January 16, 2025 | National Cyber Security Centre NCSC

Anti-Phishing Report 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defense,
Civil Protection and Sport DDPS
National Cyber Security Centre NCSC

Contents

1 Introduction

The federal government has been operating the "antiphishing.ch" platform for almost 10 years. This was launched in 2014 and is operated by the National Cyber Security Centre NCSC. It offers the Swiss population as well as organizations, authorities and SMEs the opportunity to report suspicious websites and emails. The platform is used to identify websites that attempt to obtain sensitive data under false pretenses. This may involve access data for email, e-banking or social media accounts, for example, or even credit card information (known as "phishing"). The fraudsters exploit the good faith and helpfulness of their victims by sending them emails with (often) fake sender addresses and well-known company logos, for example.

Suspicious e-mails or websites can be reported on the antiphishing.ch website. Suspicious e-mails can also be forwarded directly to reports@antiphishing.ch[1] . This mailbox is not read, but processed automatically. There is therefore no reply to the sender. Reporting parties who wish to receive feedback from the NCSC can report phishing e-mails and suspicious websites to the NCSC using the reporting form for all cyber incidents. Thanks to the numerous reports from the public, SMEs and operators of critical infrastructure, the Confederation has been able to identify over **79,000 phishing websites** to date together with partner organizations and initiate appropriate countermeasures.

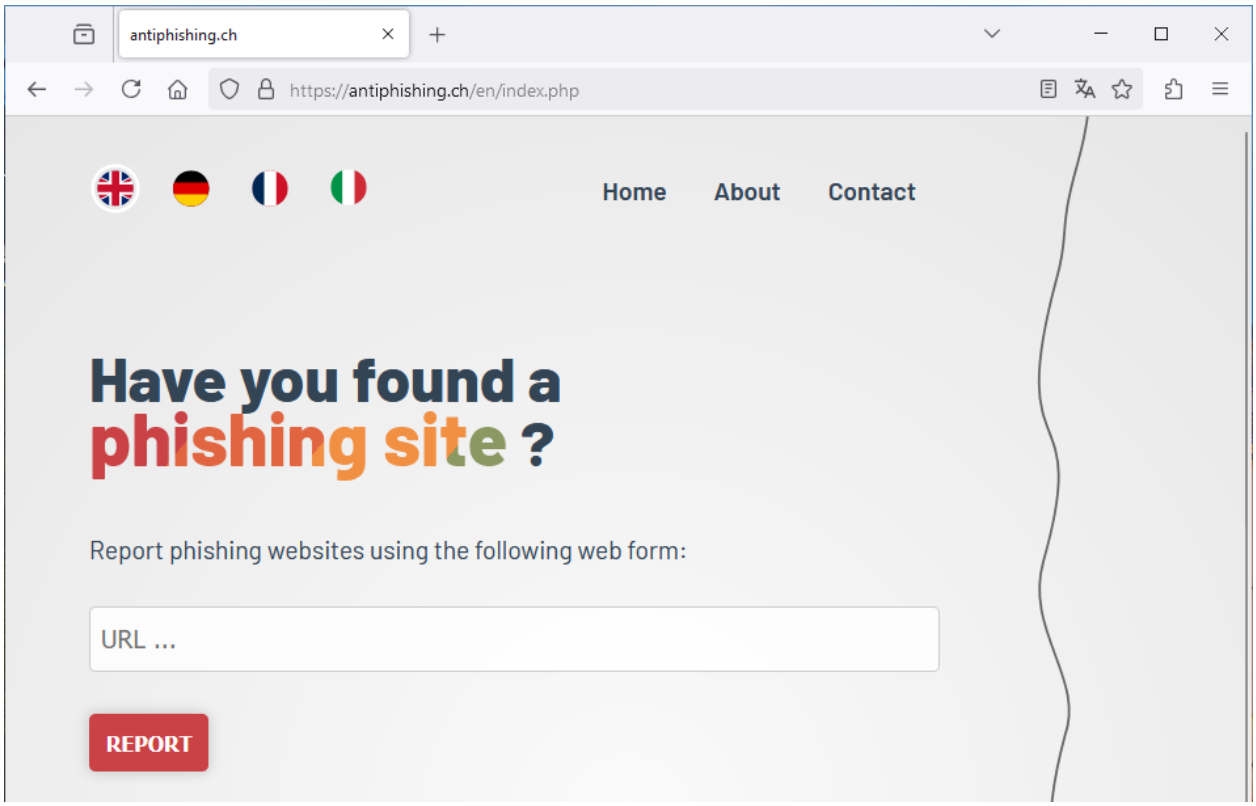

Figure 1 - "antiphishing.ch" platform of the NCSC

[1] reports@antiphishing.ch

2 What does the NCSC do with phishing messages?

Reports submitted via antiphishing.ch are subjected to an automated preliminary check. Many websites are reported to the NCSC several times, which is why phishing URLs that have been reported several times are filtered out first. Publicly accessible metadata is then collected, such as the provider of the suspected phishing website. In addition, a screenshot of the reported website is automatically created. This helps the NCSC analysts to assess whether the reported website is actually a phishing website. At the end of the process, each report is manually reviewed and assessed by analysts.

If a website is identified as phishing by the analyst, the NCSC sends an abuse complaint. This is sent by email to the web hosting provider, the domain registrar and the domain holder ("registrant"). Wherever possible, NCSC also informs the owner of the trademark that is being misused by the cybercriminals for the phishing campaign.

As with many cyber threats, national and international exchange is also an important factor in phishing. The NCSC therefore provides internet providers, spam filter manufacturers and web browser manufacturers with up-to-date technical information on current phishing websites. The exchange of information in the international Anti-Phishing Working Group (APWG)[2] is also an important cornerstone in the fight against phishing.

3 The most important figures for 2024

In the year 2024, a total of **975,309 reports** were submitted via the "antiphishing.ch" platform. This corresponds to a 79% increase in suspicious activity reports compared to the previous year (544,367 reports). After filtering out multiple phishing URLs, **20,872 websites were identified as phishing websites** from the reports. This corresponds to an increase of 108% compared to the previous year (10,007). With 2,215 phishing websites, the most phishing websites in 2024 were identified in March. In July, the most suspicious activity reports were submitted to the NCSC with 235,310 reports.

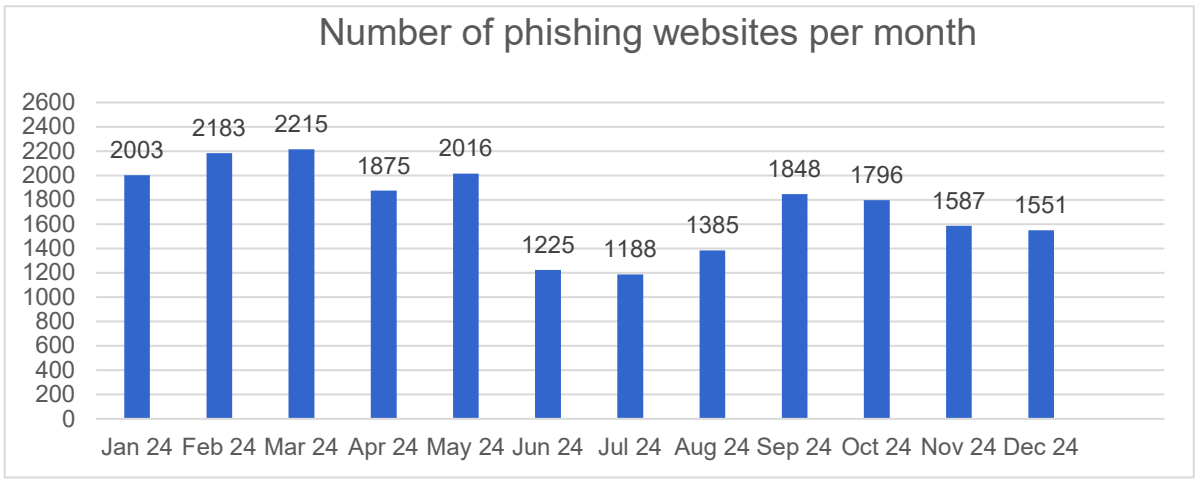

Figure 2 - Number of phishing websites per month

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

At 98%, the majority of suspicious activity reports came from the general public and SMEs. In each case, 1% of the reports came from operators of critical infrastructures or from the NCSC itself. However, it should be noted that a large proportion of the websites reported by critical infrastructures are actually phishing. This contrasts with reports from the general public and SMEs, most of which are not phishing, but spam or legitimate newsletters, for example. There is therefore a big difference between reports from the general public and those from critical infrastructure operators in terms of whether they are actually phishing websites.

The phishing websites identified in 2024 misused **338 different brand names**, with **63.9% of the reported phishing websites misusing Swiss brand names** and 31.1% misusing names of foreign brands. 5% of the phishing websites did not abuse any explicit brand names. For the most part, these are generic phishing websites that try to trick the victim into disclosing their e-mail access data

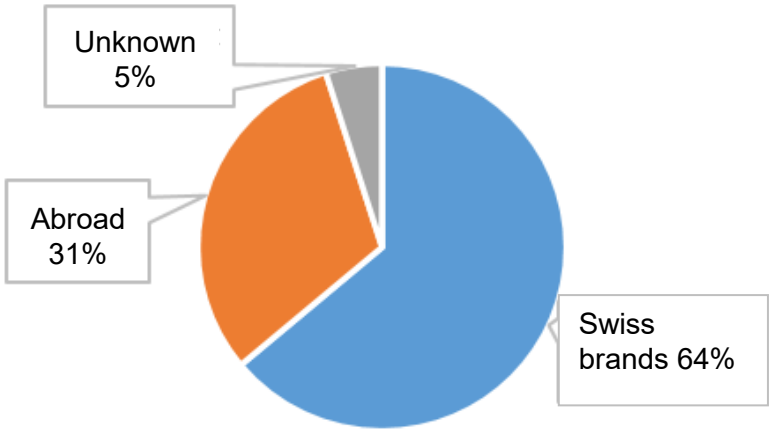

Figure 3 - Responsibility of the misused brand names

While the Swiss Post brand was still the focus of cybercriminals in 2023**, the brand name of the Alliance SwissPass was the most abused by cybercriminals for phishing** in 2024**, accounting for 22%**. Together with foreign providers, phishing websites that misuse the brand names of well-known letter and parcel delivery companies only account for 21%. For the majority of phishing websites, however, it was not the providers' platforms that were targeted by the cybercriminals. Instead, their brand names were used as bait to obtain credit card data. Alleged parcel delivery or customs fees are collected from the mail and parcel delivery companies. These fees are then supposed to be paid by credit card. In reality, however, the victim does not pay any fees, but becomes a victim of credit card phishing.

However, the picture is different for phishing websites that misused the brand names of financial institutions. **In 2024, 17% of all phishing websites misused the brand names of banks, credit card issuers or online payment providers**. In many cases, cyber criminals used fake login portals in an attempt to gain access to e-banking portals, for example. The misuse of the TWINT brand name to obtain victims' credit card information was also popular.

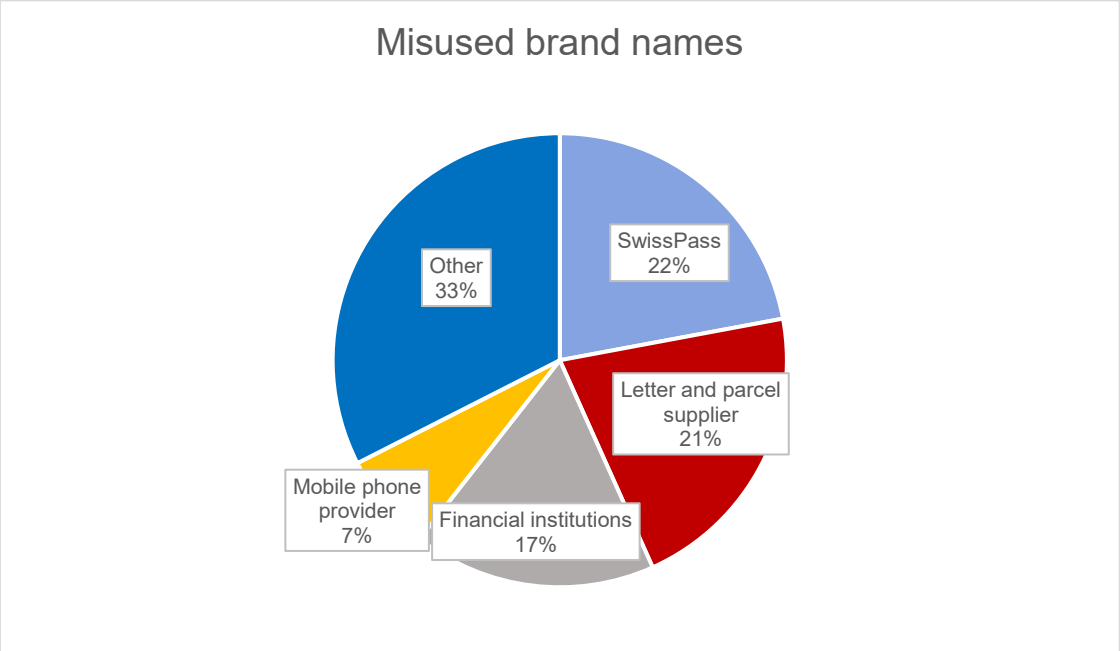

Figure 4 – Misused brand names

The majority of phishing websites were operated on foreign top-level domains (TLDs). Almost half of all identified phishing websites were hosted on the gTLDs[3] ".com" and ".me". Unlike the ccTLD[4] ".ch", the Ordinance on Internet Domains (OID)[5] does not apply here, which means that the NCSC and other authorities in Switzerland are unable to take effective action against phishing in these gTLDs.

[3] Generic top-level domain

[4] Country code top-level domain

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

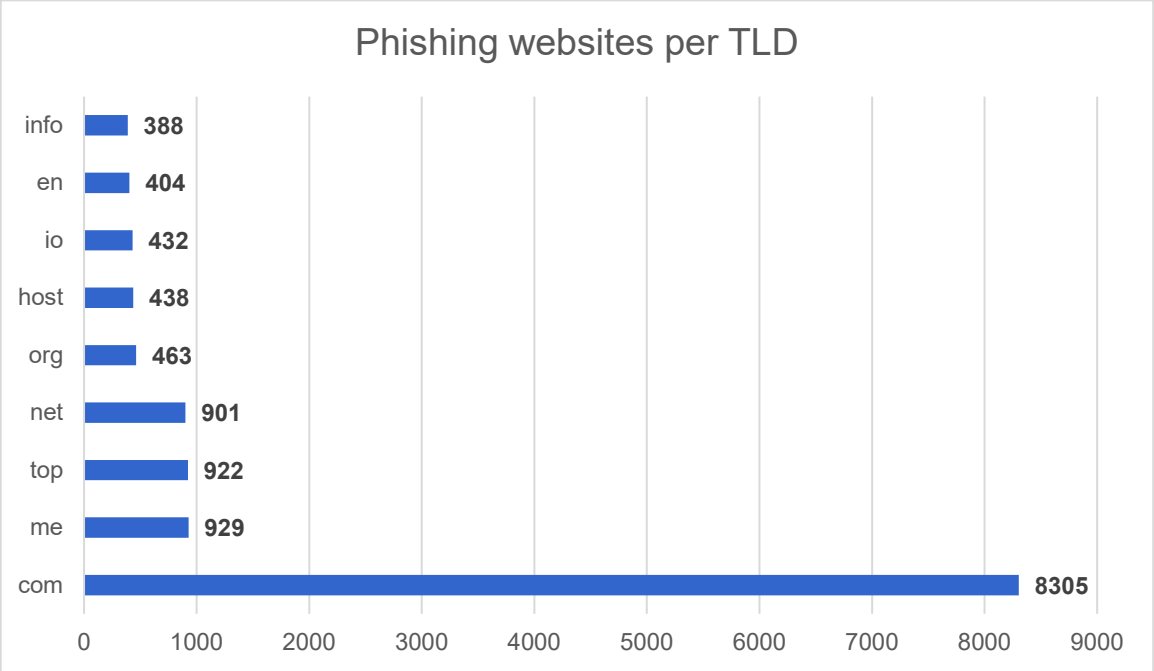

Figure 5 - Top level domain (TLD) with the most phishing websites

To provide phishing websites, cyber criminals use hacked websites, among other things. However, they also often register dedicated domain names themselves for the sole purpose of providing the phishing websites. **In 2024, the NCSC identified 140 phishing websites whose domain names were registered in the ccTLD ".ch". Of these, 57 domain names were allegedly registered directly by cybercriminals for exclusively fraudulent purposes.** This is an increase in fraudulent domain registrations in the ".ch" ccTLD zone of over 50%. The domain names concerned were technically and administratively blocked at the request of the NCSC by the registry operator (domain registry) on the basis of Art. 15 of the Ordinance on Internet Domains (OID).

At 28%, the majority of phishing websites were provided by Cloudflare's content delivery network (CDN). This temporarily stores website content (caching) and disguises the actual server on which the actual phishing content is stored. It is therefore not surprising that cyber criminals like to use this service to provide their phishing websites.

The following table shows the ranking of network operators that hosted the most phishing websites in 2024.

Rank	Phishing sites	In %	Network operator	Country
1	6010	28%	Cloudflare	USA
2	1205	5%	Google	USA
3	1102	5%	BlueHost	USA
4	1004	4%	GoDaddy	USA
5	920	4%	Amazon	USA
6	616	3%	DigitalOcean	USA
7	527	2%	Microsoft	USA

8	394	2%	Endurance	USA
9	393	2%	HostGator	USA
10	373	2%	OVH	France

Providers of free internet platforms are also popular with cybercriminals. The following table shows the internet platforms and their operators on which the NCSC 2024 identified the most phishing content.

Rank	Phishing sites	Domain name	Provider	Country
1	793	mybluehost.me	Bluehost	USA
2	536	blogspot.com	Google	USA
3	416	sviluppo.host	n/a	Italy
4	245	codeanyapp.com	Codeanywhere	USA
5	181	secureserver.net	GoDaddy	USA
6	170	web.app	cyber_Folks	Poland
7	165	pages.dev	Cloudflare	USA
8	127	cloudflare-ipfs.com	Cloudflare	USA
9	118	cprapid.com	cPanel	USA
10	95	web.app	Google	USA

4 Other types of phishing

4.1 Fake bus portal

Digitalization is advancing, also in the public authority environment. Various administrative procedures can now also be completed digitally. In some cantons, parking fines or speeding fines, for example, can now be paid online via a portal. Cyber criminals have also taken note of this and are abusing the credibility of such portals to obtain credit card data. For example, 30 phishing websites imitating the Lucerne police's fines portal were reported to the NCSC in 2024.

Figure 6 - Fake bus portal

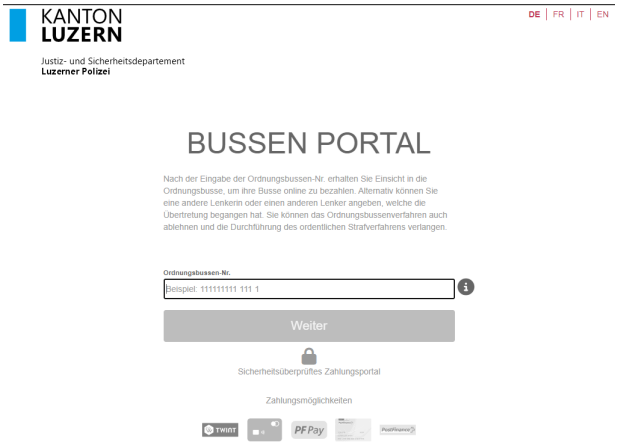

Figure 7 - Legitimate fines portal

4.2 Alleged AHV refunds

In 2024, cyber criminals also misused the reputation of the Old Age and Survivors' Insurance (AHV) for phishing. Under the pretext of an AHV refund of CHF 370.72, attempts were made to obtain citizens' credit card details. To this end, the cybercriminals registered corresponding domain names to trick the victim into believing they were on the official AHV website.

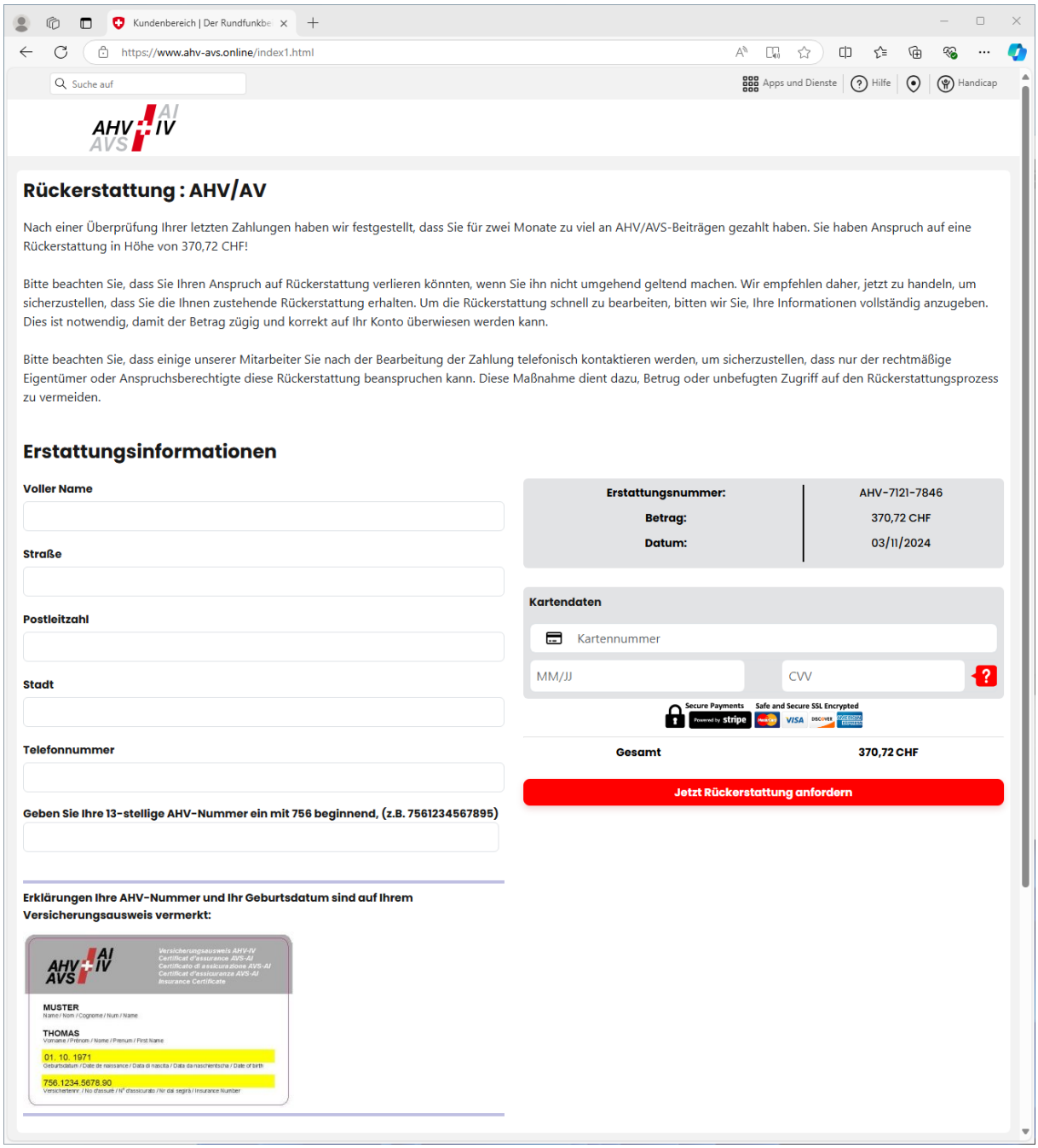

Figure 8 - Fake AHV website

5 Recommendations

Always be skeptical of e-mails and text messages that try to persuade you to click on a link. The NCSC also recommends the following:

- **Report to the NCSC:** Report suspicious e-mails or websites to the NCSC on antiphishing.ch. If you would like feedback on your report, please use the report form at https://www.report.ncsc.admin.ch/ as an alternative;

- **Be skeptical**: No bank or credit card company will ever ask you to change passwords or verify credit card details by e-mail or text message;

- **Multi-factor authentication (MFA):** Enable multi-factor authentication (MFA) on your online accounts such as email or social media whenever possible. Check your account settings with the provider to see whether MFA is offered and activate this option;

- **Multiple use of passwords:** Never use the same password for several online accounts. Use a password manager to manage your access data;

- **Credit card statement:** Check your credit card statement regularly for discrepancies and contact your credit card provider immediately in the event of unknown transactions;

- **SMS filter:** Activate the SMS filter of your operating system on your smartphone to filter suspicious SMS;

- **Use of favorites:** Use the favorites function ("bookmarks") of your web browser for regular access to online accounts such as e-banking, social media or e-mail;

- **Spoofing:** Bear in mind that senders of e-mails and text messages as well as phone numbers of incoming phone calls are easy to spoof. If in doubt, ask to be able to call the caller back. Look up the relevant telephone numbers on the Internet and do not rely on numbers given in e-mail signatures etc.