16 Gennaio 2025 | Ufficio federale della cibersicurezza UFCS

Rapporto anti-phishing 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della cibersicurezza UFCS

Contenu

1 Introduzione 3

2 Cosa fa l'UFCS con i messaggi di phishing? 4

3 Cifre chiave per il 2024 4

4 Altri tipi di phishing 9

4.1 Falsi portali di multa 9

4.2 Rimborso presunto dell'AVS 10

5 Raccomandazioni 11

1 Introduzione

Da quasi 10 anni la Confederazione gestisce la piattaforma «antiphishing.ch». È stata lanciata nel 2014 ed è gestita dall'Ufficio federale della cibersicurezza (UFCS). Essa offre al pubblico svizzero, così come alle organizzazioni, alle autorità e alle PMI, l'opportunità di segnalare siti web ed e-mail sospetti. La piattaforma viene utilizzata per identificare i siti web che tentano di accedere a dati sensibili con un pretesto. Tra questi potrebbero esserci i dati di accesso agli account di posta elettronica, e-banking o social media, oppure i dati delle carte di credito (il cosiddetto «phishing»). I truffatori approfittano della credulità e della disponibilità delle loro vittime, ad esempio inviando loro e-mail con indirizzi di mittente (spesso) falsificati e loghi aziendali ben noti.

Le e-mail o i siti web sospetti possono essere segnalati al sito web antiphishing.ch. Le e-mail sospette possono anche essere inoltrate direttamente all'indirizzo reports@antiphishing.ch[1]. Questa casella di posta non viene letta, ma elaborata da una macchina. Pertanto, non è prevista alcuna risposta al mittente. Chiunque desideri ricevere un riscontro dall'UFCS può segnalare le e-mail di phishing e i siti web sospetti tramite il modulo di segnalazione per tutti gli incidenti informatici. Grazie al gran numero di segnalazioni fatte dal pubblico, dalle PMI e dai gestori di infrastrutture critiche, la Confederazione, in collaborazione con le organizzazioni partner, è stata finora in grado di identificare più di 79.000 siti web di phishing e di adottare contromisure adeguate.

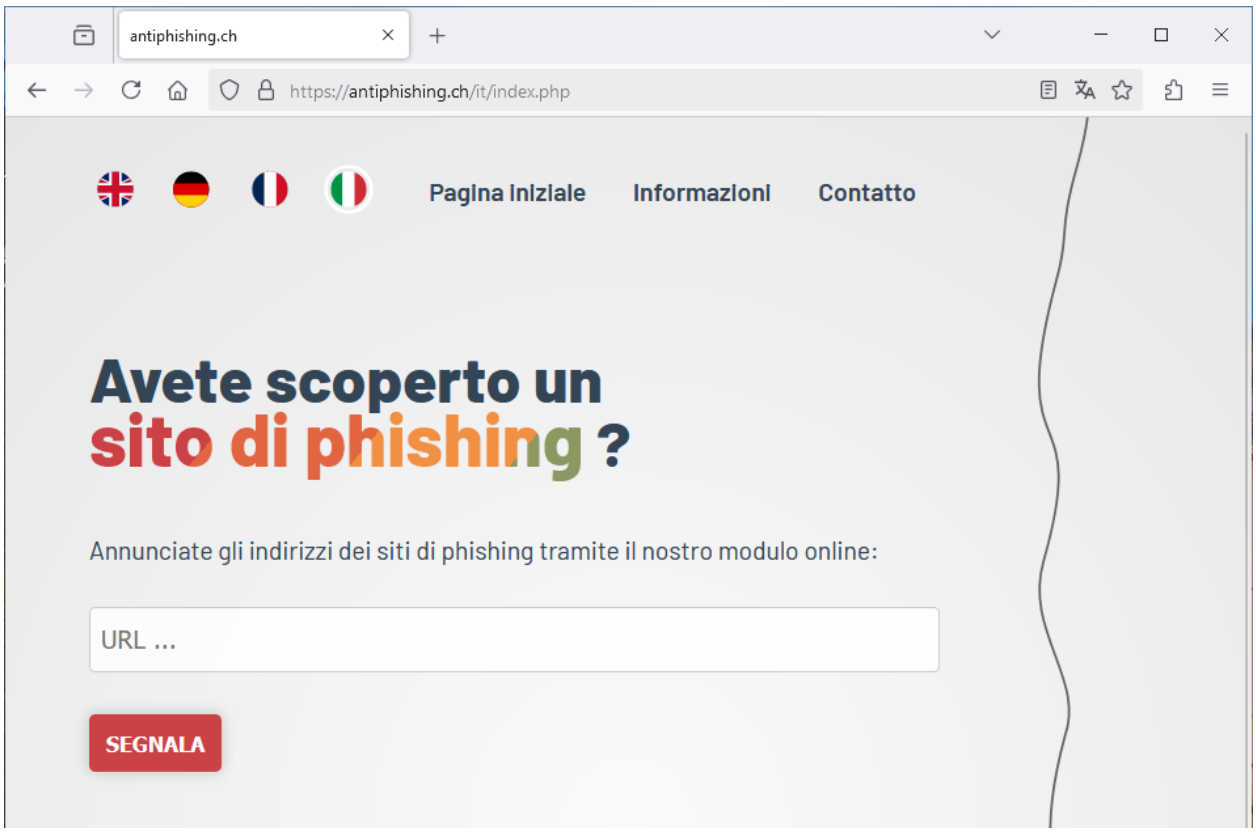

Figura 1 - Piattaforma «antiphishing.ch» dell'UFCS

[1] reports@antiphishing.ch

2 Cosa fa l'UFCS con i messaggi di phishing?

I messaggi inviati tramite antiphishing.ch sono sottoposti a un controllo automatico. Molti siti web vengono segnalati più volte all'UFCS, per questo motivo gli URL di phishing segnalati più volte vengono prima filtrati. Successivamente, vengono raccolti i metadati disponibili pubblicamente, come ad esempio il provider che mette a disposizione il sito web sospetto di phishing. Inoltre, viene automaticamente eseguito uno screenshot del sito web segnalato. Questo aiuta gli analisti dell'UFCS a determinare se il sito segnalato è effettivamente un sito di phishing. Al termine del processo, ogni notifica viene esaminata e valutata manualmente dagli analisti.

Se un sito web viene identificato come phishing dall'analista, l'UFCS invia un reclamo per abuso. Questa viene inviata per e-mail al provider di web hosting, al registratario del dominio e al proprietario del dominio («registrante»). Se possibile, l'UFCS informa anche il proprietario del marchio utilizzato dai criminali informatici nella campagna di phishing.

Come per molte minacce informatiche, lo scambio nazionale e internazionale è un fattore importante nel phishing. Per questo motivo, l'UFCS fornisce ai provider di servizi Internet, ai produttori di filtri antispam e ai produttori di browser web informazioni tecniche sui siti web di phishing attuali in tempo reale. Anche lo scambio all'interno dell'Anti-Phishing Working Group (APWG)[2] internazionale è un pilastro importante nella lotta al phishing.

3 Cifre chiave per il 2024

Nel 2024 sono state inviate **975'309 segnalazioni** tramite la piattaforma «antiphishing.ch». Ciò rappresenta un aumento del 79% del numero di segnalazioni rispetto all'anno precedente (544'367 segnalazioni). Dopo aver filtrato gli URL di phishing citati più volte, dai messaggi è stato possibile identificare **20'872 siti web come siti di phishing**. Ciò rappresenta un aumento del 108% rispetto all'anno precedente (10'007). Con 2'215 siti di phishing, marzo ha visto il maggior numero di siti di phishing identificati nel 2024. A luglio si è registrato il maggior numero di segnalazioni di attività sospette inviate all'UFCS, con 235'310 segnalazioni.

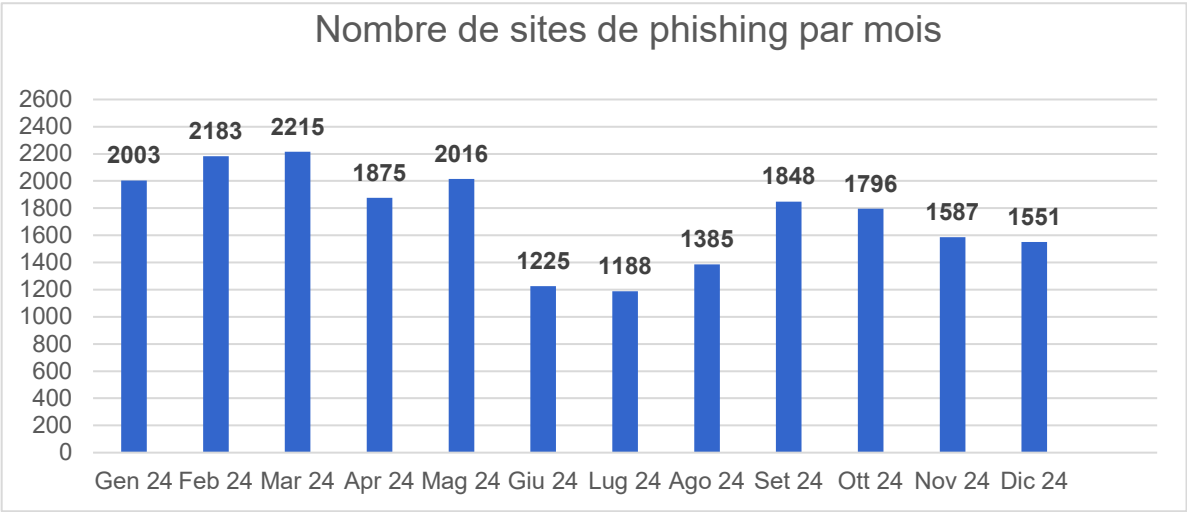

Figura 2 – Numero di siti di phishing per mese

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

Il 98% delle segnalazioni proviene dalla popolazione e dalle PMI. L'1% delle segnalazioni proviene da operatori di infrastrutture critiche o dallo stesso UFCS. Va notato, tuttavia, che gran parte dei siti web segnalati dalle infrastrutture critiche sono in realtà siti di phishing. Al contrario, i messaggi provenienti dalla popolazione e dalle PMI non sono generalmente phishing, ma spam o newsletter legittime. Esiste quindi una grande differenza tra i messaggi del grande pubblico e quelli degli operatori delle infrastrutture critiche in termini di effettiva presenza di siti di phishing.

Nel 2024 i siti di phishing identificati hanno abusato **di 338 marchi diversi, con il 63,9% dei siti di phishing segnalati** che hanno abusato **di marchi svizzeri** e il 31,1% di marchi stranieri. Il 5% dei siti di phishing non ha utilizzato nomi di marchi espliciti. Si tratta per lo più di siti di phishing generici che tentano di ingannare le vittime per indurle a divulgare i loro dati di accesso alla posta elettronica.

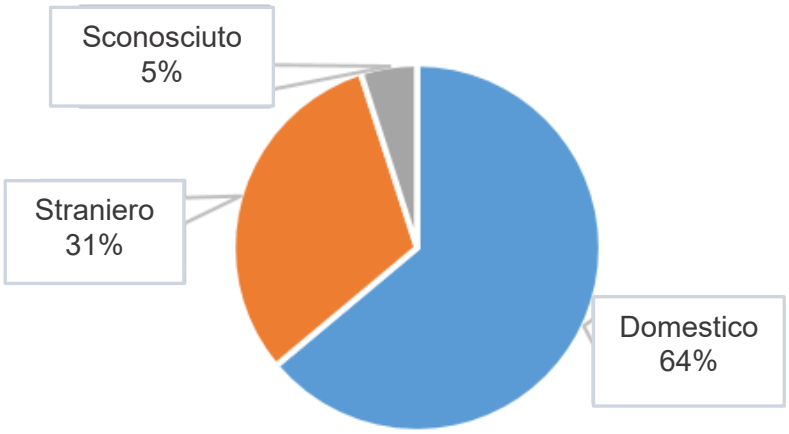

Figura 3 – Provenienza marchi abusati

Mentre nel 2023 il marchio più utilizzato dai criminali informatici era quello della Posta Svizzera, **nel 2024 è stato il marchio di SwissPass Alliance a essere utilizzato più frequentemente dai criminali informatici per il phishing, con una percentuale del 22%**. Insieme ai provider stranieri, i siti di phishing che utilizzano i marchi di noti fornitori di lettere e pacchi rappresentano solo il 21%. Per gran parte dei siti di phishing, i criminali informatici non hanno utilizzato le piattaforme dei fornitori. Hanno utilizzato però i loro marchi come esca per ottenere i dati delle carte di credito inducendo le persone a pagare finte spese di consegna dei pacchi o di spese doganali mediante carta di credito. In realtà, la vittima non paga queste spese, ma è vittima di phishing con carta di credito.

La situazione è diversa per i siti di phishing che utilizzano impropriamente i marchi delle istituzioni finanziarie. Nel 2024, il 17% dei siti di phishing ha utilizzato il marchio di banche, emittenti di carte di credito o fornitori di pagamenti online. In molti casi, i criminali informatici hanno cercato di ottenere i dati di accesso ai portali di e-banking, ad esempio utilizzando portali di login falsificati. Anche l'uso massiccio del marchio TWINT per ottenere i dati delle carte di credito dalle vittime è stato molto diffuso.

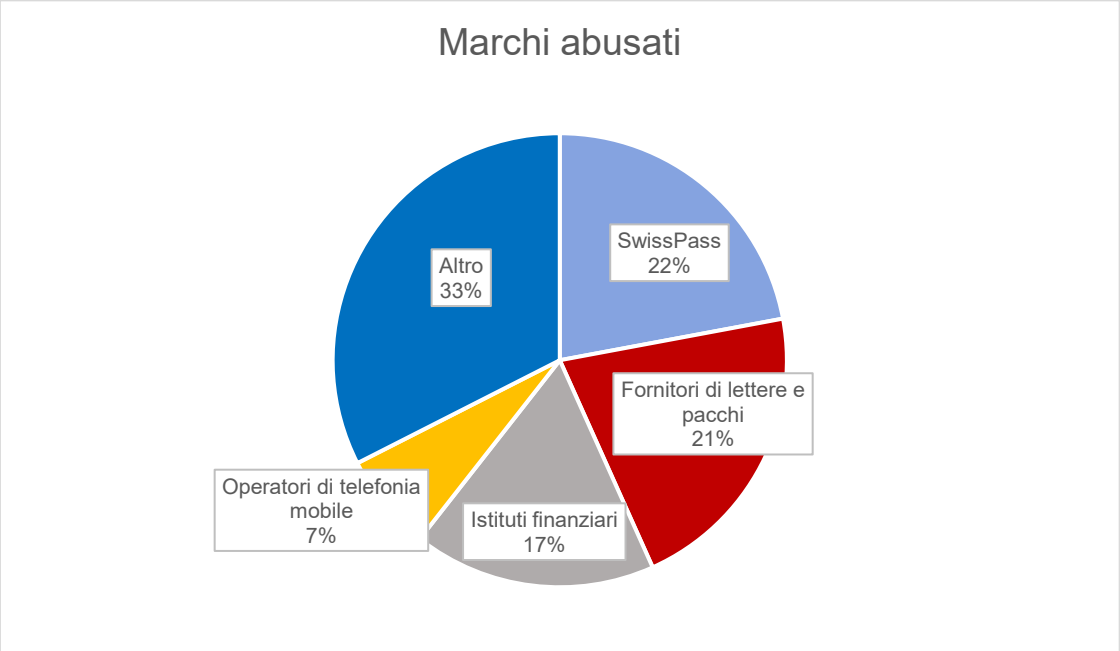

Figura 4 – Categorie dei marchi abusati in percentuale

Un'ampia percentuale di siti di phishing era gestita su domini di primo livello (TLD) stranieri. Quasi la metà dei siti di phishing identificati erano disponibili sui gTLDs[3] «.com» e «.me». A differenza del ccTLD[4] «.ch», in questo caso non si applica l'ordinanza sui domini Internet (VID)[5], il che significa che l'UFCS e le altre autorità svizzere non sono in grado di intervenire efficacemente contro il phishing in questi gTLDs.

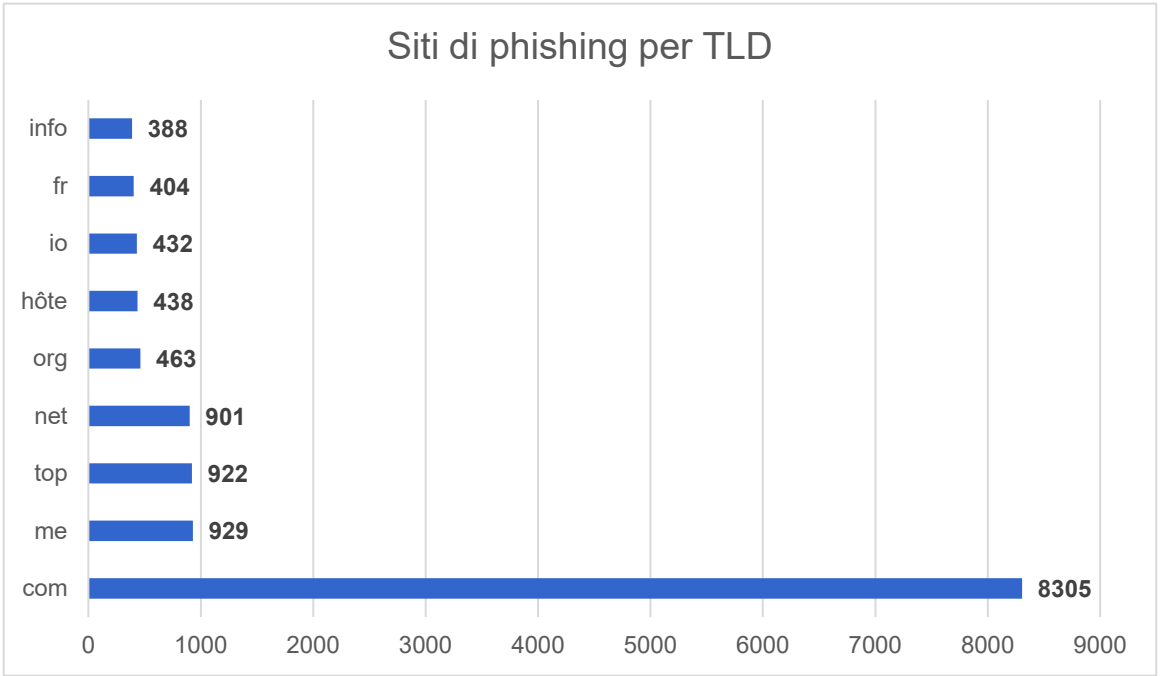

Figura 5 – Domini di primo livello (TLD) con il numero maggiore di Siti Web di phishing

[3] Generic Top Level Domain

[4] Country Code Top-Level-Domain

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

Per rendere disponibili i siti di phishing, i criminali informatici utilizzano spesso siti web compromessi. Ma non è raro che registrino essi stessi nomi di dominio dedicati al solo scopo di rendere disponibili siti web di phishing. **Nel 2024, l'UFCS ha identificato 140 siti di phishing con nomi di dominio registrati nel ccTLD ".ch". Di questi, si presume che 57 nomi di dominio siano stati registrati direttamente dai criminali informatici per scopi esclusivamente fraudolenti.** Ciò rappresenta un aumento di oltre il 50% delle registrazioni fraudolente di nomi di dominio nella zona del ccTLD ".ch". Su richiesta dell'UFCS, i nomi a dominio in questione sono stati bloccati tecnicamente e amministrativamente dal gestore del registro (Domain-Registry) sulla base dell'articolo 15 dell'ordinanza sui domini Internet (VID).

Il 28% dei siti web di phishing è stato reso disponibile tramite la rete di distribuzione dei contenuti (CDN) di Cloudflare. Questa rete memorizza temporaneamente il contenuto delle pagine web (caching) e nasconde il server effettivo su cui è memorizzato il contenuto di phishing. Non sorprende quindi che i criminali informatici utilizzino volentieri questo servizio per rendere disponibili i loro siti web di phishing.

La tabella seguente mostra quali operatori di rete hanno hostato il maggior numero di siti web di phishing nel 2024.

Rango	Siti di phishing	In percentuale	Operatore di rete	Paese
1	6010	28%	Cloudflare	Stati Uniti d'America
2	1205	5%	Google	Stati Uniti d'America
3	1102	5%	BlueHost	Stati Uniti d'America
4	1004	4%	GoDaddy	Stati Uniti d'America
5	920	4%	Amazon	Stati Uniti d'America
6	616	3%	DigitalOcean	Stati Uniti d'America
7	527	2%	Microsoft	Stati Uniti d'America
8	394	2%	Endurance	Stati Uniti d'America
9	393	2%	HostGator	Stati Uniti d'America
10	373	2%	OVH	Francia

Ai criminali informatici piacciono anche i fornitori di piattaforme Internet gratuite. La tabella seguente mostra le piattaforme Internet e i relativi operatori su cui l'UFCS nel 2024 ha individuato il maggior numero di contenuti di phishing.

Rango	Siti di phishing	Nome di dominio	Fornitore	Pays
1	793	mybluehost.me	Bluehost	Stati Uniti d'America
2	536	blogspot.com	Google	Stati Uniti d'America
3	416	sviluppo.host	n/a	Italia
4	245	codeanyapp.com	Codeanywhere	Stati Uniti d'America
5	181	secureserver.net	GoDaddy	Stati Uniti d'America
6	170	web.app	cyber_Folks	Polonia
7	165	pages.dev	Cloudflare	Stati Uniti d'America
8	127	cloudflare-ipfs.com	Cloudflare	Stati Uniti d'America
9	118	cprapid.com	cPanel	Stati Uniti d'America
10	95	web.app	Google	Stati Uniti d'America

4 Altri tipi di phishing

4.1 Falsi portali di multa

La digitalizzazione sta progredendo anche nell'ambiente amministrativo e diverse procedure amministrative possono ora essere eseguite digitalmente. In alcuni cantoni, ad esempio, un portale consente di pagare online le multe per divieto di sosta o per eccesso di velocità. I criminali informatici ne approfittano e stanno abusando della credibilità di questi portali per ottenere i dati delle carte di credito. Ad esempio, nel 2024, sono stati segnalati all'UFCS 30 siti di phishing che imitano il portale delle multe della polizia di Lucerna.

Figura 6 - Portale della multa falsificato

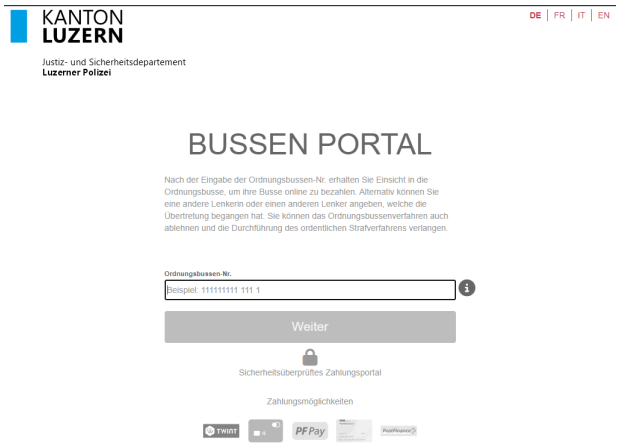

Figura 7 - Portale della multa legittimo

4.2 Rimborso presunto dell'AVS

Nel 2024, i criminali informatici hanno anche sfruttato la notorietà dell'Assicurazione per la vecchiaia e superstiti (AVS) per fare phishing. Con il pretesto di un rimborso AVS di 370,72 franchi, hanno cercato di ottenere i dati della carta di credito dei cittadini. A tal fine, i criminali informatici hanno registrato nomi di dominio simili per indurre la vittima a pensare di trovarsi sul sito ufficiale dell'AVS.

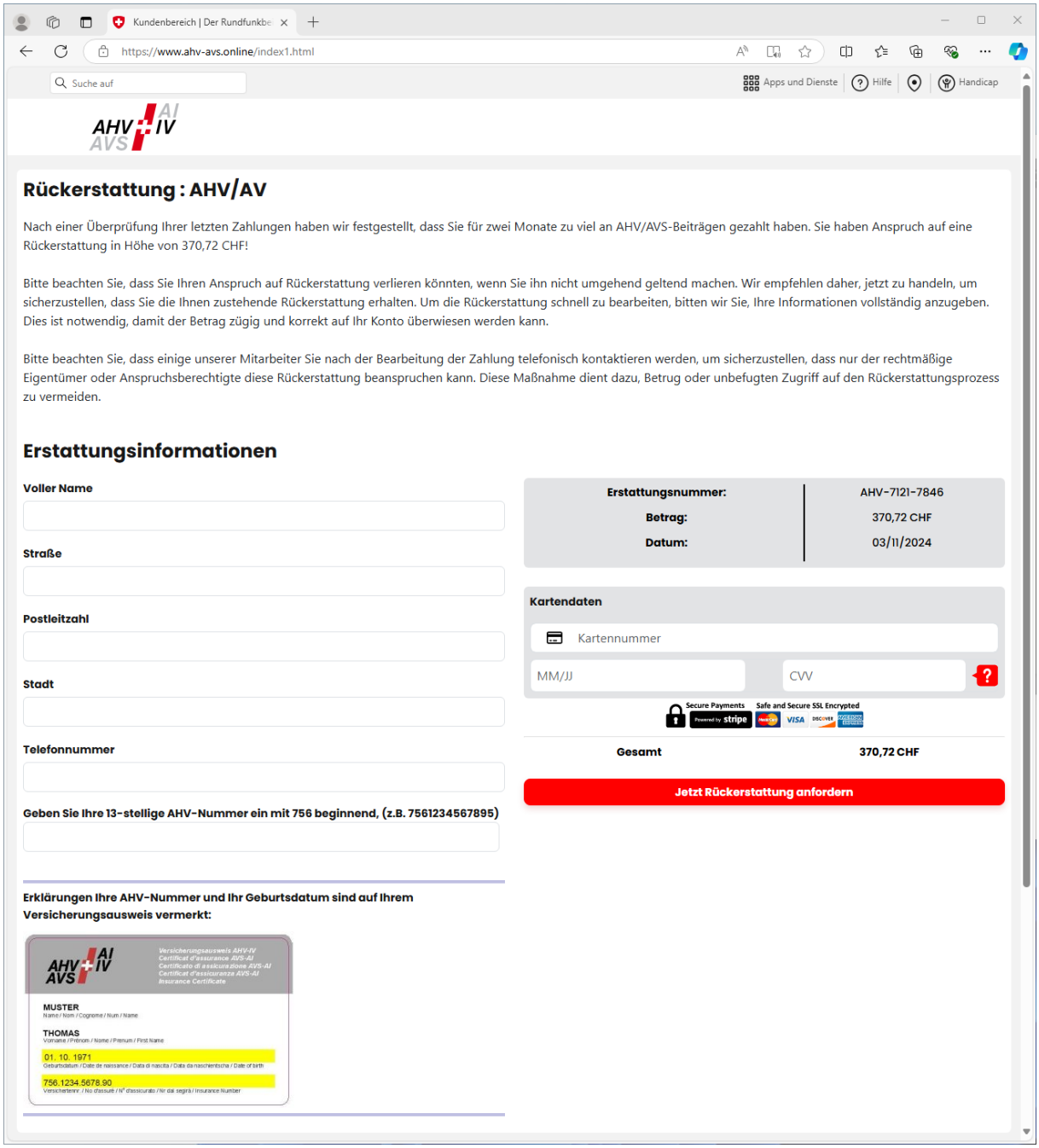

Figura 8 - Falso sito web AVS

5 Raccomandazioni

Siate sempre scettici nei confronti di e-mail e messaggi di testo che cercano di invogliarvi a cliccare su un link.

Inoltre, l'UFCS raccomanda quanto segue:

- **Segnalare all'UFCS**: segnalare e-mail o siti web sospetti all'UFCS all'indirizzo antiphishing.ch. Se desiderate un feedback sulla vostra segnalazione, potete utilizzare il modulo di segnalazione all'indirizzo https://www.report.ncsc.admin.ch/;
- **Siate scettici**: nessuna banca o società di carte di credito vi chiederà mai di cambiare la password o di controllare i dati della vostra carta di credito via e-mail o SMS;
- **Autenticazione a più fattori (MFA)**: ove possibile, attivate l'autenticazione a più fattori (MFA) sui vostri account online, come la posta elettronica o i social media. Controllate le impostazioni del vostro account con il provider per vedere se l'MFA è disponibile e attivate questa opzione;
- **Uso multiplo delle password**: non utilizzate mai la stessa password per diversi account online. Utilizzate un gestore di password per gestire i vostri dati di accesso;
- **Estratto conto della carta di credito**: controllare regolarmente l'estratto conto della carta di credito per verificare eventuali incongruenze e contattare immediatamente il fornitore della carta di credito in caso di transazioni sconosciute;
- **Filtro SMS**: attivate il filtro SMS del vostro sistema operativo sul vostro smartphone per filtrare gli SMS sospetti;
- **Uso dei preferiti**: per accedere regolarmente agli account online come l'e-banking, i social media o la posta elettronica, utilizzate la funzione «Preferiti» del vostro browser web;
- **Furto d'identità**: non dimenticate che è facile falsificare i mittenti di e-mail e SMS, nonché i numeri di telefono delle chiamate in entrata. In caso di dubbio, chiedete di poter richiamare il chiamante. Cercate i numeri di telefono corrispondenti su Internet e non fidatevi dei numeri riportati nelle firme delle e-mail, ecc.