Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

29 janvier 2024

Rapport Anti-Phishing 2023

Introduction

La Confédération exploite la plateforme « antiphishing.ch » depuis une dizaine d'années. Celle-ci a été lancée en 2014 par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et est gérée depuis 2020 par le Centre national pour la cybersécurité (NCSC), qui est devenu l'Office fédéral de la cybersécurité (OFCS) le 1er janvier 2024. Cette plateforme permet non seulement à la population suisse, mais aussi aux organisations, aux autorités et aux PME, d'annoncer les sites web et les courriels suspects. L'objectif consiste à identifier les sites internet qui utilisent un contenu frauduleux pour tenter d'accéder à des données sensibles, comme les données de connexion à un compte de messagerie électronique ou d'e-banking et aux réseaux sociaux, ou encore pour obtenir des données de cartes de crédit (hameçonnage ou phishing en anglais). Les escrocs abusent de la crédulité et de la complaisance de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur (souvent) usurpées et des logos d'entreprise connus.

Les courriels et sites web suspects peuvent être annoncés sur la page internet *antiphishing.ch*. Il est aussi possible de transférer directement les courriels suspects à l'adresse *reports@antiphishing.ch*. Les messages qui sont envoyés à cette adresse sont traités automatiquement sans être lus. Par conséquent, l'expéditeur ne reçoit pas de réponse. Les personnes qui souhaitent recevoir une réponse de l'OFCS peuvent annoncer les courriels d'hameçonnage et les sites web suspects en remplissant le formulaire d'annonce de l'OFCS[1]. Jusqu'à aujourd'hui, les dénonciations adressées par la population, les PME et les exploitants d'infrastructures critiques ont permis à la Confédération et à ses organisations partenaires d'identifier plus de 55 000 sites web d'hameçonnage et de prendre les mesures requises.

[1] https://www.report.ncsc.admin.ch/

Traitement des annonces d'hameçonnage par l'OFCS

Illustration 1 – Plateforme antiphishing.ch de l'OFCS

Les annonces qui sont enregistrées sur *antiphishing.ch* sont soumises à un premier examen automatique. De nombreux sites web sont signalés à plusieurs reprises à l'OFCS, raison pour laquelle il faut commencer par dédupliquer les sites web qui ont déjà été dénoncés. Les métadonnées publiques, qui indiquent par exemple qui est l'hébergeur du site web d'hameçonnage, sont ensuite recueillies. Une capture d'écran du site web en question est en outre générée automatiquement. Elle aide les analystes à déterminer si le site internet sert effectivement à des activités d'hameçonnage. À la fin du processus, les analystes effectuent un contrôle manuel de toutes les annonces.

Lorsque les analystes identifient un site web d'hameçonnage, un message d'avertissement est généralement envoyé par courriel. Si possible, cette mise en garde est ensuite transmise à l'hébergeur du site, au registraire de domaine et au détenteur du domaine (*registrant*). Quand cela est possible, l'OFCS informe également le détenteur de la marque qui est utilisée à des fins d'hameçonnage par les cybercriminels.

Comme pour d'autres cybermenaces, il est important de pouvoir échanger les données relatives aux activités d'hameçonnage sur le plan national et international. L'OFCS met donc rapidement à disposition toutes les informations techniques concernant les actuels hébergeurs de sites web d'hameçonnage, les créateurs de filtres antipourriels et les exploitants de navigateurs internet. Les échanges au sein du groupe de travail international contre l'hameçonnage (*Anti-Phishing Working Group APWG*)[2] sont aussi essentielles pour lutter contre l'hameçonnage.

[2] https://apwg.org/about-us/

Principaux chiffres de l'année 2023

En 2023, **544 367 annonces** en tout ont été enregistrées sur la plateforme *antiphishing.ch*. En outre, 9395 annonces relatives à des tentatives d'hameçonnage ont été reçues via le formulaire d'annonce au cours de la même année. Après la déduplication, **10 007 sites web** ont été identifiés comme étant des **sites d'hameçonnage**, ce qui correspond à une augmentation de 10 % par rapport à 2022. C'est au mois de décembre que le plus grand nombre de sites d'hameçonnage ont été identifiés en 2023 (1380). 99 % des annonces ont été adressées par la population et les PME, et 1 % par des exploitants d'infrastructures critiques. Il faut toutefois préciser que si une grande partie des sites web dénoncés par les exploitants d'infrastructures critiques servaient effectivement à des activités d'hameçonnage, la plupart des cas signalés par la population et les PME concernaient plutôt des pourriels ou des newsletters tout à fait légitimes. Il existe donc une importante différence entre les annonces de la population et celles des exploitants d'infrastructures critiques en termes de reconnaissance de réelle pages web d'hameçonnage.

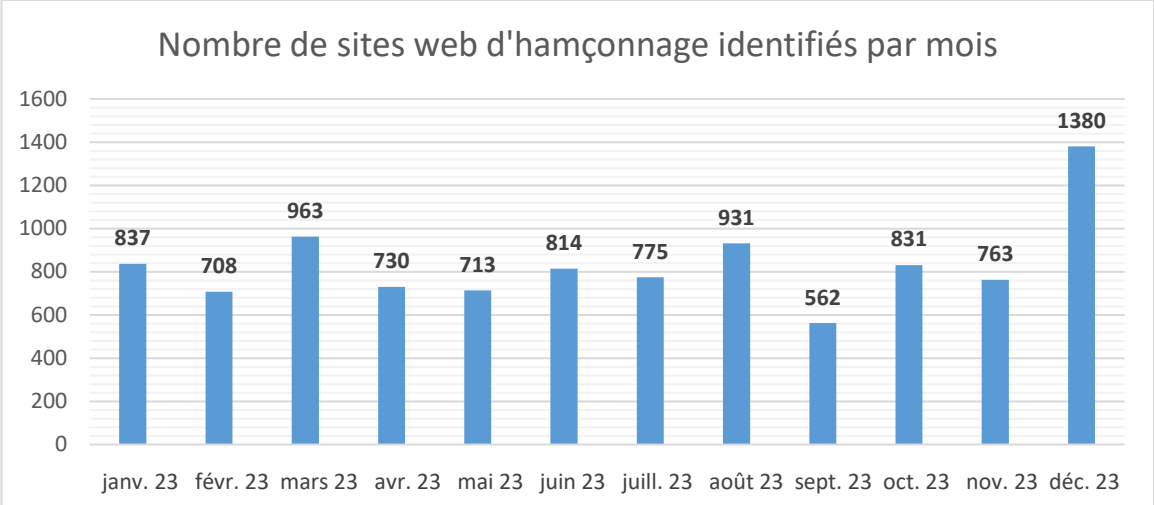

Illustration 2 – Nombre de sites web d'hameçonnage identifiés par mois

Sur les sites web d'hameçonnage identifiés en 2023, les escrocs ont usurpé **260 noms de marque différents**, parmi lesquels **61,1 % de marques suisses,** 33,1 % de marques étrangères et 5,8 % sans utilisation explicite de marque spécifique. Il s'agissait surtout de sites d'hameçonnage génériques permettant d'obtenir les données d'accès au compte de messagerie électronique des victimes.

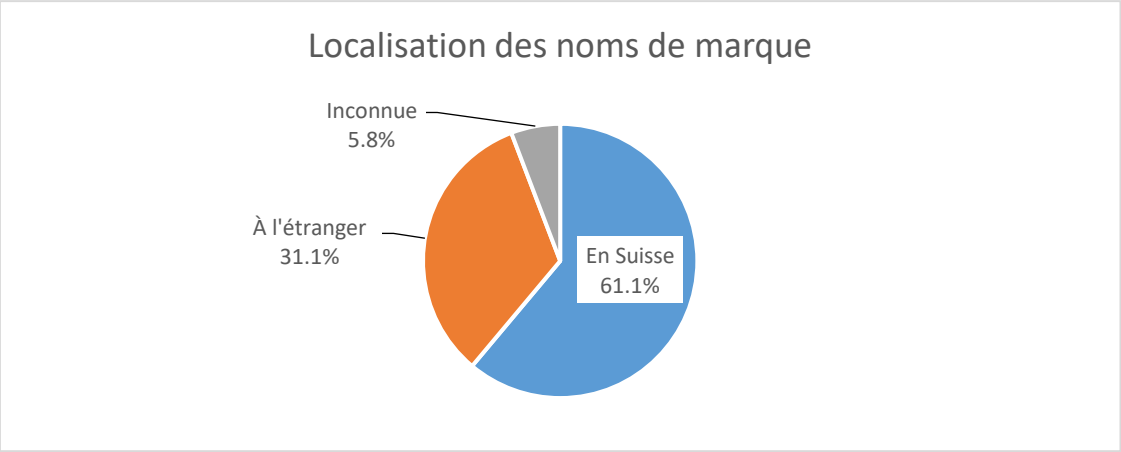

Illustration 3 – Localisation des noms de marque usurpés

Avec 21 %, La Poste Suisse est la marque qui a été la plus fréquemment utilisée par les cybercriminels pour des activités d'hameçonnage en 2023. En tenant compte des fournisseurs étrangers, les sites web d'hameçonnage utilisés par les cybercriminels pour se faire passer pour des entreprises de livraison de courrier et de colis dépassent 40 %. Cependant, les escrocs ne ciblent en principe pas directement les plateformes de ces fournisseurs. Leurs noms de marque sont plutôt utilisés pour tromper les victimes et encaisser de prétendus frais de livraison de colis ou de douane. Ces taxes doivent être réglées par carte de crédit. En réalité, la personne lésée ne paie aucune taxe, mais est victime d'une fraude à la carte de crédit.

Les cybercriminels se servent aussi volontiers de la marque SwissPass (14 % des sites web d'hameçonnage) et des noms de marque d'opérateurs internet et de téléphonie mobile (8 %).

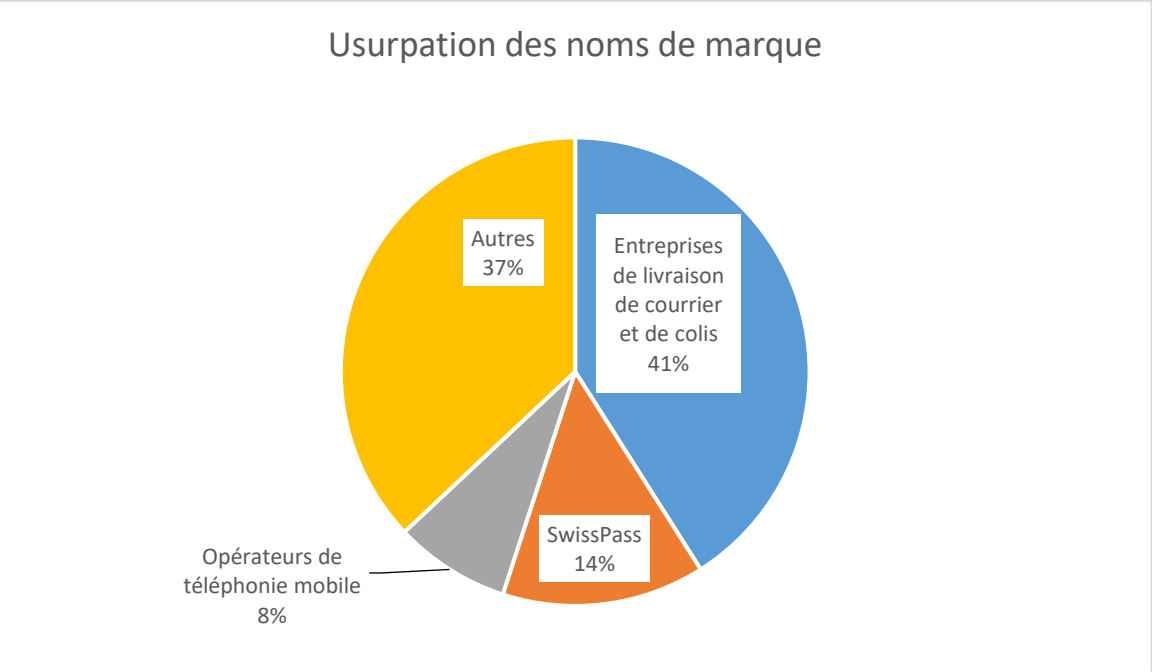

Illustration 4 – Noms de marque usurpés

La plupart des sites web d'hameçonnage sont hébergés sur un domaine de premier niveau (top-level domain *TLD*) étranger. Près de la moitié de tous les sites web identifiés sont exploités sur les domaines génériques de premier niveau (gTLD)[3] *.com* et *.net*. Contrairement au domaine national de premier niveau (ccTLD)[4] *.ch*, l'ordonnance sur les domaines Internet (ODI)[5] ne s'applique pas dans ces cas, si bien que ni l'OFCS ni les autres autorités suisses ne peuvent agir activement contre le site web d'hameçonnage.

[3] *Generic Top-Level-Domain*

[4] *Country Code Top-Level-Domain*

[5] https://www.fedlex.admin.ch/eli/cc/2014/701/fr

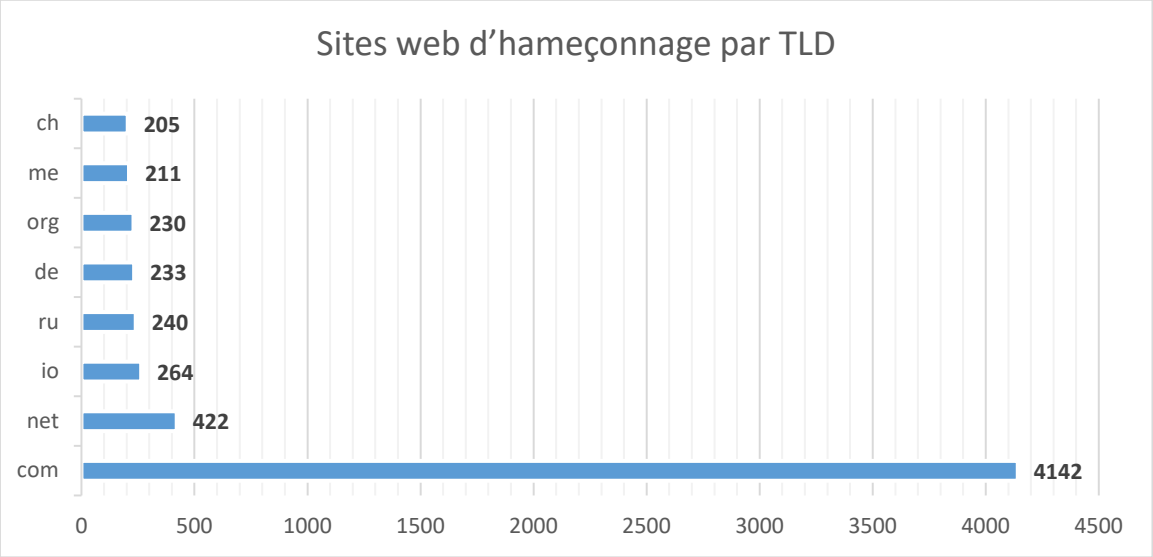

Illustration 5 – Domaine de premier niveau des principaux sites web d'hameçonnage

Pour créer des sites web d'hameçonnage, les cybercriminels se servent entre autres de sites web piratés. Cependant, ils enregistrent aussi souvent directement un nom de domaine dédié, dont l'unique objectif consiste à fournir des sites web d'hameçonnage. **En tout, 205 sites web d'hameçonnage ont été hébergés sur le ccTLD *.ch*. Parmi ceux-ci, on suppose que 25 noms de domaine ont été enregistrés directement par les cybercriminels à des fins frauduleuses exclusivement.** À la demande du NCSC, ces noms de domaine ont été bloqués techniquement et administrativement par le registre, conformément à l'art. 15 ODI.

Les cybercriminels sévissent aussi auprès des hébergeurs de plateformes internet. Le tableau ci-après indique les plateformes internet sur lesquelles le NCSC a identifié la plupart des sites web d'hameçonnage en 2023. Leurs hébergeurs sont également mentionnés.

Rang	Pages d'hame-çonnage	Nom de domaine	Hébergeur	Pays
1	201	codeanyapp.com	Codeanywhere	États-Unis
2	180	plesk.page	Plesk International	États-Unis
3	146	mybluehost.me	Bluehost	États-Unis
4	117	secureserver.net	GoDaddy	États-Unis
5	96	web.app	Google	États-Unis
6	96	cprapid.com	cPanel	États-Unis
7	85	page.link	Google	États-Unis
8	74	tempurl.host	Incsub	États-Unis
9	72	hoster-test.ru	Hoster.ru	Russie
10	72	dweb.link	Protocol Labs	États-Unis
11	71	sviluppo.host	non disponible	non disponible
12	71	cleverapps.io	Clever Cloud	France
13	54	wpengine.com	WP Engine	États-Unis
14	53	builderallwppro.com	non disponible	non disponible
15	51	r2.dev	Cloudflare	États-Unis

Variantes d’hameçonnage

Hameçonnage par SMS

L’an dernier, le NCSC a constaté une augmentation du nombre de cas d’hameçonnage par SMS (*smishing*). Contrairement à l’hameçonnage traditionnel, les tentatives de fraude sont envoyées par SMS ou par son successeur, le protocole RCS, qui est utilisé par de nombreux services de messagerie. L’année dernière, les noms de marque de services de livraison de courrier et de colis ont été régulièrement usurpés pour essayer d’attirer les destinataires vers un site web d’hameçonnage et de leur soutirer ensuite leurs données de cartes de crédit.

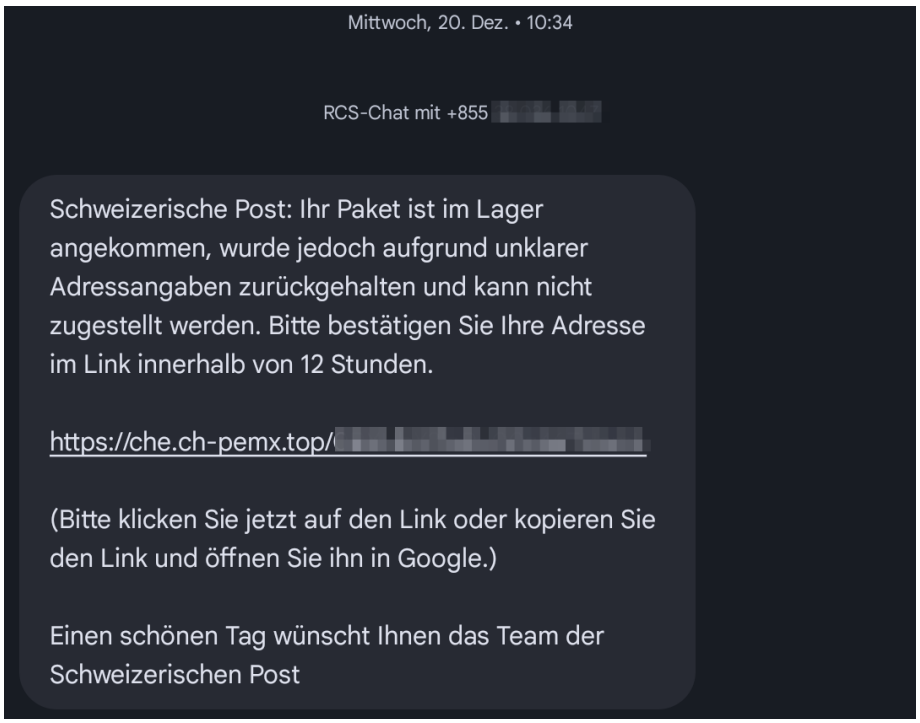

Illustration 6 – Exemple d’hameçonnage par SMS ou RCS

Contrairement à l’hameçonnage par courriel, il n’est pas facile de transférer les SMS suspects ou frauduleux vers la plateforme *antiphishing.ch*, ce qui complique la saisie et l’initialisation de contre-mesures adaptées par l’OFCS. Les utilisateurs doivent s’en remettre aux mesures de protection de leur opérateur de télécommunications ou de système d’exploitation.

L’hameçonnage via les moteurs de recherche

Aujourd’hui, les moteurs de recherche font partie intégrante de notre quotidien numérique. Ils nous permettent de trouver très rapidement toutes sortes d’informations sur le web, qu’il s’agisse d’un artiste, d’une destination pour nos prochaines vacances ou d’informations utiles à notre travail. En Suisse, les moteurs de recherche les plus fréquemment utilisés sont Google (Alphabet) et Bing (Microsoft).

Consulter un moteur de recherche est gratuit. Toutefois, pour que le fournisseur puisse proposer ce service gratuitement, il doit percevoir des recettes. Dans ce contexte, le marché de la publicité représente un modèle économique courant et lucratif : les fournisseurs des moteurs de recherche vendent les premières places des résultats de recherche à des fins publicitaires.

Lorsqu'une personne recherche par exemple un hôtel, il est fréquent que le site web d'un établissement concurrent apparaisse avant celui de l'hôtel initialement recherché dans la liste des résultats, simplement parce que la concurrence paie le fournisseur du moteur de recherche pour cette insertion publicitaire.

Pour les entreprises qui souhaitent diffuser ces publicités, les moteurs de recherche sont une solution très lucrative. Le profilage permet d'orienter les publicités vers le public cible souhaité. Les insertions publicitaires s'affichent alors uniquement lorsque les utilisateurs font partie du groupe ciblé. Les critères sont pratiquement illimités : âge, genre, intérêts, mais aussi pays depuis lequel la recherche est effectuée ou encore langue utilisée par le navigateur web. Ces possibilités ne sont toutefois pas seulement attrayantes pour les entreprises qui ont un intérêt légitime. En effet, les cybercriminels ont compris depuis longtemps que ces insertions publicitaires constituent un moyen idéal pour attirer des victimes potentielles sur des sites web d'hameçonnage.

Au cours du deuxième semestre 2023, le NCSC a reçu beaucoup d'annonces qui concernaient des messages publicitaires frauduleux sur les moteurs de recherche (*rogue ads*). Nombre d'entre eux apparaissent actuellement sur Bing (Microsoft). À l'aide de comptes piratés ou d'identités volées, les cybercriminels louent une surface publicitaire pour un mot clé sur Bing. Comme mots clés, les escrocs utilisent les noms de célèbres établissements de financement suisses ou d'émetteurs de cartes de crédit. Lorsqu'une victime potentielle cherche l'e-banking de sa banque sur Bing, elle voit apparaître l'insertion publicitaire des cybercriminels en premier dans les résultats de la recherche. L'annonce publicitaire est conçue de manière à faire croire qu'il s'agit effectivement du résultat de la recherche de l'e-banking. Si la victime clique sur la publicité, elle est dirigée vers le site web d'hameçonnage des cybercriminels. Grâce à l'hameçonnage en temps réel, le site web peut également accéder aux systèmes e-banking protégés par l'authentification multifactorielle (MFA).

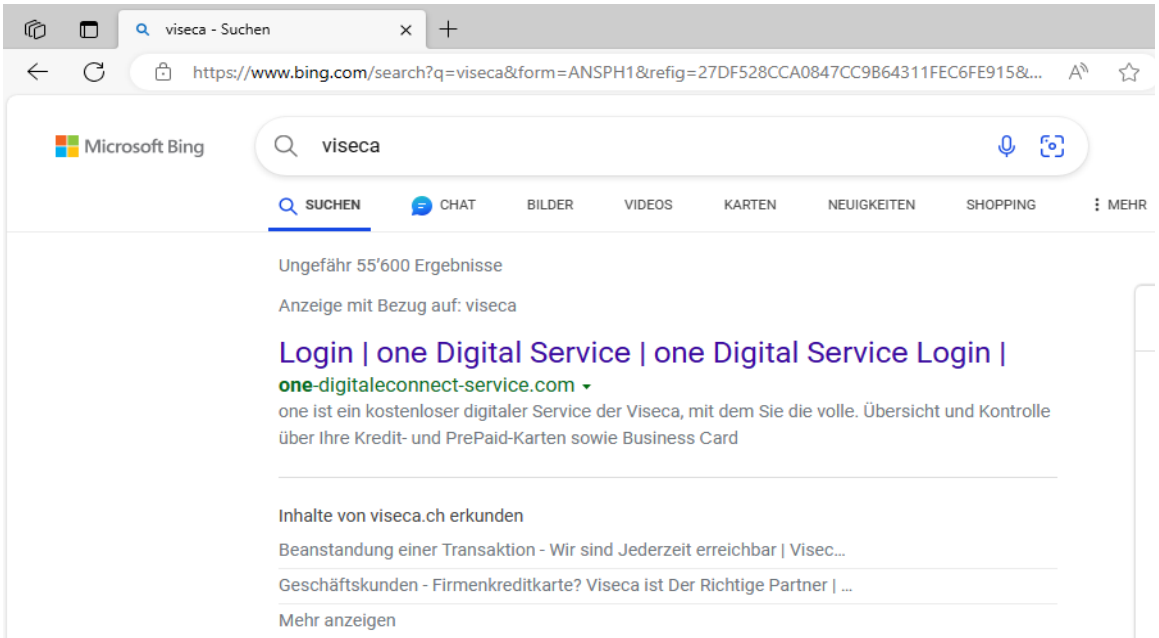

Illustration 7 – Exemple de rogue ad sur un moteur de recherche qui mène vers un site web d'hameçonnage

Pour les cybercriminels, ce mode opératoire comporte de nombreux avantages. D'une part, ils peuvent déterminer de manière ciblée quand la publicité frauduleuse doit s'afficher (pour une banque cantonale de Suisse romande par exemple, les cybercriminels peuvent limiter la publicité à *Suisse* et *langue française*). D'autre part, et contrairement à l'hameçonnage par courriel, ils peuvent contourner les filtres antipourriels susceptibles de détecter les messages frauduleux.

Ce mode opératoire est cependant problématique pour les entreprises de sécurité et les autorités comme l'OFCS qui luttent contre l'hameçonnage dans le cyberespace. En effet, les fournisseurs de moteurs de recherche ne transmettent aucune information sur qui se cache derrière une publicité, ce qui empêche une détection précoce. L'OFCS ne peut donc réagir qu'après la publication de la publicité frauduleuse et l'annonce par la population ou une infrastructure critique. L'OFCS encourage par conséquent la population, les entreprises, les autorités et les organisations à annoncer les cas auxquels elles sont confrontées.

Recommandations

De manière générale, faites preuve d'une grande vigilance à l'égard des courriels et des SMS qui vous invitent à cliquer sur un lien. L'OFCS vous recommande en outre de respecter les points ci-après :

- **Annonce à l'OFCS :** annoncez à l'OFCS tous les courriels ou sites web suspects sur *antiphishing.ch*. Si vous souhaitez recevoir une réponse à votre message, vous pouvez aussi remplir le formulaire d'annonce en ligne sur *https://www.report.ncsc.admin.ch/*.

- **Vigilance :** aucune banque ni aucun établissement de carte de crédit ne vous enverra un courriel ou un SMS pour vous demander de modifier vos mots de passe ou de vérifier vos données de carte de crédit.

- **Authentification multifactorielle (MFA) :** quand cela est possible, activez l'authentification multifactorielle (MFA) sur vos comptes en ligne comme la messagerie électronique ou les réseaux sociaux. Contrôlez dans les paramètres du compte de votre fournisseur si l'option MFA est disponible et activez-la le cas échéant.

- **Utilisation multiple des mots de passe :** n'utilisez jamais un même mot de passe pour plusieurs comptes en ligne. Ayez recours à un gestionnaire de mots de passe pour le traitement de vos données de connexion.

- **Relevé de carte de crédit :** contrôlez régulièrement votre relevé de carte de crédit et prenez immédiatement contact avec l'émetteur de carte de crédit si vous constatez des irrégularités ou des transactions d'origine inconnue.

- **Filtre SMS :** activez le filtre SMS du système d'exploitation de votre smartphone afin de bloquer les SMS suspects.

- **Utilisation de favoris :** utilisez la fonction des favoris (signets) de votre navigateur web pour l'accès à vos comptes en ligne (e-banking, réseaux sociaux ou courriel).

- **Usurpation d'adresse :** n'oubliez pas qu'il est facile de falsifier le nom de l'expéditeur de courriels et de SMS, mais aussi le numéro de téléphone de l'appelant. En cas de doute, exigez de pouvoir rappeler l'appelant.