16 janvier 2025 | Office fédéral de la cybersécurité OFCS

Rapport anti-phishing 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
Protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS

Contenu

1 Introduction

Depuis près de 10 ans, la Confédération gère la plateforme « antiphishing.ch ». Celle-ci a été lancée en 2014 et est gérée par l'Office fédéral de la cybersécurité OFCS. Elle offre à la population suisse, mais aussi aux organisations, aux autorités et aux PME, la possibilité de signaler les sites web et les e-mails suspects. La plate-forme sert à identifier les sites Web qui tentent d'accéder à des données sensibles en se faisant passer pour des entités légitimes. Il peut s'agir par exemple de données d'accès à des comptes de messagerie, d'e-banking ou de médias sociaux, mais aussi d'informations sur des cartes de crédit (ce que l'on appelle le « phishing »). Les escrocs profitent de la crédulité et de la serviabilité de leurs victimes en leur envoyant par exemple des e-mails avec une adresse d'expéditeur (souvent) falsifiée et des logos d'entreprise connus.

Les e-mails ou sites web suspects peuvent être signalés sur le site antiphishing.ch. Mais les e-mails suspects peuvent aussi être transmis directement à reports@antiphishing.ch[1] . Cette boîte aux lettres n'est pas lue, mais traitée par une machine. Il n'y a donc pas de réponse à l'expéditeur. Les personnes qui souhaitent recevoir un retour d'information de la part du OFCS peuvent lui signaler les e-mails de phishing et les sites web suspects via le formulaire d'annonce pour tous les cyberincidents. Grâce aux nombreux signalements effectués par la population, les PME et les exploitants d'infrastructures critiques, la Confédération a pu, en collaboration avec des organisations partenaires, identifier à ce jour plus de **79 000 sites web de phishing** et prendre des contre-mesures appropriées.

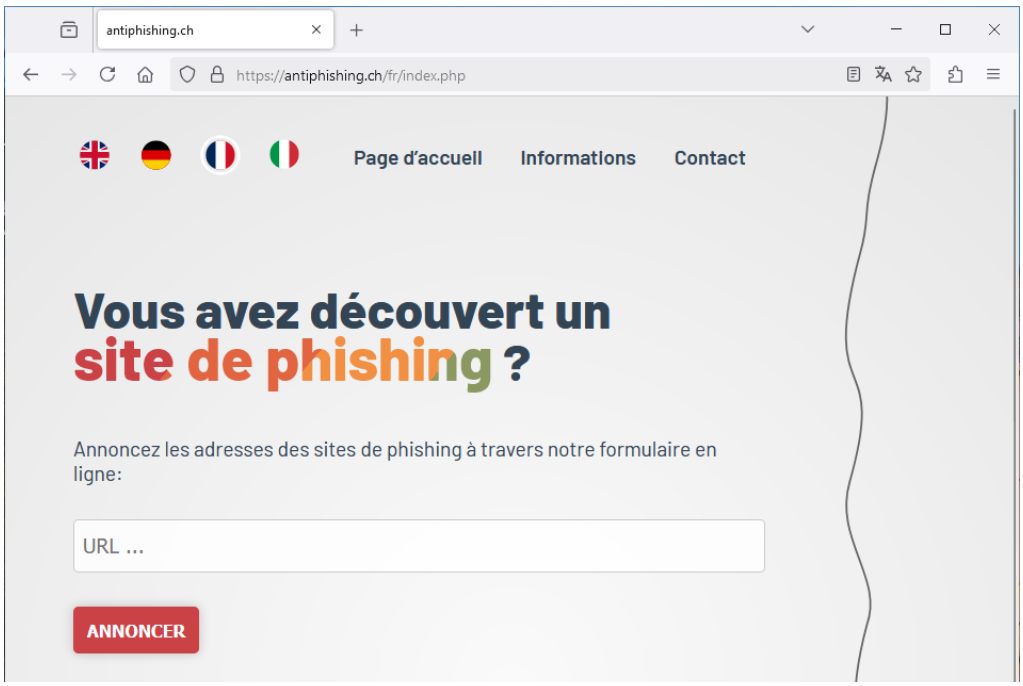

Illustration 1 - Plateforme « antiphishing.ch » du OFCS

[1] reports@antiphishing.ch

2 Que fait le OFCS avec les messages de phishing ?

Les messages envoyés via antiphishing.ch sont soumis à un contrôle préalable par une machine. De nombreux sites web sont signalés plusieurs fois au OFCS, c'est pourquoi les URL de phishing signalées plusieurs fois sont filtrées en premier lieu. Ensuite, des métadonnées accessibles au public sont collectées, par exemple le fournisseur qui met à disposition le site web de phishing présumé. En outre, une capture d'écran du site Web signalé est automatiquement réalisée. Cela aide les analystes du OFCS à déterminer si le site signalé est effectivement un site de phishing. À la fin du processus, chaque notification est examinée et évaluée manuellement par les analystes.

Si un site web est identifié comme hameçonnage par l'analyste, le OFCS envoie une plainte pour abus. Celle-ci est envoyée par e-mail au fournisseur d'hébergement web, au registraire de domaine ainsi qu'au propriétaire du domaine (« registrant »). Dans la mesure du possible, le OFCS informe également le propriétaire de la marque utilisée par les cybercriminels dans le cadre de la campagne de phishing.

Comme pour de nombreuses cybermenaces, l'échange national et international est un facteur important pour le phishing. C'est pourquoi le OFCS met à la disposition des fournisseurs d'accès à Internet, des fabricants de filtres anti-spam ainsi que des fabricants de navigateurs Web des informations techniques sur les sites Web actuels de phishing en temps réel. L'échange au sein du groupe de travail international Anti-Phishing Working Group (APWG)[2] est également un pilier important de la lutte contre le phishing.

3 Les principaux chiffres de 2024

En 2024, un total **de 975 309 déclarations** ont été envoyées via la plateforme « antiphishing.ch ». Cela correspond à une augmentation de 79% des communications de soupçons par rapport à l'année précédente (544'367 communications). Après avoir filtré les URL de phishing mentionnées plusieurs fois, **20 872 sites web** ont pu **être identifiés comme sites de phishing** à partir des messages. Cela correspond à une augmentation de 108% par rapport à l'année précédente (10'007). Avec 2 215 sites de phishing, c'est au mois de mars que le plus grand nombre de sites de phishing de l'année 2024 a été identifié. C'est au mois de juillet que le plus grand nombre de déclarations de soupçon a été envoyé au OFCS, avec 235'310 déclarations.

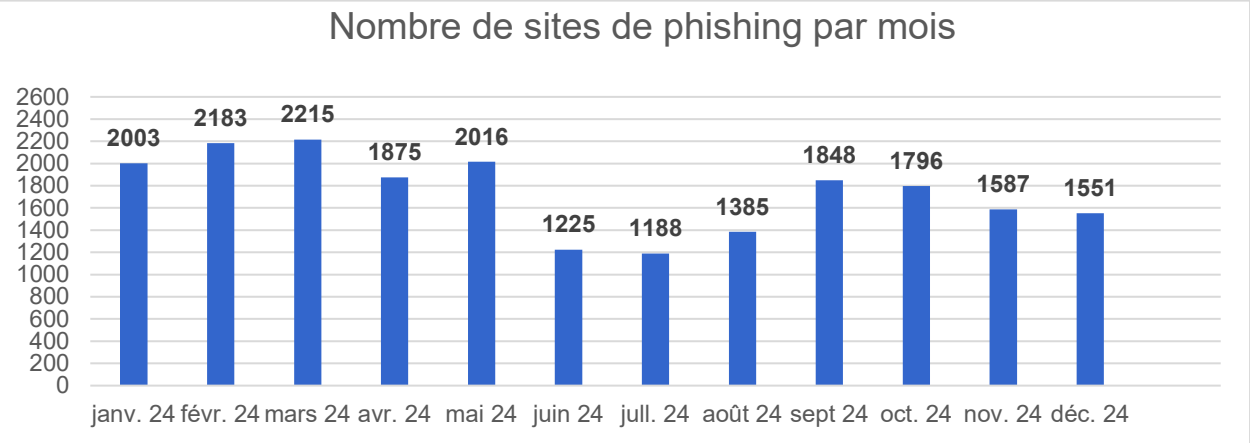

Illustration 2 - Nombre de sites de phishing par mois

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

Avec 98%, une grande partie des communications de soupçons provenait de la population et des PME. Un pour cent des communications provenait d'exploitants d'infrastructures critiques ou du OFCS lui-même. Il convient toutefois de noter qu'une grande partie des sites web signalés par les infrastructures critiques sont effectivement des sites de phishing. A l'inverse, les messages émanant de la population et des PME ne sont généralement pas des hameçonnages, mais des spams ou des newsletters légitimes. Il existe donc une grande différence entre les messages de la population et ceux des exploitants d'infrastructures critiques en ce qui concerne la question de savoir s'il s'agit effectivement de sites de phishing.

Les sites de phishing identifiés en 2024 abusaient **de 338 noms de marque différents**, **63,9% des sites de phishing signalés** abusant de **noms de marque suisses** et 31,1% de noms de marques étrangères. 5% des sites de phishing n'utilisaient pas de noms de marque explicites. Il s'agit en grande partie de sites de phishing génériques qui cherchent à inciter la victime à divulguer ses données d'accès à la messagerie

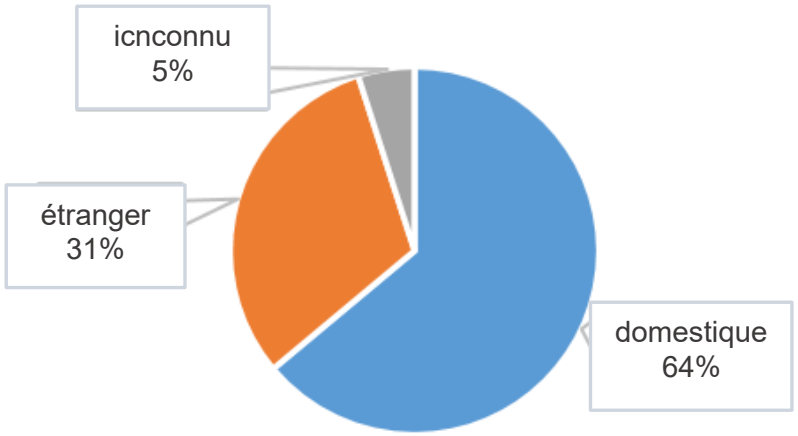

Illustration 3 - Compétence des noms de marque abusés

Alors qu'en 2023, la marque de la Poste Suisse était encore dans la ligne de mire des cybercriminels**, c'est le nom de marque de l'Alliance SwissPass qui a été le plus utilisé par les cybercriminels pour le phishing** en 2024**, avec 22%**. Avec les fournisseurs étrangers, les sites de phishing qui utilisent les noms de marque de fournisseurs de lettres et de colis connus ne représentent plus que 21%. Pour une grande partie des sites de phishing, les cybercriminels ne visaient pas les plates-formes des fournisseurs. Ce sont plutôt leurs noms de marque qui ont été utilisés comme appât pour obtenir des données de cartes de crédit. Des frais de livraison de colis ou de douane sont prétendument perçus auprès des livreurs de lettres et de colis. Ces frais doivent ensuite être réglés par carte de crédit. En réalité, la victime ne s'acquitte pas de ces frais, mais est victime de phishing par carte de crédit.

La situation est différente pour les sites de phishing qui utilisent abusivement des noms de marque d'établissements financiers. **En 2024, 17 % des sites de phishing ont utilisé des noms de marque de banques, d'émetteurs de cartes de crédit ou de prestataires de paiement en ligne**. Dans de nombreux cas, les cybercriminels ont tenté d'obtenir des données d'accès à des portails d'e-banking par exemple, en utilisant des portails de connexion falsifiés. L'utilisation abusive du nom de marque de TWINT pour obtenir des informations sur les cartes de crédit des victimes a également été très appréciée.

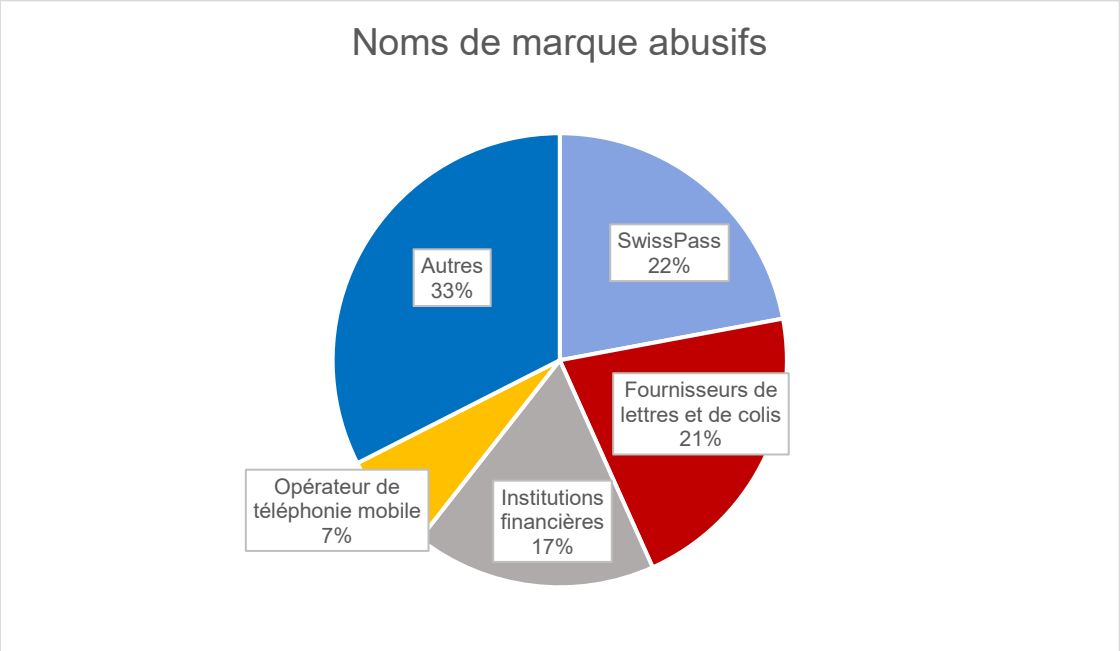

Illustration 4 – Noms de marque abusifs

Une grande partie des sites de phishing étaient exploités sur des domaines de premier niveau (TLD) étrangers. Près de la moitié des sites de phishing identifiés étaient mis à disposition sur les gTLDs[3] « .com » et « .me ». Contrairement au ccTLD[4] « .ch », l'ordonnance sur les domaines Internet (VID)[5] n'est pas applicable ici, ce qui prive le OFCS ainsi que d'autres autorités en Suisse de la possibilité d'agir efficacement contre le phishing dans ces gTLD.

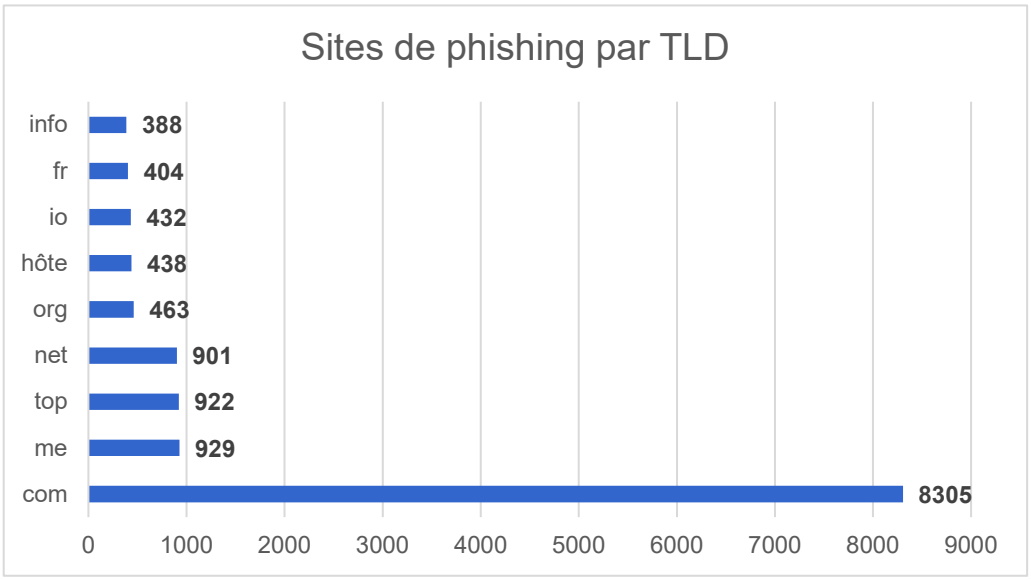

Illustration 5 - Domaine de premier niveau (TLD) avec le plus grand nombre de pages Web de phishing

[3] Domaine générique de premier niveau

[4] Code du pays Domaine de premier niveau

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

Pour mettre à disposition des sites Web d'hameçonnage, les cybercriminels ont notamment recours à des sites Web piratés. Mais il n'est pas rare qu'ils enregistrent eux-mêmes directement des noms de domaine dédiés dans le seul but de mettre à disposition des sites de phishing. **En 2024, le OFCS a identifié 140 sites de phishing dont les noms de domaine étaient enregistrés dans le ccTLD « .ch ». Parmi eux, 57 noms de domaine ont été présumés être enregistrés directement par des cybercriminels à des fins exclusivement frauduleuses.** Cela représente une augmentation de plus de 50% des enregistrements frauduleux de noms de domaine dans la zone ccTLD « .ch ». Les noms de domaine concernés ont été bloqués techniquement et administrativement auprès de l'exploitant du registre (Domain-Registry) sur la base de l'ordonnance sur les domaines Internet (ODI), art. 15, à la demande du OFCS.

Avec 28 %, une grande partie des pages Web de phishing a été mise à disposition par le réseau de diffusion de contenu (CDN) de Cloudflare. Celui-ci stocke temporairement les contenus des pages Web (mise en cache) et dissimule le serveur réel sur lequel sont stockés les contenus d'hameçonnage proprement dits. Il n'est donc pas étonnant que les cybercriminels utilisent volontiers ce service pour mettre à disposition leurs pages Web d'hameçonnage.

Le tableau suivant montre le classement des opérateurs de réseau chez lesquels le plus grand nombre de pages web de phishing a été mis à disposition en 2024.

Rang	Sites de phishing	En pourcentage	Opérateur de réseau	Pays
1	6010	28%	Cloudflare	ÉTATS-UNIS
2	1205	5%	Google	ÉTATS-UNIS
3	1102	5%	BlueHost	ÉTATS-UNIS
4	1004	4%	GoDaddy	ÉTATS-UNIS
5	920	4%	Amazon	ÉTATS-UNIS
6	616	3%	DigitalOcean	ÉTATS-UNIS
7	527	2%	Microsoft	ÉTATS-UNIS
8	394	2%	Endurance	ÉTATS-UNIS
9	393	2%	HostGator	ÉTATS-UNIS
10	373	2%	OVH	France

Les cybercriminels apprécient également les fournisseurs de plateformes Internet mises gratuitement à disposition. Le tableau suivant montre les plateformes Internet et leurs exploitants sur lesquels le OFCS 2024 a identifié le plus grand nombre de contenus d'hameçonnage.

Rang	Sites de phishing	Nom de domaine	Fournisseur	Pays
1	793	mybluehost.me	Bluehost	ÉTATS-UNIS
2	536	blogspot.com	Google	ÉTATS-UNIS
3	416	sviluppo.host	n/a	Italie
4	245	codeanyapp.com	Codeanywhere	ÉTATS-UNIS
5	181	secureserver.net	GoDaddy	ÉTATS-UNIS
6	170	web.app	cyber_Folks	Pologne
7	165	pages.dev	Cloudflare	ÉTATS-UNIS
8	127	cloudflare-ipfs.com	Cloudflare	ÉTATS-UNIS
9	118	cprapid.com	cPanel	ÉTATS-UNIS
10	95	web.app	Google	ÉTATS-UNIS

4 Autres types de phishing

4.1 Faux portail d'amendes

La numérisation progresse, y compris dans l'environnement administratif. Ainsi, diverses démarches administratives peuvent désormais être effectuées par voie numérique. Dans certains cantons, un portail permet par exemple de régler en ligne les amendes de stationnement ou pour excès de vitesse. Les cybercriminels en ont également pris connaissance et abusent de la crédibilité de ces portails pour obtenir des données de cartes de crédit. Par exemple, 30 sites de phishing imitant le portail des amendes de la police lucernoise ont été signalés au OFCS 2024.

Illustration 6 - Portail des amendes falsifiées

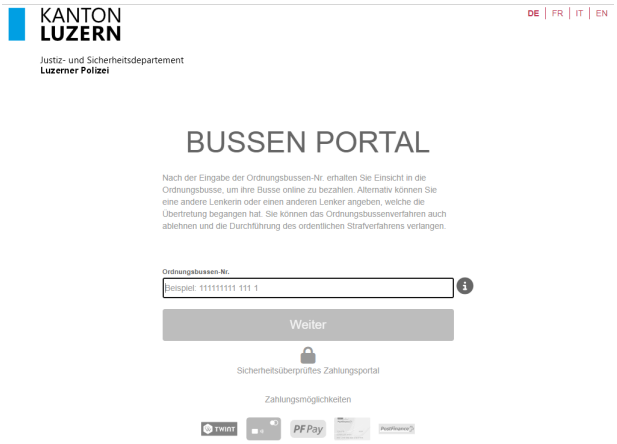

Illustration 7 - Portail des amendes légitimes

4.2 Remboursements présumés de l'AVS

En 2024, des cybercriminels ont également abusé de la notoriété de l'assurance vieillesse et survivants (AVS) pour faire du phishing. Sous le prétexte d'un remboursement AVS de 370,72 CHF, ils ont tenté d'obtenir les données des cartes de crédit de citoyens. Pour ce faire, les cybercriminels ont enregistré des noms de domaine correspondants afin de faire croire à la victime qu'elle se trouvait sur le site officiel de l'AVS.

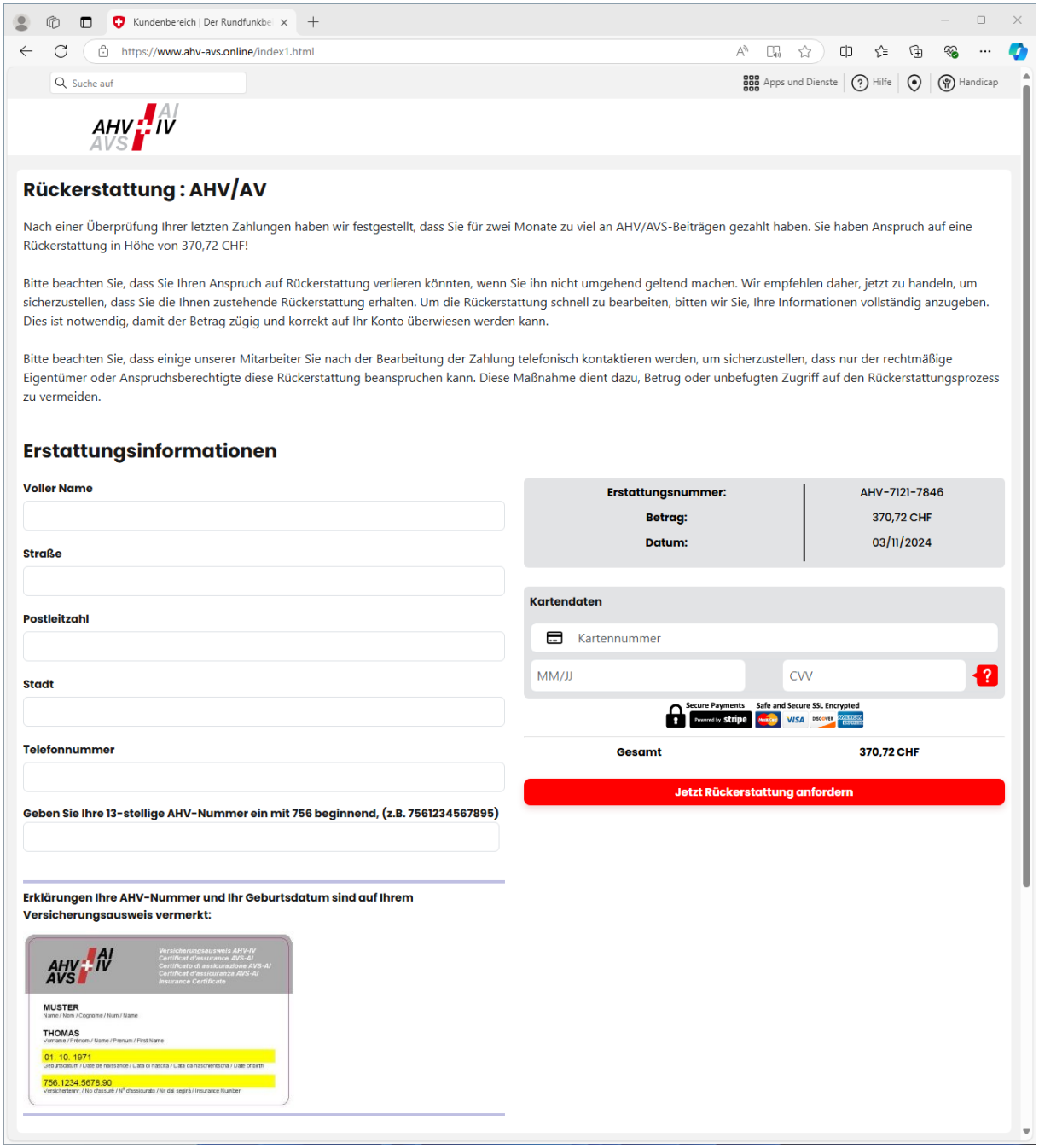

Illustration 8 - Faux site web AVS

5 Recommandations

Soyez toujours sceptique face aux e-mails et aux SMS qui tentent de vous inciter à cliquer sur un lien. En outre, le OFCS recommande ce qui suit :

- **Signalement à la OFCS:** signalez à la OFCS les e-mails ou les sites web suspects sur antiphishing.ch. Si vous souhaitez un retour sur votre signalement, utilisez comme alternative le formulaire de signalement sur https://www.report.ncsc.admin.ch/ ;

- **Soyez sceptique** : aucune banque ni aucun établissement de cartes de crédit ne vous demandera jamais de changer de mot de passe ou de vérifier les données de votre carte de crédit par e-mail ou par SMS ;

- **Authentification multi-facteurs (MFA) :** Dans la mesure du possible, activez l'authentification multifactorielle (MFA) sur vos comptes en ligne tels que la messagerie électronique ou les médias sociaux. Vérifiez dans les paramètres de votre compte auprès du fournisseur si la MFA est proposée et activez cette option ;

- **Utilisation multiple de mots de passe :** n'utilisez jamais le même mot de passe pour plusieurs comptes en ligne. Utilisez un gestionnaire de mots de passe pour gérer vos données d'accès ;

- **Décompte de carte de crédit :** vérifiez régulièrement votre décompte de carte de crédit pour voir s'il y a des incohérences et contactez immédiatement votre fournisseur de carte de crédit en cas de transactions inconnues ;

- **Filtre SMS :** activez le filtre SMS de votre système d'exploitation sur votre smartphone afin de filtrer les SMS suspects ;

- **Utilisation des favoris :** Pour accéder régulièrement à des comptes en ligne tels que l'e-banking, les médias sociaux ou le courrier électronique, utilisez la fonction « Favoris » de votre navigateur web ;

- **Usurpation d'identité :** n'oubliez pas qu'il est facile de falsifier les expéditeurs d'e-mails et de SMS, mais aussi les numéros de téléphone des appels entrants. En cas de doute, exigez de pouvoir rappeler l'appelant. Cherchez les numéros de téléphone correspondants sur Internet et ne vous fiez pas aux numéros indiqués dans les signatures d'e-mails, etc.