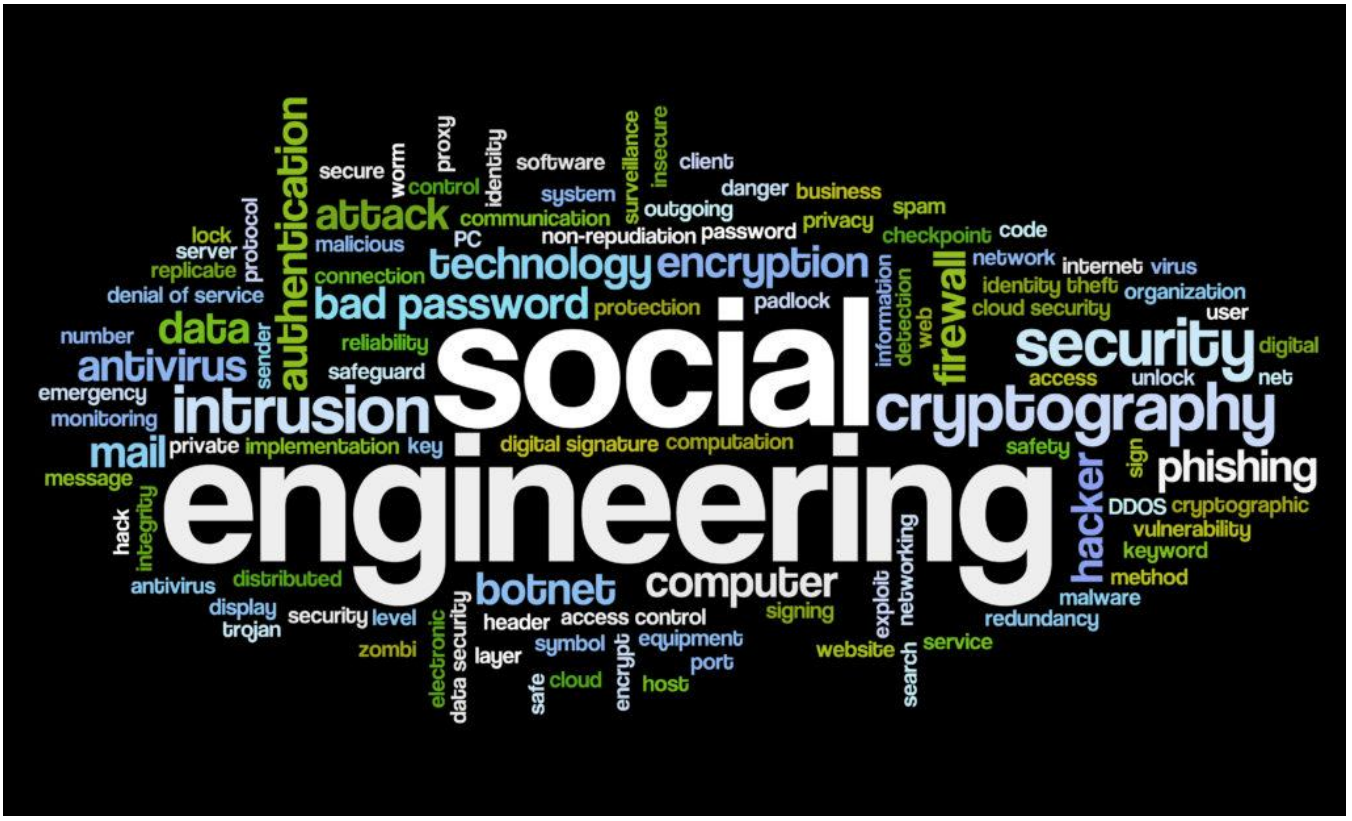
Matrod Rémi
Jacquet Virgile

Social Engineering



Sommaire

1. Introduction

L'Homme essaie toujours d'améliorer la sécurité informatique du côté de la machine : on la rend sûre, on la rend robuste et on la rend résistante en utilisant des protocoles, des firewalls…

Malheureusement, il y aura toujours un maillon de la chaîne que l'on ne pourra pas complètement renforcer, et c'est l'utilisateur qui se sert de la machine. C'est de ce maillon le plus faible qu'à été créé le social engineering, utilisé pour exploiter la naïveté et les sentiments humains.

2. Définition

L'**ingénierie sociale** (en anglais "**social engineering**") est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie. Les termes plus appropriés à utiliser sont le **piratage psychologique** ou la **fraude psychologique**. Dans le contexte de la sécurité de l'information, la désignation d'ingénierie sociale est déconseillée puisqu'elle n'accentue pas le concept de tromperie [1].

Cela nous permet de définir plusieurs points techniques :

- Premièrement, la manipulation, car on incite les gens à donner de leur plein gré des informations qu'ils ne devraient pas divulguer.
- Deuxièmement, la fraude, car l'acte en lui-même est un délit d'usurpation d'identité numérique : « L'usurpation d'identité 'numérique', telle que prévue à l'article 226-4-1 alinéa 2 du code pénal [...]. L'auteur de l'infraction, personne physique, encourt un an d'emprisonnement et 15.000€ d'amende. La condamnation peut atteindre 75.000€ lorsque l'auteur de l'infraction est une personne morale » [2].
- Enfin, le piratage, car une fois les informations ciblées obtenues, l'individu peut récupérer voire modifier les comptes obtenus, ainsi qu'utiliser ou revendre les informations de ce dernier.

De plus, le social engineering ne se limite pas à simplement attaquer des individus isolés, des entreprises peuvent également être visées par ce type d'attaques.

Également, le social engineering exploite la plus grande faiblesse humaine, les sentiments. Ce type d'attaque joue sur les sentiments humains forts tels que la peur, la curiosité, la culpabilité ou encore la colère.

3. Des faits

En 2021, 98% des cyberattaques utilisent du social engineering de manière globale, que ce soit pour viser des entreprises comme des particuliers.

La forme principalement utilisée pour faire du social engineering est le **phishing** (décrit plus bas).

Les cyberattaques de ce type qui réussissent peuvent mener à différents résultats. Voici la décomposition des différents types de données récupérées au travers d'une attaque de social engineering :

- 65% de vol d'identité numérique,
- 17% de vol de compte,
- 13% d'accès à un compte bancaire,
- 4% de nuisance (récupération d'informations pour du spam ou des appels malicieux),
- 1% de vol de données.

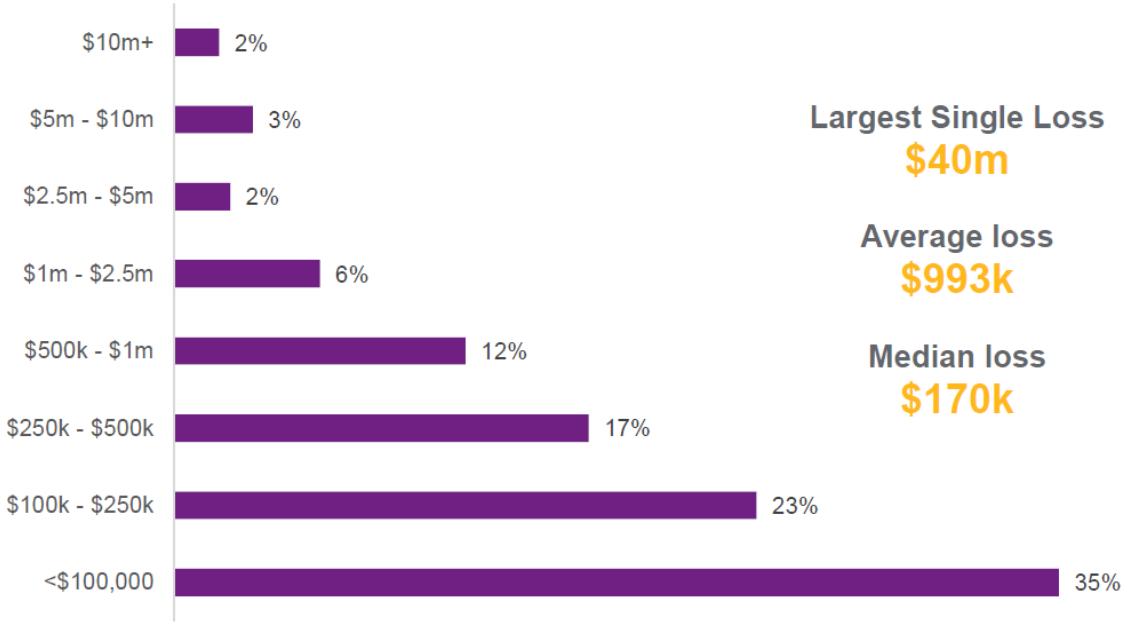


Schéma de la perte économique des entreprises victimes de social engineering en 2020
Source : Willis Towers Watson Claims Database

De plus, une attaque de social engineering est bien moins coûteuse qu'une attaque informatique à grande échelle. En effet, une seule personne et un seul ordinateur sont nécessaires pour faire du social engineering, alors qu'une attaque de type « **ransomware** » (crypter des fichiers sur un ordinateur et les décrypter contre une rançon) ou « **DDoS** » (attaque par déni de service distribué, où des milliers d'ordinateurs se connectent à un site en même temps, le rendant inaccessible)

demandent beaucoup plus de ressources ainsi que des compétences en informatique. Au contraire, le social engineering ne requiert aucune compétence en informatique et même peu de compétences psychologiques, et un simple mail envoyé à une entreprise est environ 64 fois moins coûteux que de mettre en place un ransomware, pour des résultats qui seront la plupart du temps similaires.

Une attaque de social engineering possède un coefficient de réussite qui est juste en dessous de **80%**, ce qui en fait le modèle d'attaque de choix pour un grand nombre de hackers qui ne souhaitent pas mettre en place de grosses infrastructures, faire de la cryptanalyse, développer des systèmes de cassage de mots de passe… Il suffit d'un mail sur le bon maillon pour obtenir l'intégralité des informations que l'on cherche.

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Healthcare	176	170	242	209	239	215	301	236	305	223	256
Other Industries	152	111	138	137	176	140	116	46	59	27	159
Financial Services	80	85	87	126	154	122	145	97	156	87	134
Education	8	30	86	88	102	64	108	58	136	78	86
Professional Services	-	-	-	1	0	0	0	1	17	88	68
Government	131	65	114	180	161	138	162	127	118	89	61
Retail	56	41	82	115	132	109	122	126	147	75	55
Technology	55	57	73	67	61	63	121	84	85	59	37
Industrial	-	-	-	-	-	-	20	12	41	24	31
Hospitality	1	0	0	1	2	0	15	15	26	15	15
Insurance	-	-	-	-	1	1	9	6	11	14	15
Entertainment	-	-	-	-	3	2	20	10	37	9	11
Non-Profit	-	-	-	-	-	-	17	11	18	7	11
Social Media	-	-	-	1	1	1	1	1	6	3	6
TOTALS	659	559	822	924	1,032	855	1,163	830	1,162	798	945

Source: BREACHLEVELINDEX.COM

Évolution des incidents impliquant du social engineering dans les différentes industries.

On remarque une très nette augmentation du nombre d'attaques de type social engineering entre 2013 et 2017, date à partir de laquelle les protocoles de protection informatiques anti-phishing et anti-social-engineering ont été mis en place dans les entreprises.

4. Les formes

Il existe autant de formes de social engineering que de personnes qui le pratiquent, que ce soit sous forme d'un mail d'un « ami » qui a préalablement été piraté, d'une image diffusée sur un réseau social, d'un coup de fil d'une entreprise qui n'arrive plus à vous trouver dans leur base de données, ou bien d'une offre commerciale alléchante, les possibilités sont quasiment infinies. On peut cependant regrouper ces méthodes en quatre grands groupes : les attaques par appel téléphonique, les attaques par écrit, les attaques « physiques », et enfin les attaques par Internet.

Brièvement, la forme par appel téléphonique revient à se faire passer pour un organisme (ONG, association…) pour obtenir des informations sans que la personne ne se doute de rien.

La version papier utilise un principe similaire, avec la plupart du temps un appel à passer à un numéro donné dès la réception de la lettre ou bien en renvoyant un formulaire donné dans la lettre.

L'attaque Internet est celle qui nous intéresse le plus, car il s'agit aujourd'hui du type d'attaque le plus vastement pratiqué, ainsi que celui qui ne nécessite aucun logiciel tiers pour récupérer des données, des mots de passe ou même des groupes de comptes.

Nous excluons ici les attaques physiques qui opèrent au niveau de l'inattention de la personne qui a laissé son matériel déverrouillé et s'est absenté, ou bien qui a été forcé à donner ses codes d'accès contre son gré, par exemple :

- **Le (reverse) tabnabbing** : L'attaquant accède physiquement à l'ordinateur de la victime et ouvre son navigateur Internet pour en changer manuellement l'URL d'un des onglets afin de le rediriger sur un site infecté.
- Le **tailgating** : L'attaquant obtient des informations par la persuasion plus ou moins physique d'une personne prise à part dans une situation à son désavantage (chantage, harcèlement physique, prise de stupéfiants…)

Il existe donc plusieurs dénominations pour les différentes attaques sur Internet :

- Le **phishing** : L'attaquant se fait passer pour le service consommateur d'une entreprise.
- Le **pharming** : L'attaquant envoie une redirection sur un site qui copie le site original.
- Le **BEC** (Business Email Compromise) : La victime reçoit un faux mail provenant d'un de ses supérieurs.
- Le **Whaling** (CEO Fraud) : L'attaquant se fait passer pour le PDG de l'entreprise à laquelle le mail est envoyé. Cette attaque est principalement utilisée sur des personnes travaillant pour la trésorerie de l'entreprise.

- Le **baiting** : L'attaquant se fait passer pour un jeu concours, dont le lien de participation redirige vers un site demandant des informations personnelles et/ou bancaires.
- Le **scareware** : La victime reçoit un pop-up qui l'informe d'une faille de sécurité avant de rediriger sur un site web qui est en fait une publicité avec un lien camouflé vers un site de pharming/baiting.
- Le **Quid pro quo** : L'attaquant propose des informations en l'échange de différentes informations personnelles de la victime. Souvent la personne est ciblée dans le contexte de divorces difficiles, de suspicions de tromperie, etc.
- Le **419** (Nigerian Prince / Advance Fee Scams) : L'attaquant demande un transfert d'argent afin de pouvoir faire un second transfert plus important vers le compte bancaire de la victime, qui ne se fera jamais.
- Le **vishing** (voice phishing) : L'attaquant se fait passer pour la banque ou un organisme économique de la victime et lui demande les informations de son compte afin d'y avoir accès.

Il existe beaucoup d'autres types d'attaques de social engineering par Internet, mais celles citées au-dessus sont parmi les plus courantes aujourd'hui.

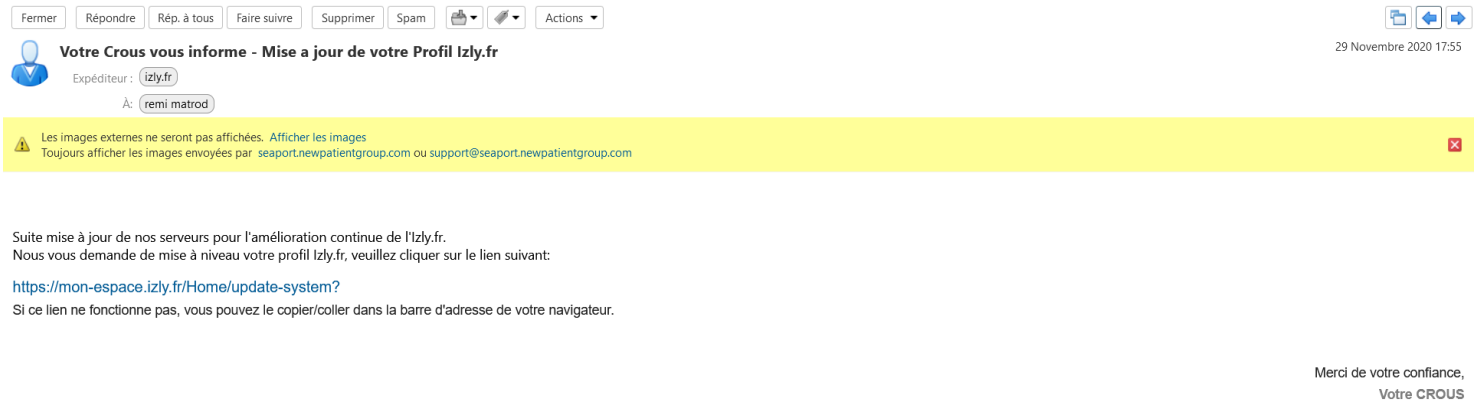
5. Exemples d'attaques

La forme la plus camouflée d'une attaque de social engineering se fait via les réseaux sociaux. En publiant un post public avec un sondage dont la question ressemble, voire est identique à une question de sécurité d'un site, l'attaquant se base sur la probabilité qu'au moins un des utilisateurs ayant répondu à la question a bel et bien utilisé cette question de sécurité pour protéger son compte sur le site en question. En récupérant son adresse mail (en faisant une simple recherche de pseudo sur Internet, ou en utilisant l'API du réseau social), on peut lancer un processus de récupération de compte via l'adresse mail en utilisant des outils comme « J'ai perdu mon compte / mon mot de passe », qui nous permet de changer le mot de passe en toute discrétion. Une fois cette étape réalisée, le compte est désormais entièrement accessible à l'attaquant, lui permettant de publier des messages sous le nom de la victime, de changer son adresse mail d'accès, divulguant toutes les données stockées à l'intérieur comme ses contacts, ses messages privés…

Ensuite, l'attaquant peut utiliser les données obtenues pour les revendre, pour demander une rançon à la victime, mais il peut également envoyer un virus aux amis de l'utilisateur qui ne se doutent de rien, en continuant à utiliser une attaque de social engineering : un simple message avec un lien, une image ou un fichier joint et un grand nombre d'utilisateurs peuvent y perdre leurs comptes s'ils ne font pas attention.

Un autre exemple d'attaque commun est le « **pharming** » : l'attaquant remplace le lien d'un site par un autre lien menant à une copie exacte du site initial. La personne accédant à ce site frauduleux rentre ses identifiants de compte sans se méfier du lien, puis on peut le rediriger vers le vrai site où il se connecte, mais ses identifiants auront entre-temps été récupérés par l'attaquant. La victime ne saura que trop tard que son compte a été piraté, quand ce dernier aura été utilisé afin de réaliser d'autres attaques, ou quand ses identifiants d'accès auront changé.

Voici enfin un dernier exemple d'attaque avec le « **honey baiting** », où un robot se connecte sur un réseau social ou un site de rencontre et contacte des utilisateurs pour se faire passer pour quelqu'un d'émotionnellement et/ou de sexuellement attiré par l'utilisateur en lui envoyant un lien vers un autre site Internet qui demande des informations personnelles voire bancaires. Dans ce cas l'attaquant joue sur les sentiments des utilisateurs pour les pousser à la faute. Ici il n'y a pas de technique précise qui est utilisée pour choisir la ou les victimes, il est très probable que n'importe qui aie déjà reçu un message privé sur un réseau social provenant d'une personne trop bien pour être vraie.


Fermer | Répondre | Rép. à tous | Faire suivre | Supprimer | Spam | Actions

Votre Crous vous informe - Mise a jour de votre Profil Izly.fr

29 Novembre 2020 17:55

Expéditeur : izly.fr

À: remi matrod

Les images externes ne seront pas affichées. Afficher les images
Toujours afficher les images envoyées par seaport.newpatientgroup.com ou support@seaport.newpatientgroup.com

Suite mise à jour de nos serveurs pour l'amélioration continue de l'Izly.fr.
Nous vous demande de mise à niveau votre profil Izly.fr, veuillez cliquer sur le lien suivant:

https://mon-espace.izly.fr/Home/update-system?

Si ce lien ne fonctionne pas, vous pouvez le copier/coller dans la barre d'adresse de votre navigateur.

Merci de votre confiance,
Votre CROUS

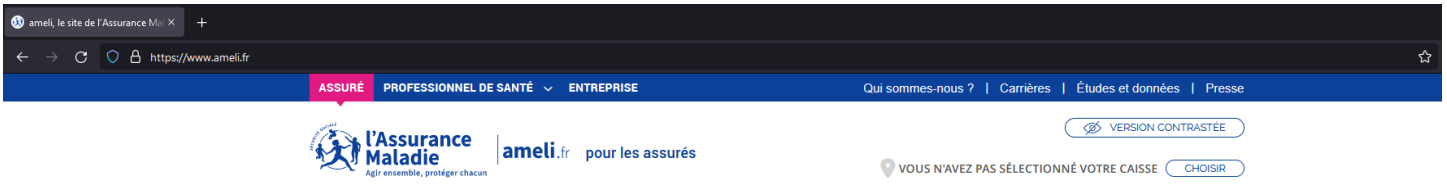
Un exemple de mail frauduleux (il semble être envoyé par IZLY, on remarque des fautes d'orthographe et de grammaire, l'URL redirige sur un autre site que celui du CROUS…)

6. Se protéger

La première règle simple que l'on apprend en créant des mots de passe, c'est de les générer et les protéger avec un gestionnaire de mots de passe (comme **Keepass** ou **Bitwarden**, qui sont des gestionnaires de mots de passe open-source) afin de les rendre non liés à la personne possédant le compte. De la même façon, les réponses aux questions secrètes doivent être non liées à notre personne afin d'éviter de la divulguer dans un moment où on ne pense pas au danger. Il est ainsi préconisé d'éviter de répondre à des sondages qui questionnent votre passé ou votre vie privée, car les informations que vous pouvez laisser échapper dans un moment d'inattention peuvent représenter un danger potentiel pour votre sécurité.

Une réponse secrète peut mener jusqu'au vol de vos coordonnées et de votre compte bancaire, à la photocopie de vos papiers d'identité, de votre RIB, ou de l'adresse de votre domicile, rendant vulnérable les biens qui y sont entreposés.

Pour se prémunir des différents types de phishing, il faut toujours vérifier l'URL du site sur lequel on navigue et éviter au maximum de rentrer des informations sans être sûr de l'authenticité du site, en utilisant différents signes visuels comme le symbole du cadenas sur les sites HTTPS ainsi que les logos, l'orthographe et les dimensions du site web.



Un exemple de site sécurisé : logos à gauche de l'URL pour la protection (certificat du site valide, pas de trackers, cadenas HTTPS), URL normale, contenu du site non louche…

Pour se prémunir contre les attaques de style 419 ou baiting, il n'existe pas des milliers de techniques, il suffit simplement de ne pas croire aux mails que l'on reçoit qui nous informent de notre victoire à un jeu concours auquel nous n'avons jamais participé, ni de croire aux mails ou aux messages des soi-disantes « personnes riches » qui nous demandent de l'aide contre un juteux retour sur investissement.

En somme, la seule vraie défense contre le social engineering est de faire attention à tout ce que l'on trouve sur Internet et de ne pas faire facilement confiance aux mails, aux sites ou à toute information qui tente d'influencer directement nos sentiments, que ce soit pour nous attaquer ou simplement dans une autre fin en soi.

7. La valeur philosophique

Ce qu'il faut vraiment retenir de cette expérience, c'est que l'Homme peut créer des machines aussi sophistiquées que possible et aussi sécurisées que possible, tant que l'utilisateur dévoilera ses données aux plus grand nombre, que ce soit au travers d'un réseau social ou d'un sondage, c'est lui qui restera la plus grosse faille de sécurité du produit. Il est donc mieux de régler ce problème plutôt que de permettre à n'importe qui de pouvoir récupérer nos comptes sans même s'en apercevoir, en suivant des formations par exemple. La sécurité informatique évolue sans cesse et toujours plus vite, alors que la sécurité mise en place par l'utilisateur s'amenuise à chaque avancée technologique.

Pour conclure, d'après les statistiques, nous pouvons nous assurer que la machine informatique est fiable, cependant l'Homme ne l'est pas. Il est temps de renforcer le maillon défectueux et d'apprendre à mieux gérer nos informations et nos données que l'on transmet aux travers des différents médias sociaux et des outils que nous utilisons tous les jours.

Sources

1. Source : Wikipédia
2. Village de la justice - article : LE DÉLIT D'USURPATION D'IDENTITÉ NUMÉRIQUE, UN NOUVEAU FONDEMENT JURIDIQUE POUR LUTTER CONTRE LA CYBERCRIMINALITÉ.

SécuritéInfo.com
https://www.securiteinfo.com/attaques/divers/social.shtml

Purplesec
https://purplesec.us/resources/cyber-security-statistics/

Village de la justice
https://www.village-justice.com/articles/Delit-usurpation-identite,18790.html

IT governance
https://www.itgovernance.co.uk/social-engineering-attacks#:~:text=The%20most%20common%20form%20of,or%20links%20to%20malicious%20websites.