personne ou par une machine :

- Écrivez au moins 12 caractères, dont 1 symbole, 1 minuscule, 1 majuscule et 1 chiffre.
- Évitez les mots disponibles dans le dictionnaire. Ils sont facilement devinables pour une machine.
- Évitez aussi d'y mentionner des données disponibles sur vos appareils ou en ligne, comme votre date de naissance.

Écrivez un mot de passe unique pour chaque compte. Comme ça, si un de vos mots de passe est volé, cela ne concerne qu'un compte.

De nombreux outils vous proposent de générer un mot de passe fort. Privilégiez des outils venant d'entreprises réputées pour éviter que votre mot de passe ne soit volé. Vous pouvez même demander à une intelligence artificielle générative (du style ChatGPT) de vous programmer un générateur de mots de passe. Ainsi, vous aurez votre propre outil. Attention à ne pas demander directement à une IA de vous générer un mot de passe, car les conversations peuvent être relues par d'autres personnes. Voici aussi une solution artisanale :
"Je joue au Lotto chaque fois que le jackpot dépasse 5 millions !" => "JjaLcfqljd5m!" Chaque première lettre des mots est une lettre du mot de passe. Attention à bien obtenir tous les types de caractères recommandés. Et ce pourrait être un bon mot de passe pour un compte à la Loterie Nationale. La phrase complète sans les espaces forme aussi un bon mot de passe.

Par ailleurs, vous pouvez utiliser un gestionnaire de mots de passe. Google en propose un gratuitement. Ce sont des applications qui stockent tous vos mots de passe en un seul endroit et qui verrouillent cet endroit par un mot de passe maître (à ne surtout pas perdre). Ces applications peuvent proposer d'autres fonctionnalités comme :

- surveiller le dark web pour savoir si vos informations ont fuité (mail, mots de passe,...),
- le partage de vos mots de passe à d'autres utilisateurs (comme par exemple pour

Netflix),
- la génération de mots de passe forts
- un avertissement si un de vos mots de passe est trop faible,
- un avertissement si vous avez deux mots de passe identiques,
- …

C'est peut-être une bonne idée si vous avez beaucoup de comptes. Si vous optez pour cette solution, soyez conscient que vous confiez la sécurité de vos données à un tiers.

Pour renforcer davantage votre sécurité, utilisez des solutions de double authentification. C'est-à-dire qu'en plus du mot de passe, il vous est demandé d'entrer un code supplémentaire sécurisé. La seule connaissance du mot de passe ne suffit plus à se connecter.

Concernant la sécurité de façon générale, sachez que rien n'est infaillible, mais qu'en combinant plusieurs couches de sécurité, vous pouvez réduire considérablement les risques de violation.

Ce qu'il ne faut surtout pas faire, c'est enregistrer vos mots de passe sur votre navigateur web. En effet, ils sont lisibles directement par un malware ou une personne qui aurait accès à votre ordinateur puisqu'ils ne sont pas (toujours) protégés par un mot de passe maître.

Il faudrait idéalement changer vos mots de passe après quelques mois afin de minimiser la possibilité qu'ils soient découverts.

Renseignez une adresse mail ou un numéro de téléphone de récupération dans les paramètres de votre compte dans le cas où vous perdriez votre mot de passe.

Si vous avez un doute concernant la sécurité de votre compte ou si vous êtes curieux, vérifiez les activités de connexion dans les paramètres également. Elles vous diront quels appareils sont connectés à votre compte, s'il y a eu des tentatives d'accès, etc. Tous les comptes n'ont pas cette fonctionnalité.

Pour terminer ce chapitre, j'aimerais aussi vous dire que l'authentification par les données biométriques (empreintes digitales, reconnaissance du visage essentiellement) peut se révéler plus conviviale mais en cas de piratage, il est très (trop ?) complexe d'en changer.

Vos données sur les réseaux sociaux

Vos données sur les réseaux sociaux peuvent être détournées. Vos photos, vos informations personnelles, les informations dans vos publications et vos interactions sont une véritable mine d'or pour les arnaqueurs.

Voici quelques exemples concrets d'utilisation :
- Deviner un mot de passe trop faible (une date de naissance, le nom d'un proche,...)
- Deviner la réponse à une question secrète. Parfois, pour récupérer un mot de passe, vous avez besoin de répondre à une question secrète à laquelle vous seul connaissez la réponse. C'est un procédé mis en place par certains sites à la création

du compte. Mais cette réponse n'est-elle pas écrite quelque part sur vos réseaux sociaux ? Quel était le nom de votre premier animal de compagnie ? Et votre date de naissance ? Est-elle accessible au public ?

- Prendre connaissance de votre départ en vacances pour préparer un cambriolage. Idem si vous partagez votre intérêt pour rejoindre un événement comme un concert ou autre.
- Créer un faux compte de vous avec vos photos et vos informations personnelles afin de soutirer de l'argent à vos contacts, de nuire à votre réputation, d'envoyer des messages de hameçonnage à vos contacts, de demander à vos contacts de vous rappeler des secrets vous concernant,…
- Vous harceler, vous menacer, se moquer de vous, propager des rumeurs à votre égard, vous insulter,... suite à vos commentaires ou publications sur les réseaux sociaux. Cela nuirait à votre santé / santé mentale, votre sécurité et votre estime de vous.
- Vous informer, à partir d'un faux compte, que vous venez de gagner le concours auquel vous venez de participer (puisque vous avez dû partager votre participation pour qu'elle soit prise en compte). Ainsi, pour récupérer votre lot, vous devez compléter un formulaire en ligne disponible en suivant un lien. Si vous ne remarquez pas qu'il s'agit d'un faux compte, vous risquez de vous faire hameçonner.
- Comprendre qui vous êtes, vos idées politiques et essayer de vous faire changer d'avis, ou plus simplement vous faire parvenir de fausses informations qui vous intéressent.
- Se faire passer pour vous pour obtenir une nouvelle carte SIM auprès de votre opérateur avec votre numéro de téléphone. Ça s'appelle "SIM swapping". Ainsi, les arnaqueurs récupèrent toutes les informations qui accèdent à votre numéro de téléphone (des codes de confirmation, vos prochains SMS,…). Si vous constatez que votre carte SIM ne capte plus le réseau, signalez-le immédiatement à votre opérateur. Notez : ne vous alarmez pas si vous êtes au fond d'une grotte et que vous n'avez plus de réseau. Pour en capter, il faut être dans une zone proche d'une antenne.
- Les photos anodines de vos enfants sur les réseaux sociaux peuvent se retrouver sur des sites pédopornographiques.

Bref, tout ce que vous direz ou ferez pourra être retenu contre vous, même illégalement (et ce, partout sur internet, pas uniquement sur les réseaux sociaux !). Sur les réseaux sociaux, vous pouvez, bien sûr, choisir quelle audience pourra lire votre prochaine publication ou vos informations personnelles (les amis, le public, vous uniquement). Vous pouvez aussi créer des listes spécifiques d'amis concernés. Mais tout ceci ne sera respecté qu'à condition qu'aucune brèche ne soit jamais exploitée.

Dans un contexte plus global, j'ajouterai même que tout objet connecté peut potentiellement recueillir et transmettre des informations à qui saura s'y prendre.

L'ingénierie sociale

En matière de cyberactivités malveillantes, l'ingénierie sociale est la mise en œuvre de stratégies liées à la technologie et à la psychologie destinées à altérer le comportement

d’une personne dans le but de la tromper.

À vrai dire, la plupart des attaques utilisent, à un moment ou un autre, une forme d’ingénierie sociale. Un peu de naïveté devant une personne sûre d’elle, une réponse urgente pour un compte supprimé dans 48h, 1 minute d’inattention parce qu’on est occupé ailleurs en même temps… Ces exemples pourraient aussi rejoindre les tentatives d’hameçonnage.

La liste des sous-catégories ne sera pas exhaustive, mais je souhaiterais vous montrer, entre autres, quelques exemples où la manipulation est une pièce maîtresse.

La communication par téléphone ou par message écrit

Vos arnaqueurs sont de beaux parleurs et inspirent confiance. Ils ne sont pas dans le stéréotype du hacker avec une capuche qui écrit des choses incompréhensibles sur son ordinateur dans le noir (et qui semble quelque peu antisocial, voire méchant).

Concernant les coups de fil, s’ils vous pressent et vous disent que c’est urgent, vous dites simplement que vous ne pouvez pas répondre à leur demande actuellement et que vous les rappellerez ultérieurement.

Si vous restez en ligne, ne communiquez jamais d’informations confidentielles (coordonnées bancaires, réponse du lecteur de carte, mots de passe, adresse mail,...). Même l’adresse mail ? Oui. Ne communiquez pas cette information si vous n’êtes pas certain de savoir qui est au bout du fil.

Si quelqu’un que vous connaissez vous demande de l’argent ou toute autre information confidentielle par message, contactez-le via un autre canal pour être sûr que c’est bien lui. En effet, il pourrait s’agir d’une personne mal intentionnée qui essaie d’usurper son identité. Exemple : “votre enfant” pourrait vous demander de l’argent dans l’urgence pour le dernier train. Admettons même que ce soit vrai. Dans ce cas-ci, votre enfant doit s’attendre à recevoir une demande de confirmation via un autre canal (par exemple en l’appelant directement). C’est donc très important de bien communiquer sur la sécurité en ligne avec vos enfants, je le répète.

Si quelqu’un que vous ne connaissez pas vous demande des informations confidentielles, ne les communiquez jamais. Si le message est écrit, ne répondez pas (et signalez-le).

Certaines applications de communication ont des fonctionnalités vous avertissant d’un éventuel appel / SMS indésirable. N’hésitez pas à aller faire un tour dans les paramètres de l’application téléphone ou messages pour voir ce qu’elles proposent.

Les numéros surtaxés et les services par SMS

Une autre catégorie de l’ingénierie sociale inclut les numéros surtaxés et les services par SMS. L’idée est simple. L’appel coûte cher. Il faut donc multiplier les communications ou les faire durer. L’un des automatismes qui favorise l’arnaque est notre volonté de rappeler le numéro. Voici des tableaux reprenant les différents numéros surtaxés / services par SMS :

Numéro de téléphone	Tarif maximal	Type de service
070 xxx xxx	max. € 0,30 par minute	Services généraux
0900 xx xxx	max. € 0,50 par minute	Services généraux
0901 xx xxx	max. € 0,50 par appel	Services généraux
0902 xx xxx	max. € 1,00 par minute	Services généraux
0903 xx xxx	max. € 1,50 par minute	Services généraux
0904 xx xxx	max. € 2,00 par minute	Services généraux
0905 xx xxx	max. € 2,00 par appel	Services pour les jeux, logos, sonneries, etc.
0906 xx xxx	max. € 1,00 par minute	Services érotiques (18+)
0907 xx xxx	max. € 2,00 par minute	Services érotiques (18+)
0909 xx xxx	max. € 31,00 par appel	Services généraux

Numéro SMS	Tarif maximal	Type de service
2xxx	max. € 1,00 par SMS	Services généraux
3xxx	max. € 4,00 par SMS	Services généraux
4xxx	max. € 31,00 par SMS	Services de paiement
5xxx	max. € 0,50 par SMS	Services pour les jeux, logos, sonneries, etc.
6xxx	max. € 2,00 par SMS	Services pour les jeux, logos, sonneries, etc.
7xxx	max. € 4,00 par SMS	Services érotiques (18+)
8xxx	gratuit	Services gratuits
9xxx	max. € 2,00 par SMS	Services d'abonnement pour les jeux, logos, sonneries, etc.

Attention aussi aux numéros n'ayant pas le préfixe de la Belgique (+32). Il s'agit de numéros étrangers qui pourraient potentiellement coûter cher.

Ici aussi, les applications des opérateurs peuvent vous aider à bloquer certains services / numéros.

Pour bloquer un service payant, envoyez "STOP" par SMS en majuscule et sans guillemet

au numéro de SMS du fournisseur de services ou au numéro de contact du fournisseur.

Autre conseil : vérifiez toujours le numéro avant de rappeler pour savoir s'il est surtaxé, surtout s'il ne sonne qu'une fois. Vous pouvez également faire une recherche inversée (à partir du numéro) afin de savoir qui vous appelle. Le site pour cette recherche est indiqué dans les ressources complémentaires ainsi que d'autres liens afin que vous puissiez approfondir les sujets qui vous intéressent.

Pourquoi ne peut-on pas tout simplement interdire ces méthodes ? Car tout le monde y trouve son compte sauf les victimes. L'entreprise qui propose le service, l'opérateur par qui passe la communication et l'entreprise qui loue ces numéros. Toutefois, certains services légitimes en dépendent aussi.
Par exemple :

- Les radios pour répondre à un sondage, participer à un concours, faire un don,
- Les services informatiques qui souhaitent dissuader leurs utilisateurs de les appeler trop souvent pour des problèmes qu'ils peuvent régler eux-mêmes,
- Les services d'astrologies,
- ...

Certaines des sociétés qui proposent la location de ces numéros imposent des vérifications aux entreprises intéressées mais d'autres s'en foutent.

Les services sont légalement tenus de communiquer leurs tarifs. Exemple : 1€ par SMS envoyé ou reçu.

<u>L'arnaque aux sentiments</u>

Vous rencontrez quelqu'un en ligne qui prétend vous aimer. Il travaille la conversation. Quand il pense que vous êtes prêt, il vous demande de l'argent pour effectuer le trajet pour venir vous voir. Il peut aussi raconter être coincé à l'aéroport et avoir un besoin urgent d'argent.

<u>Les influenceurs</u>

Un influenceur est toute entité capable d'altérer le comportement d'une autre entité via un échange d'information. Dans le cadre de ce cours, nous nous intéresserons particulièrement aux influenceurs des réseaux sociaux. Ce sont des gens qui partagent leurs expériences, leurs hobbies et leurs passions avec une communauté de personnes, appelées "followers", qui les suivent et s'intéressent à leur contenu. Ensemble, ils constituent un espace d'échanges enrichissants, favorisant un partage d'idées et de connaissances, qui s'avèrent bénéfiques et instructifs pour tous les membres.

Cependant, certaines dérives peuvent parfois survenir. Voici deux exemples :

- Certains influenceurs outrepassent les bonnes pratiques commerciales, avec ou sans mauvaises intentions particulières, en faisant des promotions non approuvées par la loi (ne pas citer qu'il s'agit d'une publicité, vanter les mérites de la chirurgie esthétique,...).
- Ils pourraient également vous inciter à dépenser de l'argent lors d'événements particuliers en mettant l'accent sur l'idée que vous êtes une équipe et qu'ensemble,

vous pouvez y arriver. Bon, dis comme ça, c'est sûr que vous êtes immunisés. Mais quand vous êtes intimement convaincus par un ou plusieurs mensonges, c'est une autre paire de manches. Contrer ce détournement des réseaux sociaux passe par l'éducation et la communication. Les plus jeunes sont plus souvent ciblés dans ce cas, puisqu'ils sont majoritaires.

Par ailleurs, à la différence de la publicité classique qui conserve un discours moins engageant, ces personnes ont quelques atouts. Elles créent un lien avec vous. Elles se confient. Une proximité, un attachement et une relation de confiance s'installent.

Un documentaire est joint dans les ressources complémentaires pour vous fournir davantage d'informations à ce sujet.

La technologie NFC

La technologie NFC (near field communication ou communication en champ proche) est utilisée, notamment, pour les paiements sans contact.

Les pickpockets n'ont plus besoin de cacher votre téléphone avec un journal ou de vous faire les poches. Ils peuvent simplement passer à côté de vous et s'en aller sans rien faire du tout. Ils vous volent à l'aide d'un dispositif caché sur eux ou dans leur sac.

Si vous possédez une carte bancaire sans contact, ils peuvent dérober le numéro de celle-ci et la date d'expiration mais pas le nom ni le pictogramme. C'est suffisant pour vous causer des ennuis car certains sites ne vérifient ni le nom ni le pictogramme et permettent donc d'acheter directement avec le numéro de la carte et la date d'expiration. Protégez donc vos cartes dans des étuis anti-RFID. Ils sont spécialement conçus pour bloquer les signaux.

Désactivez cette technologie dans vos appareils si vous ne l'utilisez pas. Ainsi, vous minimisez les risques qu'une faille y soit exploitée.

Les méthodes de paiement par téléphone sont un peu plus sécurisées car elles vous demandent soit un code, soit de déverrouiller votre téléphone. Privilégiez les applications les plus connues comme Google Pay ou Apple Pay pour un maximum de sécurité.

Comment se protéger ?

Tout le monde peut se faire arnaquer, mais les victimes d'extorsion ou de piratage sont principalement les personnes qui ne se sécurisent pas suffisamment. Il est important d'avoir une bonne hygiène numérique. C'est-à-dire :

Prendre le temps

Prendre le temps de discerner le vrai du faux, surtout si c'est urgent. La location d'un appartement ? Êtes-vous sûr qu'il existe ? Une vente en seconde main ? L'acheteur vous demandera-t-il de créer un compte pour le transport du colis ? Un voyage organisé ? Ne payez-vous pas un petit peu trop tôt ? Un compte à réactiver dans les 48h sous peine de le voir supprimé ? L'adresse mail ou l'adresse du site est-elle fiable ? Une amende à payer dans les 24h ? À qui ?

N'achetez en ligne que sur des sites de confiance et auprès de vendeurs de confiance.

S'informer sur les tendances des arnaques

De manière passive : à la télévision, à la radio,...
De manière active : sur le site Safeonweb, par des documentaires, des formations,...

Tenez-vous aussi informés de l'actualité technologique en général. Les médias traditionnels n'informent pas assez sur les outils informatiques. Or, ces derniers peuvent autant être une aide précieuse que contraignants. Ne nous le cachons pas, ça peut être compliqué à utiliser. Mais on n'est plus à une époque où on pouvait dire que c'était pour les geeks, ces gens pleins de boutons, qui mangent des chips et boivent des sodas. Il vaut mieux ne pas se laisser distancer par les évolutions technologiques. On va peut-être avoir dans les prochaines années de nouvelles innovations via l'intelligence artificielle ou la réalité mixte ! Et ici aussi, il nous faudra acquérir d'autres réflexes. La croissance de l'évolution technologique est exponentielle. Je pense que vous vous en rendez compte aussi. Je vous fournirai quelques sources d'informations à la fin.

Comment faire si tout ça ne vous intéresse pas beaucoup ou si ça vous semble trop ? Vous pouvez prendre la bonne habitude d'apprendre une petite chose de temps en temps, de préférence liée à vos centres d'intérêt pour commencer.

Mettre à jour ses appareils

Les mises à jour fournissent de nouvelles fonctionnalités, mais surtout, des correctifs de sécurité. Parfois, elles se font automatiquement. Parfois, vous devez donner votre feu vert. Si vous souhaitez vérifier manuellement, vous pouvez généralement aller dans les paramètres.

En termes de sécurité, l'adage : "Tant que ça fonctionne, …" n'est pas une bonne idée.

Opter pour une suite de sécurité

Communément appelée “antivirus”, on retrouve des versions gratuites ou payantes. Par défaut, Windows est protégé par “Windows Defender” et Android par “Play Protect” (gratuitement). Certaines suites de sécurité proposent un contrôle parental, un gestionnaire et un générateur de mots de passe, la possibilité d’enregistrer des notes ou vos cartes bancaires de façon sécurisée et d’autres fonctionnalités utiles. Choisissez celle qui correspond le mieux à vos besoins. C’est une bonne mesure additionnelle mais ça ne garantit pas votre sécurité.

Gardez à l’esprit que opter pour ces solutions vous rend petit à petit dépendants de leur système.

Sauvegarder ses données

Sauvegardez vos données régulièrement sur différents supports (pour ne pas qu’ils tombent en panne en même temps). Ayez au MINIMUM 2 copies de vos données importantes. Par exemple, vous pouvez acheter un disque dur externe pour effectuer une sauvegarde de votre ordinateur. Certains services en ligne proposent également des solutions. Cela dit, vous venez de le lire, vous dépendez de leur disponibilité.

Sauvegarder ses données est important. C’est une garantie contre la panne du système, contre une grave infection, contre le vol ou la perte d’un support.

Si vous choisissez d’utiliser un disque dur externe, évitez de le laisser brancher à votre ordinateur car il pourrait alors être infecté en même temps que ce dernier.

Paramétrer le navigateur internet

Les paramètres regorgent d’options intéressantes concernant la personnalisation de votre expérience et la sécurité. Voici quelques possibilités :

- Réduire la publicité.
- Réguler le suivi de votre navigation par les différents sites.
- Décider de la réaction du navigateur lorsque vous téléchargez un fichier.
- Supprimer les cookies.
- Supprimer l’historique de navigation ou le désactiver.
- Vous protéger contre les pages web malveillantes.
- Etc.

Je vous invite à y faire un tour. Pour ma part, je n’utilise jamais une application sans avoir fouillé ses paramètres.

Une règle d’or consiste à laisser les réglages par défaut si vous ne les comprenez pas bien. Bien sûr, vous pouvez vous contenter de comprendre la base d’un paramètre trop compliqué pour décider s’il convient de l’activer ou non. Je pense notamment aux paramètres de sécurité qui sont souvent difficiles à saisir. Et cette petite base peut éventuellement tenir sur une phrase ou un petit paragraphe.

Localiser un traceur qui vous suit

AirTag, SmartTag,… pour n'en citer que 2. Ces petits objets connectés, grands comme une pièce de 2€, sont pratiques pour retrouver vos clés ou votre portefeuille. Mais, entre de mauvaises mains, ils peuvent aussi servir à vous localiser sans votre consentement. Comment ? En en cachant un dans votre sac / sacoche ou dans votre voiture.

Heureusement, votre téléphone pourra peut-être le localiser si les conditions nécessaires sont réunies (téléphone et traceur compatibles, localisation de la position activée, Bluetooth activé et alertes de traceur inconnu activé).

Accéder aux sites par les moteurs de recherche

Afin d'être sûr que vous accédez bien aux sites souhaités, recherchez-les via un moteur de recherche (comme Google, Bing,...).

Par exemple, si vous recevez un message vous informant que vous devez cliquer sur un lien pour réactiver votre compte Netflix, passez par un moteur de recherche pour accéder au site en question. Une fois que c'est fait, ajoutez-le en favori pour y accéder plus facilement la prochaine fois.

Si vous cliquez sur le lien du message, vous pourriez être renvoyé vers un site qui y ressemble mais qui cherche à vous tromper.

Ne jamais communiquer d'informations privées sur un site http

Les communications envoyées (identifiants, mots de passe,...) sur un site http ne sont pas cryptées. Elles sont donc lisibles par n'importe qui avec un peu de moyens matériels, même si le propriétaire du site est de bonne foi.

Généralement, en haut du navigateur, à gauche de l'adresse du site, vous pouvez cliquer sur l'icône pour obtenir des informations sur le protocole utilisé (http, https,...).

Je rappelle aussi : le fait qu'un site commence par https n'est pas un critère de sécurité si le propriétaire a de mauvaises intentions.

Verrouiller son ordinateur, son smartphone / se déconnecter de sa session bancaire

Toutes les sécurités mises en place ne servent à rien, si vous laissez un accès direct à vos appareils. Permettez l'accès via un code, par exemple.

Ranger ses cartes sans contact dans des étuis anti-RFID

RFID : Radio Frequency Identification (l'identification par radiofréquence).

Ces étuis empêchent les appareils malveillants de récupérer vos informations bancaires à distance. La récupération peut aller jusqu'à un mètre avec de très bons outils.

Ne pas se connecter à un wifi public ou inconnu

Des pirates pourraient intercepter vos communications ou installer des malwares sur vos appareils. Privilégiez une connexion 4G ou 5G (les données mobiles).

Pour un maximum de sécurité en dehors de chez vous, désactivez le wifi. Vérifiez également dans vos paramètres wifi qu'aucune application n'a le droit de réactiver le wifi à votre insu.

Récapitulatif et spécificités des méthodes d'arnaque et de protection concernant les emails

Les dangers

- Pièces jointes : Malware (virus) ?
- Redirection vers un lien : compléter un formulaire frauduleux, télécharger un malware,...
- Se laisser convaincre par le mail et y répondre.
- Certaines images pourraient posséder un traqueur informant l'expéditeur que vous avez ouvert son mail. Ainsi, il saura que votre adresse mail est active et pourra vous envoyer plus d'emails.

Les pistes pour déceler l'arnaque

- Une adresse mail bizarre ou qui n'est pas de l'entreprise qu'elle prétend être. Exemple : "exemple@proxinnus.be" au lieu de "exemple@proximus.be". Parfois même, l'adresse peut être légitime mais le mail malveillant.
- Une forme d'urgence, menace, alarme (concernant un compte en banque, un compte microsoft, un compte netflix,...) qui vous incite à réagir sans réfléchir.
- Une demande d'argent ou une demande pour annuler une transaction qui, en réalité, en génère une nouvelle !
- Une demande d'informations confidentielles (aucun service sérieux ne vous les demandera par ce biais).
- Un retour sur investissement, un tirage au sort chanceux…
- Le mail contient des fautes d'orthographe ou de grammaire (ça se voit de moins en moins grâce à l'intelligence artificielle).
- Le mail n'est pas attendu (un colis).

Comment se protéger

- Ne pas l'ouvrir : si vous avez un vieux système de messagerie par mail, il pourrait être infecté à l'ouverture du mail. L'adage "Tant que ça fonctionne…" ne fonctionne pas dans la sécurité informatique. Mettez vos systèmes à jour pour combler les failles de sécurité.
- Prendre le temps de vérifier les informations.
- En discuter avec un ami, la famille, vos communautés.
- Ne pas répondre.
- Signaler le mail en tant que spam à votre service de messagerie pour lutter contre ce type de pratique.
- Ne surtout pas télécharger la pièce jointe / empêcher les téléchargements automatiques de pièces jointes dans vos paramètres.
- Ne surtout pas cliquer sur les liens. Par habitude, je ne clique même plus sur les liens des mails "bienveillants".
- Dans les paramètres, empêcher l'affichage des images qui pourraient posséder des traqueurs.
- Réfléchir avant de renseigner son adresse mail à quelqu'un, comme un commercial.

Ou posséder au moins deux adresses mails, dont l'une sert de poubelle, en quelque sorte.

- Vérifier la véracité du mail sur le site officiel, l'application officielle ou par un coup de téléphone.
- Éviter d'envoyer des mails à toute une liste de contacts, sinon, mettre les destinataires en cci (copie carbone invisible). Ainsi, personne n'a accès à toute la liste. Même si personne n'est malveillant dans la liste, l'une des personnes pourrait se faire pirater sa messagerie et donner accès à tout un réseau de contacts.

Les nouvelles / futures menaces

À l'écriture de ces quelques pages, nous sommes en pleine rupture technologique avec l'émergence de l'intelligence artificielle générative. Voici quelques inquiétudes actuelles :

- L'IA peut imiter la voix de l'un de vos proches ou reconstituer un appel vidéo avec son visage pour vous tromper. Elle peut aussi créer entièrement des vidéos de journalistes connus dans lesquelles on les verrait promouvoir des produits. C'est ce qui est arrivé à deux journalistes de la RTBF.
- L'IA pourrait remplacer le travail des humains dans l'arnaque aux sentiments. On pourrait donc imaginer quelqu'un superviser une intelligence artificielle générative traitant des centaines ou des milliers de conversations en même temps.
- L'orthographe des messages trompeurs sera correcte.
- Les "fake news" (fausses nouvelles) sont un phénomène déjà présent, même sans intelligence artificielle. On diffuse de fausses informations (vidéos, articles, bandes sonores,...) pour modifier votre opinion. Mais cette fois-ci, on peut passer à la vitesse supérieure. En effet, l'IA peut générer en quelques secondes des images qui n'existent pas, rédiger de faux articles de presse ou générer de fausses vidéos.
- Les hallucinations : demandez quelque chose à une IA et elle pourrait vous répondre quelque chose de plausible mais faux. À l'heure actuelle, c'est un phénomène répandu. On peut supposer qu'il se réduise au fil de son évolution.
- L'intelligence artificielle peut mettre le visage de votre enfant dans de sales vidéos, sur base d'une photo diffusée sur internet.
- L'intelligence artificielle pourrait vous inciter à moins penser par vous-mêmes. Si elle peut effectuer certaines choses mieux que vous, à quoi bon le faire soi-même ? L'idée pour contrer ce point est de s'en servir comme assistant dans un apprentissage actif (donc, réfléchir par soi-même avant de la consulter). Plus elle s'améliore, plus vous pouvez la considérer comme un outil pédagogique ayant un avis pertinent sur votre travail. Ainsi, votre vitesse d'apprentissage sera grandement accrue.
- L'IA reflétera probablement les mêmes valeurs, la même idéologie que celles de son créateur.
- …

Cette innovation va opérer de grands changements dans la société. Elle va booster les possibilités de chacun et créer des opportunités qui étaient peut-être difficilement envisageables avant. C'est pourquoi il est important de s'informer sur ses inconvénients mais aussi sur ses bénéfices. Et avec le temps, il vous viendra certainement à l'esprit des idées intéressantes que vous voudrez travailler avec l'IA. En complément, voici une série d'avantages qu'elle propose(ra) :

- L'IA peut déjà voir (analyser une image, un flux vidéo et vous dire ce que c'est), entendre (comprendre ce que vous lui demandez vocalement, analyser un enregistrement,...), lire (comprendre ce que vous lui demandez par écrit).
- L'interaction homme-machine est désormais possible par le langage naturel. Demandez à l'ordinateur quelque chose avec vos propres mots pour qu'il s'exécute. Actuellement, cette expérience est plutôt limitée.
- L'IA peut vous inspirer pour une idée.

- L’IA peut effectuer des tâches qui vous prendraient du temps mais qui ne vous apporteraient pas grand chose (retoucher une photo, monter une vidéo avec quelques effets, créer un powerpoint, créer une image,...)
- …

Quand vous communiquez avec ces intelligences, faites attention à ne pas divulguer d’informations sensibles, car vos conversations peuvent être relues par d’autres personnes, notamment pour améliorer leurs services.

Ressources complémentaires

- Pour suivre l'actualité technologique, abonnez-vous à la chaîne Youtube "Tech & Co". C'est gratuit.

- Child Focus : https://childfocus.be/fr-be/

- Conseils et statistiques : https://www.police.be/fr/ et https://safeonweb.be/fr
  Si vous vous faites arnaquer, le site safeonweb vous indique pas à pas les étapes à suivre en fonction de différents types d'arnaques.

- Scannez vos fichiers et adresses web en ligne : https://www.virustotal.com/fr/

- Cyber-arnaques : un piège pour tous : une émission disponible sur la plateforme Auvio de la RTBF.

- Une immersion dans le monde de l'arnaque, ses métiers, ses méthodes : https://www.youtube.com/watch?v=6Jv0EzXdQbk

- L'ia, demain : https://www.youtube.com/watch?v=yIBH9brvBPk

- Tableau des appels et SMS surtaxés et informations supplémentaires : https://www.proximus.be/support/fr/id_sfaqr_3rd_max_price/particuliers/support/factures/controler-vos-couts/numeros-sms-et-apps-payants/numeros-payants-et-sms-payants-combien-ca-coute.html

- Conseils concernant les appels et SMS indésirables : https://www.proximus.be/support/fr/id_sfaqr_unwanted_calls_or_sms/particuliers/support/telephone/voicemail-et-gestion-des-appels/gestion-des-appels/appels-ou-sms-indesirables.html

- Annuaire de recherche inversée pour les fournisseurs de services tiers : https://www.proximus.be/support/fr/id_sscr_3rd_party/particuliers/support/factures/gerer-vos-factures/plainte-a-propos-de-votre-facture/comment-contacter-les-fournisseurs-de-services-tiers.html

- Conseils pour retrouver le propriétaire d'un numéro de téléphone : https://www.proximus.be/fr/id_b_cr_look_up_cell_phone_number/particuliers/blog/news/le-bon-conseil-de/comment-retrouver-proprietaire-numero-gsm.html

- Surveiller ses enfants sans les espionner : https://www.voo.be/fr/news/surveiller-ses-enfants-sans-les-espionner

- Reportage et débat sur les pratiques commerciales des influenceurs. Peuvent-ils faire comme ils veulent ? : https://www.youtube.com/watch?v=eiP944SMI2s