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

29 gennaio 2024

Rapporto anti-phishing 2023

Introduzione

Da quasi dieci anni la Confederazione gestisce la piattaforma «antiphishing.ch», che è stata lanciata nel 2014 dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e dal 2020 viene gestita dal Centro nazionale per la cibersicurezza (NCSC), che il 1° gennaio 2024 è diventato l'Ufficio federale della cibersicurezza (UFCS). La piattaforma offre alla popolazione svizzera, ma anche a organizzazioni, autorità e PMI, la possibilità di segnalare pagine web ed e-mail sospette. L'obiettivo è di identificare le pagine web che attraverso un inganno tentano di ottenere dati sensibili, come i dati di accesso agli account di posta elettronica, e-banking o social media, o persino i dati delle carte di credito (il cosiddetto «phishing»). I truffatori sfruttano la buona fede e la disponibilità delle loro vittime e inviano loro e-mail con indirizzi e loghi aziendali (spesso) falsi.

Le e-mail o le pagine web sospette possono essere segnalate sul sito web antiphishing.ch. Le e-mail sospette possono anche essere inoltrate direttamente a reports@antiphishing.ch. Questa casella di posta elettronica non viene letta, ma elaborata automaticamente. Il mittente non riceve quindi alcuna risposta. Chi desidera ricevere un feedback dall'UFCS può segnalare all'UFCS stesso le e-mail di phishing e le pagine web sospette tramite il modulo per la segnalazione[1]. Grazie alle numerose segnalazioni da parte della popolazione, di PMI e di operatori di infrastrutture critiche, la Confederazione, unitamente alle organizzazioni partner, è stata in grado di identificare oltre 55 000 pagine web di phishing e di introdurre contromisure adeguate.

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

Cosa fa l’UFCS con le segnalazioni di phishing?

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

Le segnalazioni su antiphishing.ch sono sottoposte a un esame preliminare automatico. Molte pagine web vengono ripetutamente segnalate all’UFCS, per questo il primo passo è quello di deduplicare queste pagine. In seguito vengono raccolti metadati pubblicamente accessibili, come ad esempio quale provider gestisce la pagina web di phishing sospetta. Viene inoltre creato automaticamente uno screenshot della pagina web segnalata, che aiuta gli analisti a valutare se si tratta effettivamente di phishing o meno. Al termine del processo ogni segnalazione viene esaminata manualmente dagli analisti.

Se una pagina web viene identificata come phishing dall’analista, solitamente viene inviata una notifica via e-mail. Quando possibile, questa viene poi inviata al provider di webhosting, al domain registrar e al titolare del domain («registrant»). Inoltre, quando possibile, l’UFCS informa anche il proprietario del marchio usato impropriamente dai criminali informatici per la campagna di phishing.

Come per molte minacce informatiche, anche nel phishing gli scambi nazionali e internazionali costituiscono un fattore importante. L’UFCS fornisce quindi tempestivamente informazioni tecniche sugli attuali provider Internet di pagine web di phishing, sui produttori di filtri antispam e sui produttori di browser web. Anche lo scambio nell’Anti-Phishing Working Group (APWG)2 internazionale è un pilastro fondamentale nella lotta contro il phishing.

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

Le cifre più importanti del 2023

Nel 2023 attraverso la piattaforma «antiphishing.ch» sono state inviate in totale **544 367 segnalazioni**. Inoltre nello stesso periodo sono giunte 9395 segnalazioni di phishing attraverso il modulo di segnalazione. Dopo la deduplicazione, **10 007 pagine sono state identificate come pagine web di phishing**. Ciò corrisponde a un aumento del 10 per cento rispetto all'anno precedente (2022). Con 1380 pagine web, il mese di dicembre ha visto il maggior numero di pagine web di phishing identificate nel 2023. Il 99 per cento delle segnalazioni proveniva dalla popolazione e dalle PMI, mentre l'1 per cento dagli operatori di infrastrutture critiche. Tuttavia, va notato che nella maggior parte dei siti web segnalati dalle infrastrutture critiche si tratta davvero di phishing. Al contrario, nella maggior parte delle segnalazioni della popolazione e delle PMI non si tratta di phishing, ma di spam o ad esempio newsletter legittime. C'è quindi una grande differenza tra le segnalazioni della popolazione e quelle degli operatori di infrastrutture critiche in termini di effettiva presenza di pagine web di phishing.

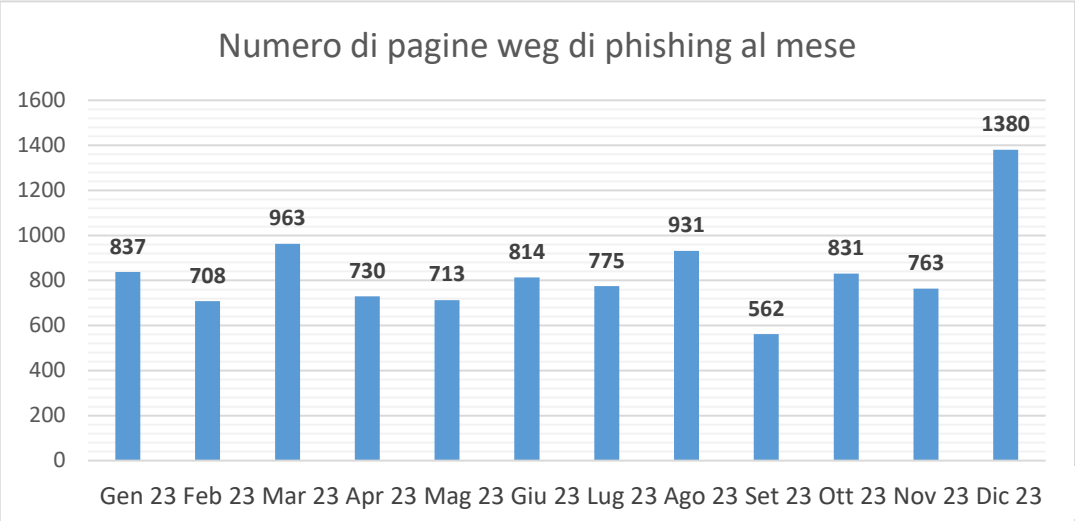

Figura 2 – Numero di pagine web di phishing al mese

Le pagine web di phishing identificate nel 2023 hanno usato impropriamente 260 nomi di marchi diversi, di cui il 61.1 per cento svizzeri e il 33,1 per cento stranieri. Il 5,8 per cento delle pagine web di phishing non hanno usato impropriamente alcun nome di marchio esplicito. In questo caso si tratta per lo più di pagine web di phishing generiche che cercano di ingannare la vittima per farle rivelare i dati di accesso alla posta elettronica.

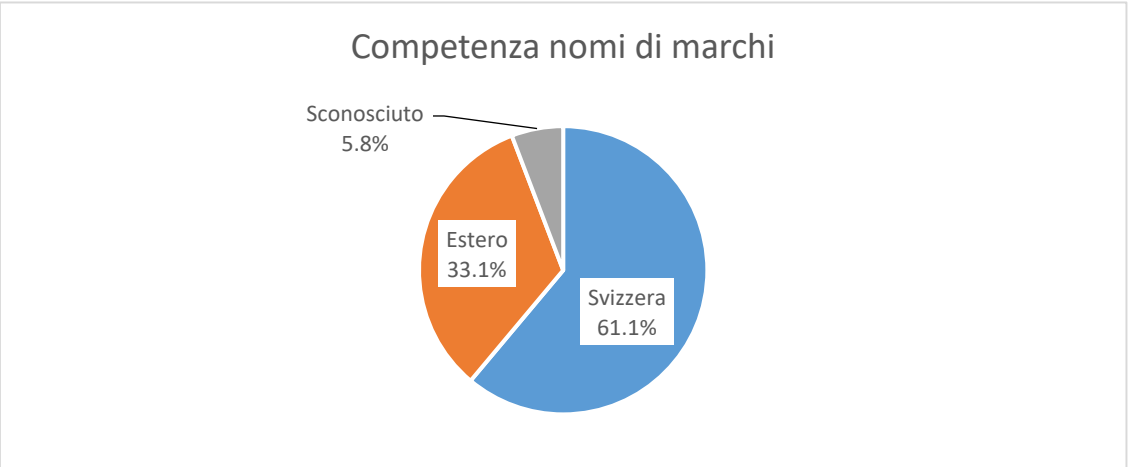

Figura 3 – Competenza dei nomi di marchi usati impropriamente

Con il 21 per cento, nel 2023 il nome del marchio della Posta Svizzera è stato il più usato dai criminali informatici per il phishing. Insieme ai fornitori di servizi stranieri, oltre il 40 per cento di pagine web di phishing usano in modo improprio il marchio di servizi di consegna di lettere e pacchi. Tuttavia, di solito non sono le piattaforme di questi fornitori a essere prese di mira dai criminali informatici. I loro marchi vengono piuttosto usati come esca per incassare presunte tasse di spedizione o doganali, che devono essere pagate con carta di credito. In realtà, la persona non sta pagando delle tasse, ma diventa vittima di phishing.

Con il 14 per cento delle pagine web di phishing, anche il marchio SwissPass è popolare tra i criminali informatici, seguito dai nomi di marchi di noti provider di Internet e telefonia mobile (8%).

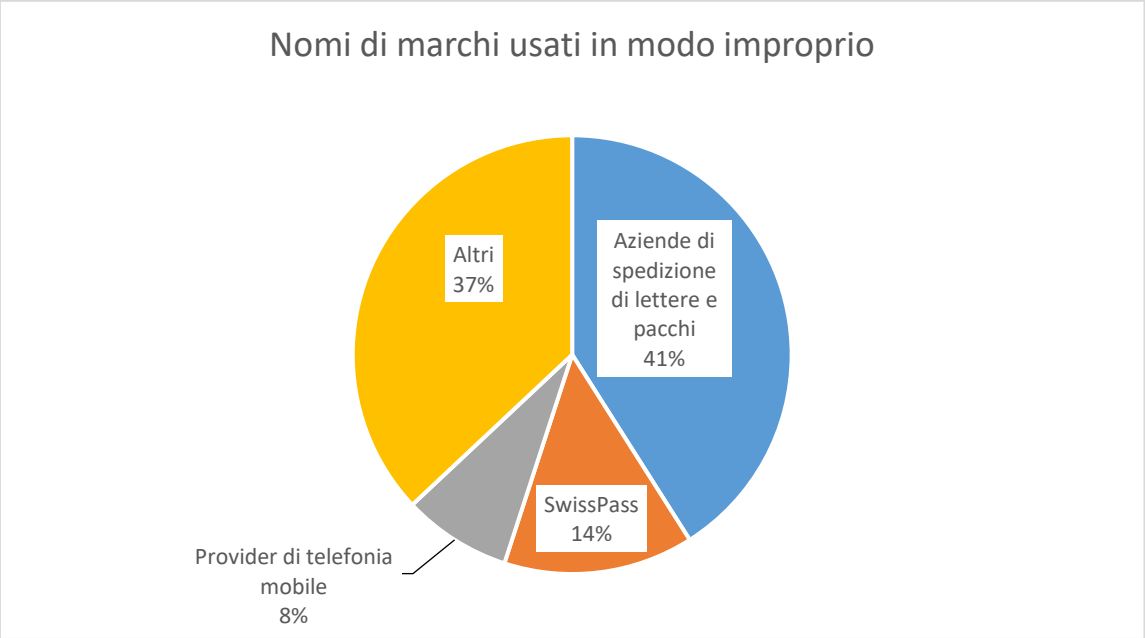

Figura 4 - Nomi di marchi usati in modo improprio

La maggior parte delle pagine web di phishing è gestita su domini di primo livello (top level domain, TLD) stranieri. Quasi la metà di tutte le pagine web di phishing identificate erano gestite sui gTLD[3] «.com» e «.net». A differenza del ccTLD[4] «.ch» in questo caso non si applica l'ordinanza sui domini Internet (ODIn)[5] e quindi l'UFCS e altre autorità svizzere non possono intervenire attivamente contro la pagina web di phishing.

[3] Dominio generico di primo livello

[4] Dominio di primo livello con codice Paese

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

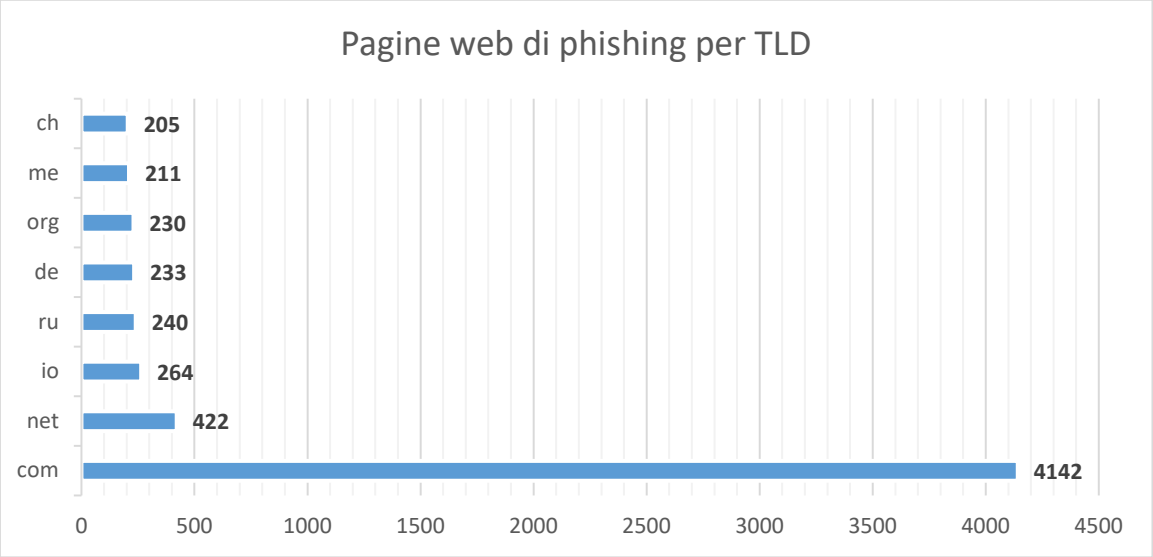

Figura 5 - Domini di primo livello (TLD) con il maggior numero di pagine web di phishing

Per mettere a disposizione pagine web di phishing, i criminali informatici usano, tra l'altro, pagine web hackerate. Tuttavia, spesso registrano loro stessi nomi di dominio dedicati al solo scopo di fornire pagine web di phishing. **Sul ccTLD «.ch» sono state gestite 205 pagine web di phishing, di cui 25 nomi di dominio sono stati registrati direttamente da criminali informatici per scopi esclusivamente fraudolenti.** Questi nomi di dominio sono stati bloccati in modo tecnico e amministrativo presso il gestore del registro (domain registry), secondo l'articolo 15 dell'ordinanza sui domini Internet (ODIn), su richiesta del NCSC.

Anche i fornitori di piattaforme Internet sono popolari tra i criminali informatici. La tabella seguente mostra le piattaforme Internet e i relativi operatori su cui l'NCSC ha individuato il maggior numero di pagine web di phishing nel 2023.

Rango	Pagine di phishing	Nome del dominio	Operatore	Paese
1	201	codeanyapp.com	Codeanywhere	USA
2	180	plesk.page	Plesk International	USA
3	146	mybluehost.me	Bluehost	USA
4	117	secureserver.net	GoDaddy	USA
5	96	web.app	Google	USA
6	96	cprapid.com	cPanel	USA
7	85	page.link	Google	USA
8	74	tempurl.host	Incsub	USA
9	72	hoster-test.ru	Hoster.ru	Russia
10	72	dweb.link	Protocol Labs	USA
11	71	sviluppo.host	n/d	n/d
12	71	cleverapps.io	Clever Cloud	Francia
13	54	wpengine.com	WP Engine	USA
14	53	builderallwppro.com	n/d	n/d
15	51	r2.dev	Cloudflare	USA

Altre varianti di phishing

Smishing: phishing via SMS

Nell'anno passato l'NCSC ha osservato un aumento dello «smishing». A differenza del phishing tradizionale, i tentativi di truffa avvengono via SMS o RCS, il successore dell'SMS, che è usato da molti servizi di messaggistica. Nello scorso anno sono stati usati in modo improprio soprattutto nomi di marchi di aziende di spedizione di lettere e pacchi per portare il destinatario su una pagina web di phishing che poi cerca di ottenere i dati della carta di credito.

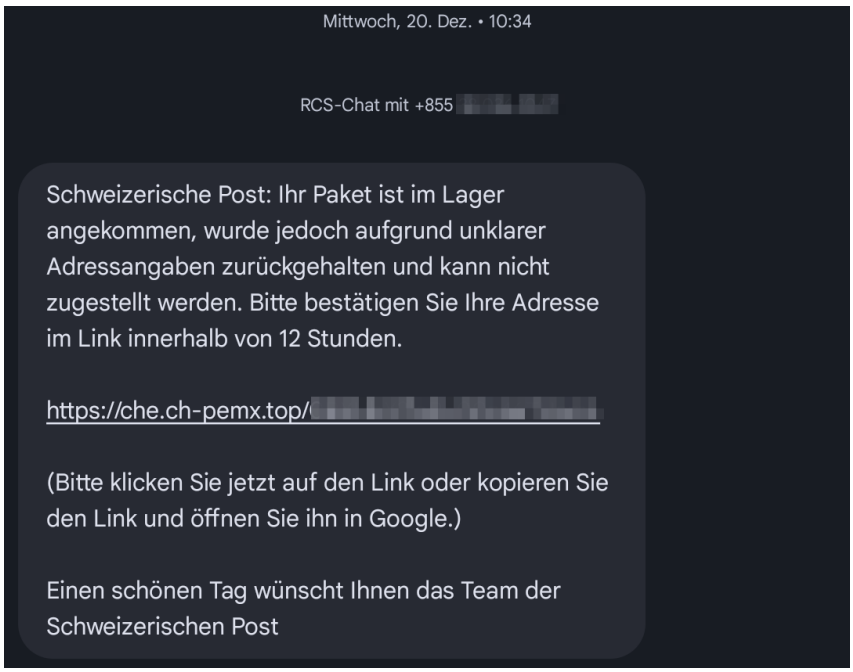

Figura 6 - Esempio di un messaggio di smishing (SMS/RCS)

A differenza del phishing via e-mail, gli SMS sospetti o fraudolenti non possono essere inoltrati ad antiphishing.ch e per l'UFCS è quindi difficile individuarli e adottare le contromisure appropriate. Gli utenti devono fare affidamento sulle misure di protezione del rispettivo operatore di telecomunicazioni o del produttore del sistema operativo.

I motori di ricerca diventano una trappola del phishing

Oggi i motori di ricerca sono parte integrante della quotidianità digitale. Ci permettono di trovare in breve tempo informazioni nel World Wide Web, che si tratti di una destinazione turistica, di un artista o di informazioni di cui abbiamo bisogno per il nostro lavoro. I motori di ricerca più utilizzati in Svizzera sono Google (Alphabet) e Bing (Microsoft).

L'offerta dei motori di ricerca è gratuita. Tuttavia, per poter offrire il servizio gratuitamente, il fornitore dipende dalle entrate. Il mercato pubblicitario è un modello di business diffuso e redditizio. I fornitori di motori di ricerca affittano agli inserzionisti le prime posizioni dei risultati di ricerca. Può quindi succedere che quando gli utenti di Internet cercano un hotel, in cima ai risultati non appare la pagina web dell'hotel che stanno cercando, ma magari quella di un concorrente, perché quest'ultimo paga il fornitore del motore di ricerca per tale inserto pubblicitario.

I motori di ricerca sono molto redditizi per le aziende che inseriscono tali annunci. Il cosiddetto «profiling» permette di indirizzare gli annunci in modo specifico al pubblico target desiderato. Solo gli utenti che corrispondono al pubblico target vedranno gli annunci. Le possibilità sono quasi illimitate: età, sesso, interessi, ma anche il Paese da cui viene effettuata la ricerca o la lingua utilizzata dal browser web. Tuttavia, queste possibilità non sono interessanti solo per le aziende con intenzioni legittime. Anche i cibercriminali hanno scoperto da tempo che tali annunci sono un modo affidabile per attirare le potenziali vittime su pagine web di phishing.

Nella seconda metà del 2023 l'NCSC ha ricevuto un numero crescente di segnalazioni di annunci ingannevoli, i cosiddetti «rogue ads», sui motori di ricerca. Al momento un numero relativamente elevato di questi è attivo su Bing (Microsoft). Con l'aiuto di account publisher hackerati o identità rubate, i criminali informatici affittano spazi pubblicitari per una parola chiave su Bing. I cibercriminali usano come parole chiave i nomi di noti istituti finanziari svizzeri o emittenti di carte di credito. Se una potenziale vittima cerca l'e-banking della propria banca su Bing, in cima ai risultati vedrà un annuncio dei criminali informatici, che è costruito in modo da suggerire che si tratta dell'effettivo risultato di ricerca del sistema di e-banking della banca. Se la vittima clicca sull'annuncio, viene indirizzata a una pagina web di phishing dei cibercriminali. Attraverso gli attacchi di phishing in tempo reale la pagina web di phishing è in grado di accedere anche ai sistemi di e-banking protetti dall'autenticazione a più fattori.

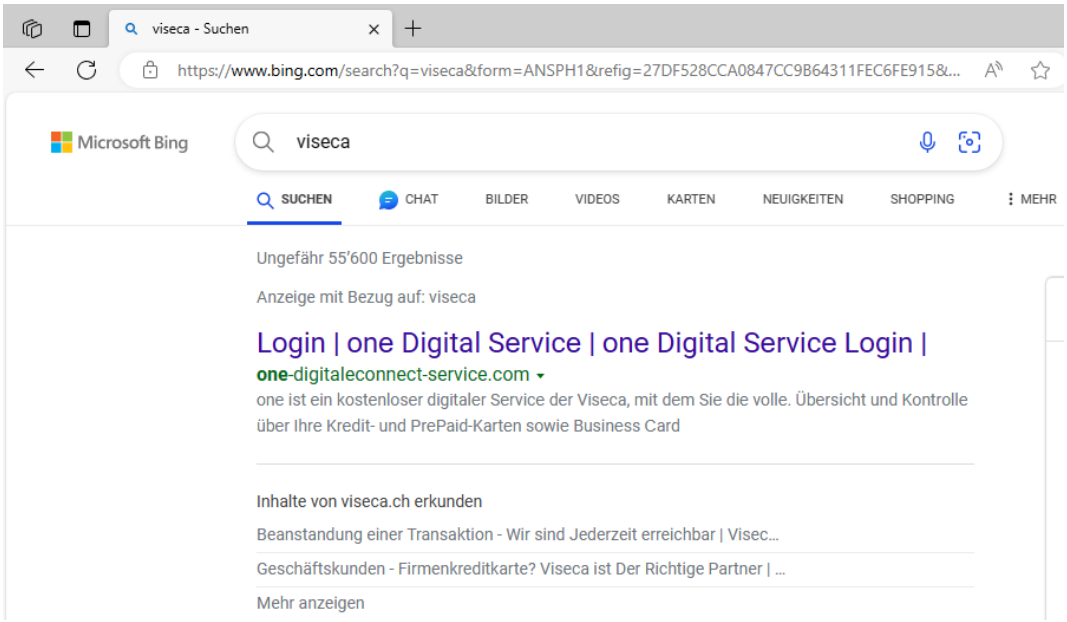

Figura 7 - Esempio di un «rogue ad» su un motore di ricerca, che porta a una pagina web di phishing

Per i cibercriminali questo modus operandi è vantaggioso sotto molti aspetti. Da un lato, possono scegliere in modo mirato a chi vengono mostrati gli annunci malevoli (per una banca cantonale in Romandia possono limitare la visualizzazione degli annunci a «Svizzera» e alla lingua «francese»). Dall'altro lato, a differenza del phishing via e-mail, non devono fare i conti con i filtri antispam che potrebbero classificare l'e-mail di phishing come spam.

Allo stesso tempo, il modus operandi pone problemi ai fornitori di servizi di sicurezza e alle autorità come l'UFCS, che intervengono contro il phishing nel ciberspazio. Non c'è trasparenza da parte dei fornitori di motori di ricerca in relazione a chi ha inserito gli annunci, pertanto non è possibile individuarli tempestivamente. L'UFCS può quindi attivarsi solo quando la pubblicità dannosa è già stata inserita e viene segnalata dai cittadini o da un'infrastruttura critica. Per questo motivo l'UFCS è molto grato di ricevere segnalazioni dalla popolazione, dalle aziende, dalle autorità e dalle organizzazioni.

Raccomandazioni

Siate sempre scettici nei confronti di e-mail e SMS che cercano di convincervi a cliccare su un link. L'UFCS raccomanda inoltre quanto segue:

- **Segnalazione all'UFCS:** segnalate all'UFCS e-mail o pagine web sospette su anti-phishing.ch. Se desiderate una risposta alla vostra segnalazione, in alternativa usate il formulario di segnalazione su https://www.report.ncsc.admin.ch/

- **Scetticismo:** nessuna banca e nessun emittente di carte di credito vi chiederà mai di modificare la password o di verificare i dati della carta di credito via e-mail o SMS.

- **Autentificazione a più fattori:** quando possibile, attivate l'autentificazione a più fattori sui vostri account online come ad esempio l'e-mail o i social media. Controllate nelle impostazioni dell'account del vostro provider se l'autentificazione a più fattori viene offerta e attivate questa opzione.

- **Uso multiplo delle password:** non usate mai la stessa password per più account online. Usate un password manager per gestire i vostri dati di accesso.

- **Estratto della carta di credito:** controllate regolarmente l'estratto della carta di credito per individuare eventuali discrepanze e in caso di transazioni sconosciute contattate subito l'emittente della carta di credito.

- **Filtro SMS:** attivate il filtro SMS del vostro sistema operativo sullo smartphone per filtrare gli SMS sospetti.

- **Uso dei preferiti:** usate la funzione dei preferiti («segnalibri») del vostro browser web per accedere regolarmente ad account online come ad esempio l'e-banking, i social media o l'e-mail.

- **Spoofing:** tenete presente che i mittenti di e-mail e SMS, così come i numeri delle chiamate in entrata, sono facili da falsificare. In caso di dubbio, chiedete di poter richiamare il mittente.