Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

29 January 2024

Anti-Phishing Report 2023

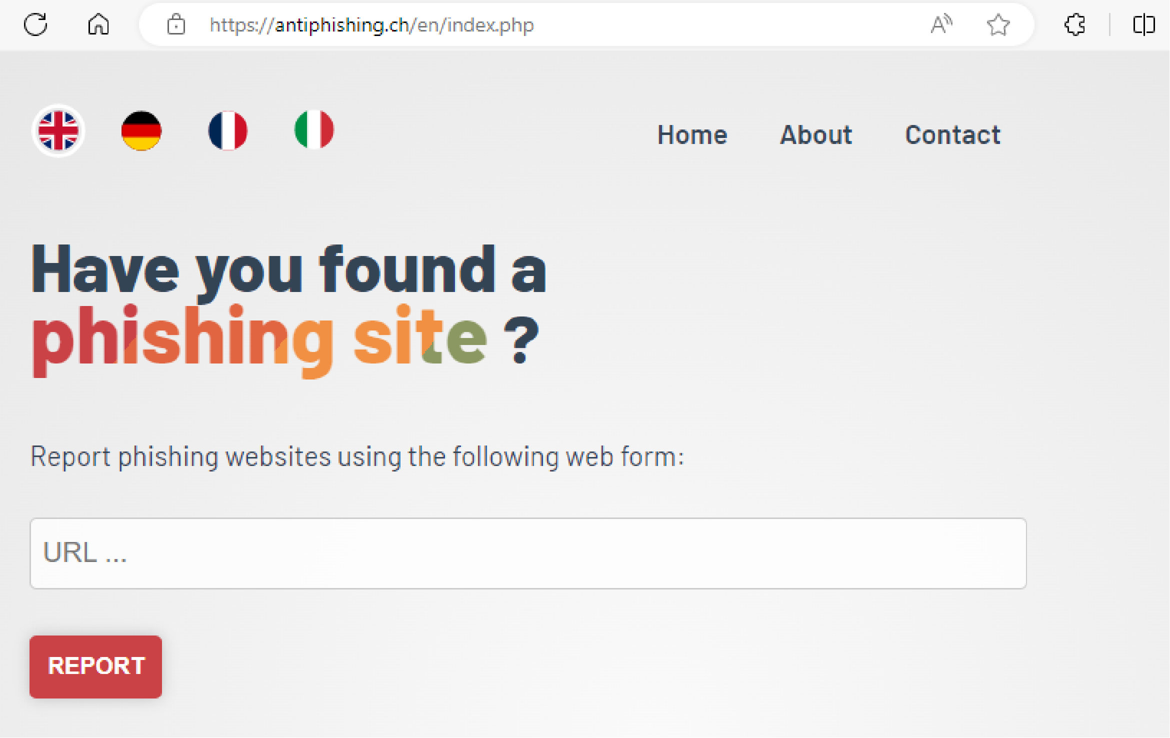
Introduction

The Swiss government has been operating the 'antiphishing.ch' platform for almost 10 years. The platform was launched in 2014 by the Reporting and Analysis Centre for Information Assurance (MELANI) and has been operated since 2020 by the National Cyber Security Centre (NCSC). The platform offers the population of Switzerland as well as organisations, public authorities and SMEs the opportunity to report suspicious websites and emails. The aim is to identify websites which attempt, under false pretences, to obtain sensitive data such as credentials for email, online banking or social media accounts or credit card details (known as 'phishing'). The fraudsters take advantage of their victims' good faith and willingness to help by sending them emails with (frequently) fake sender addresses and company logos.

Suspicious emails or websites can be reported on the website antiphishing.ch. However, suspicious emails can also be forwarded directly to reports@antiphishing.ch. This mailbox is not read but is processed automatically. The sender will therefore not receive an answer. Senders who would like confirmation from the NCSC should report phishing emails or suspicious websites to the NCSC using the reporting form.[1] Thanks to the many reports from the general public, SMEs and operators of critical infrastructures, the Swiss Confederation – together with its partner organisations – has been able to identify more than 55,000 phishing websites to date and initiate appropriate countermeasures.

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

What does the NCSC do with the phishing reports?



https://antiphishing.ch/en/index.php

Home About Contact

Have you found a phishing site ?

Report phishing websites using the following web form:

URL ...

REPORT

Figure 1 – The antiphishing.ch platform of the NCSC

Reports on antiphishing.ch are first automatically screened. Many websites are reported to the NCSC multiple times, so any duplicate websites are removed at this stage. Publicly accessible metadata is then collected, for example the name of the provider hosting the suspected phishing website. In addition, a screenshot of the reported website is automatically taken. This helps the NCSC analysts to assess whether the reported website is actually a phishing website or not. At the end of the process, each message is reviewed manually by analysts.

If a website is confirmed as a phishing website by the analysts, an email notification is usually sent. If possible, this is sent to the website hosting provider, the sponsoring domain registrar and the domain name owner ('registrant'). In addition, if possible, the NCSC informs the owner of the brand that was misused by cybercriminals for the phishing campaign.

As with many cyber threats, national and international exchange is also an important factor in countering phishing attacks. The NCSC therefore promptly provides technical information on current phishing websites to internet providers, spam filter companies and web browser vendors. Information exchange in the international Anti-Phishing Working Group (APWG)[2] is another cornerstone in the battle against phishing.

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

Key figures from 2023

In 2023, a total of **544,367 reports** were sent to the antiphishing.ch platform. In addition, 9395 phishing reports were received via the reporting form in the same period. After deduplication, **10,007 websites were identified as phishing websites**. This represents an increase of 10% compared with the previous year (2022). With 1,380 phishing websites identified in December alone, this month saw the highest number of phishing websites in 2023. 99% of the reports came from the general public and SMEs, with just 1% from operators of critical infrastructures. However, it should be noted here that a large portion of the websites reported by critical infrastructures were indeed phishing websites. This contrasts with reports from the general public and SMEs, where the majority of reports did not refer to phishing as such but to spam or even legitimate newsletters, for example. There is thus a major disparity between the reports from the general public and those from operators of critical infrastructures with regard to whether the reports actually concern phishing websites.

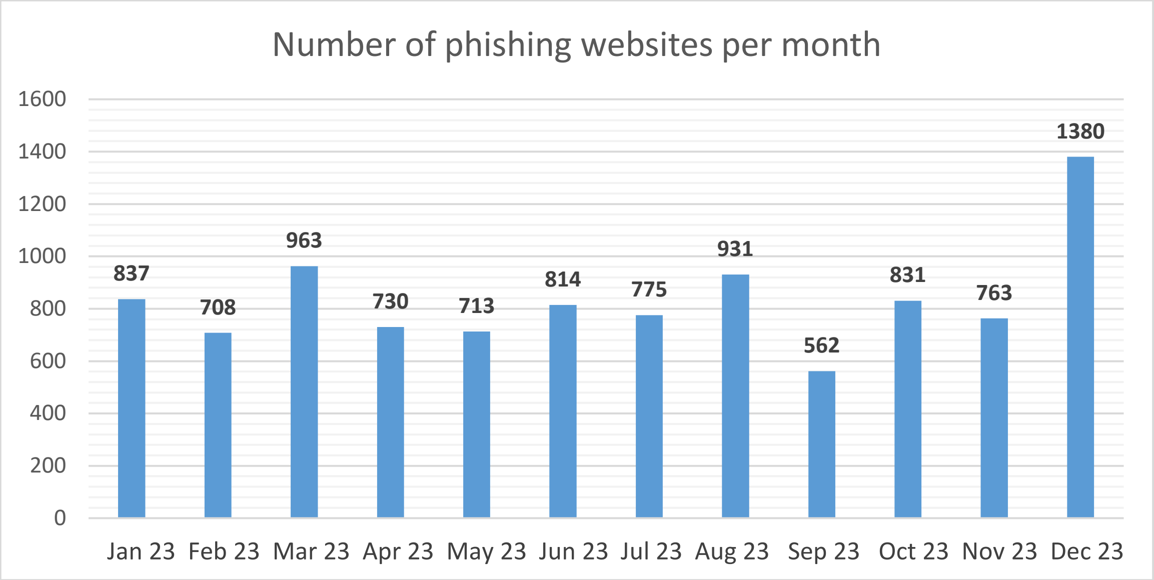


Figure 2 – Number of phishing websites per month

The phishing websites identified in 2023 misused **260 different brand names**, of which **61.1% were Swiss brands** and 33.1% were foreign brands. 5.8% of the phishing websites did not impersonate any particular brand; most of these were generic phishing websites which try to trick the victim into disclosing their email credentials.

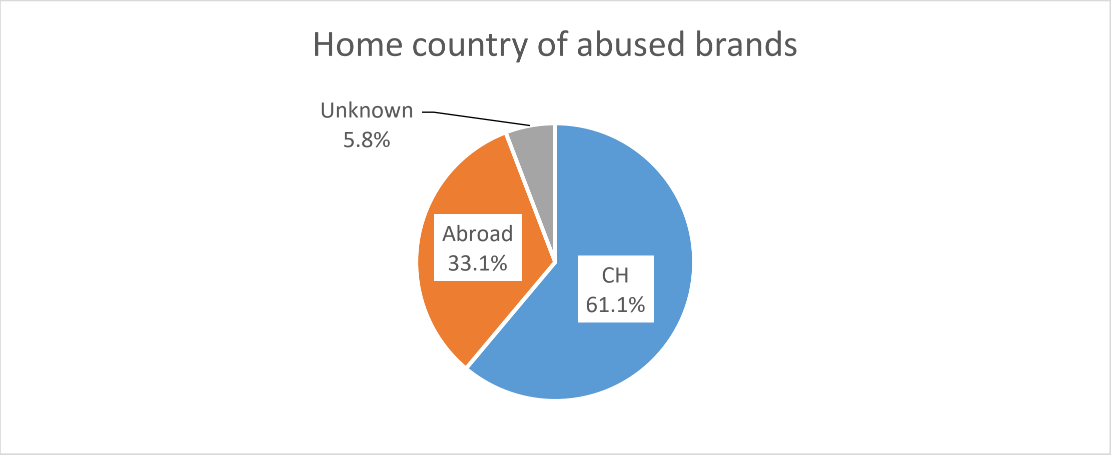


Figure 3 – Home country of brands targeted

At 21%, Swiss Post was the brand most misused for phishing attacks in 2023. Including foreign providers, phishing websites which misuse brand names of letter and parcel courier companies account for over 40%. However, it is usually not the couriers' own platforms that are targeted by cyber criminals: instead, their brand names are used as bait to collect delivery or customs fees. The phishers try to lure the recipient to settle the fees by credit card. In reality, however, the person making the payment is not settling any fees but becomes a victim of credit card phishing.

Also popular with cybercriminals is the brand SwissPass, which accounts for 14% of phishing websites, followed by well-known internet and mobile phone providers (8%).

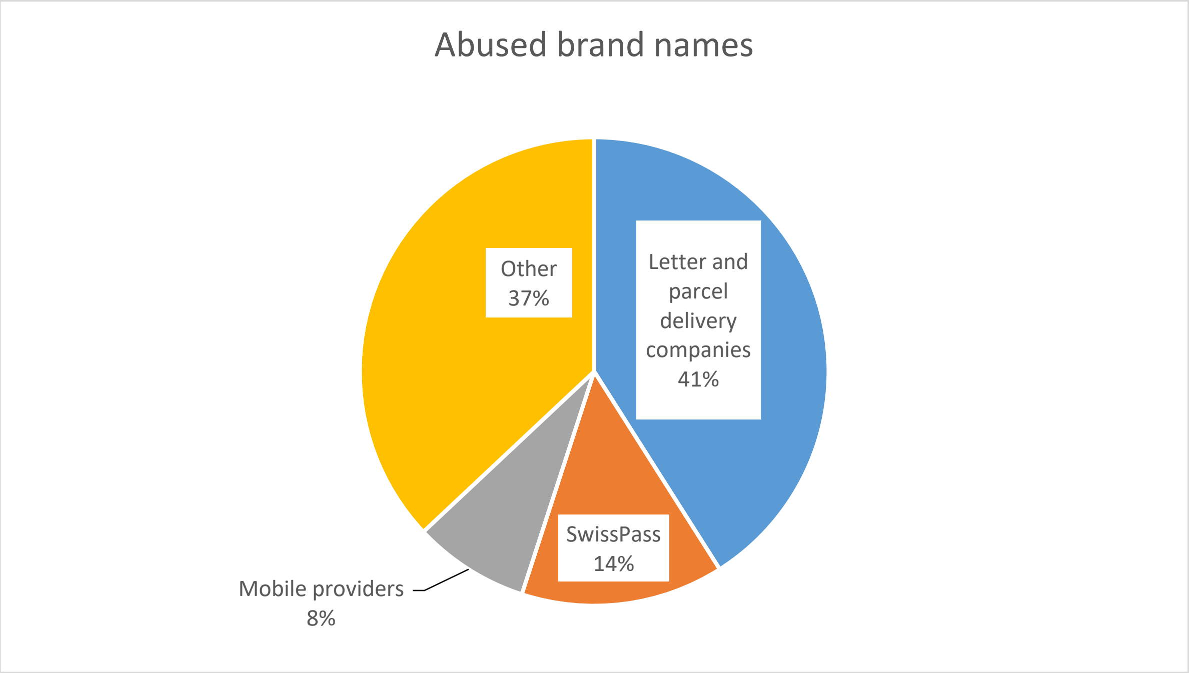


Figure 4 – Abused brand names

A large number of phishing websites are operated on foreign top-level domains (TLDs). Almost half of all identified phishing websites used the gTLD[3] **.com** or **.net**. Unlike the ccTLD[4] **.ch**, these are not subject to the Ordinance on Internet Domains (OID)[5], which means that the NCSC and other Swiss authorities are unable to take active action against them.

[3] Generic top-level domain

[4] Country code top-level domain

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

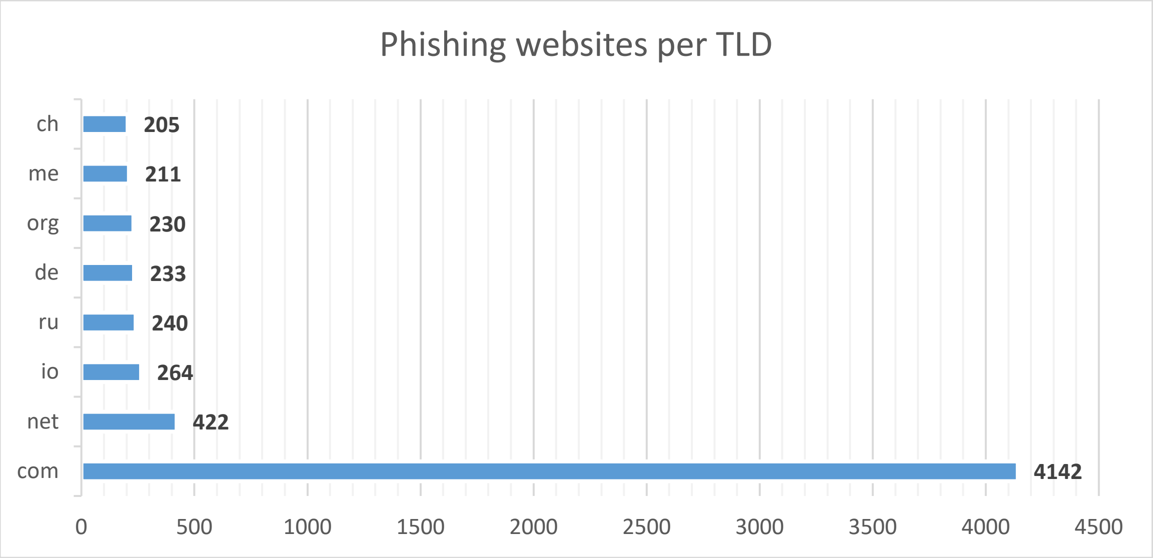


Figure 5 – Top-level domains (TLD) with the most phishing websites

Cybercriminals frequently use hacked websites as a basis for their phishing attacks. However, they also often register dedicated domain names themselves with the sole purpose of creating phishing websites. **205 phishing websites were operated on the ccTLD .ch. Of these, it is suspected that 25 domain names were registered by cybercriminals solely for fraudulent purposes.** At the request of the NCSC, these domain names have been blocked for technical and administrative purposes by the domain registry, based on Article 15 OID.

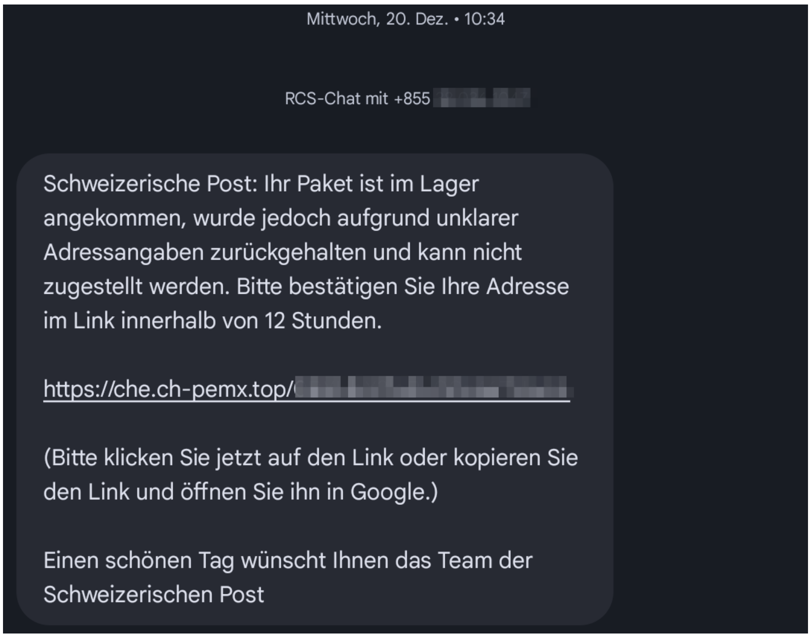
Providers of internet platforms are also a popular target for cybercriminals. The table below shows the internet platforms and their operators on which the NCSC identified the most phishing websites in 2023.

Rank	**Phishing pages**	**Domain name**	**Operator**	**Country**
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/a	n/a
12	71	cleverapps.io	Clever Cloud	France
13	54	wpengine.com	WP Engine	USA
14	53	builderallwppro.com	n/a	n/a
15	51	r2.dev	Cloudflare	USA

Other phishing variants

Smishing – phishing via SMS

Over the last year, the NCSC noticed an increase in 'smishing'. Unlike conventional phishing, this type of fraud uses SMS – or its successor RCS, now used by many messenger services. Last year, the brand names of letter and parcel courier companies were most frequently misused to lure recipients to a phishing website, which then tries to steal credit card details from them.



Mittwoch, 20. Dez. • 10:34

RCS-Chat mit +855 [redacted]

Schweizerische Post: Ihr Paket ist im Lager angekommen, wurde jedoch aufgrund unklarer Adressangaben zurückgehalten und kann nicht zugestellt werden. Bitte bestätigen Sie Ihre Adresse im Link innerhalb von 12 Stunden.

https://che.ch-pemx.top/[redacted]

(Bitte klicken Sie jetzt auf den Link oder kopieren Sie den Link und öffnen Sie ihn in Google.)

Einen schönen Tag wünscht Ihnen das Team der Schweizerischen Post

Figure 6 – Example of a smishing message (SMS/RCS)

Unlike email-based phishing, suspicious or fraudulent SMS cannot be simply forwarded to antiphishing.ch, which makes it difficult for the NCSC to detect and initiate appropriate countermeasures. Users have to rely on safeguards taken by their telecom provider (for traditional SMS) or operating system (for RCS).

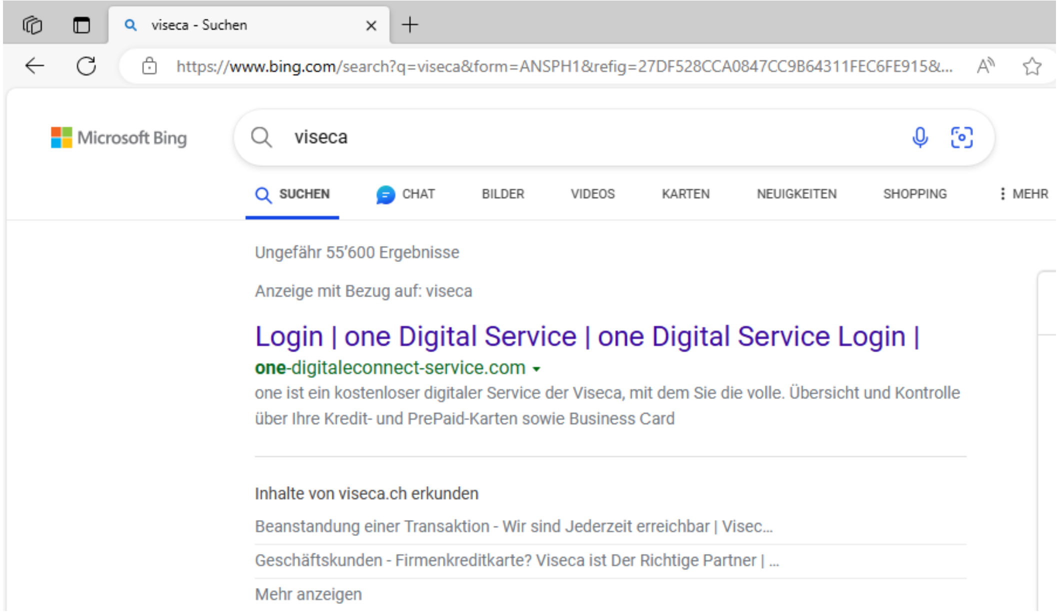
When search engines become phishing traps

Search engines have become an integral part of our everyday digital life. We use them to quickly find information online on all sorts of things – be it a holiday destination, a particular artist, or information we may need for our work. The most frequently used search engines in Switzerland are Google (Alphabet) and Bing (Microsoft).

Search engines provide this information free of charge. However, in order to be able to do so for free, they need some source of revenue stream. Online advertising is a widespread and lucrative business model which allows advertisers to pay for the top rankings on search engines. This means that when you search for a hotel online, the website that appears at the top of the search results may not be the one you are actually looking for, but perhaps a completely different hotel. When this happens, it is because the other hotel is paying the search engine to rank its ad at the top of the list.

For companies that place such online ads, search engines can be very cost effective. Through profiling, adverts can be tailored to a specific target audience, with banners displayed only for those users meeting a specific profile. The extent of user profiling is almost unlimited: age, gender, interests, the country from which the search query is sent, the web browser language, etc. However, these options are not only attractive for companies with legitimate interests. Cybercriminals, too, have long recognised that advertising banners are an easy way to lure potential victims to phishing websites.

In the second half of 2023, the NCSC received an increasing number of reports of malicious adverts on search engines – known as 'rogue ads'. A comparatively large number of these are currently appearing on Bing (Microsoft). Using hacked web publisher accounts or stolen identities, cybercriminals rent advertising space for a particular keyword or search query on Bing. They tend to use the names of well-known Swiss financial institutions or credit card issuers as keywords. If a potential victim then searches for their usual online banking portal on Bing, they may see the fake sponsored ad as the top search result. The ad is designed to suggest that it is a genuine search result for the online banking portal. However, if the user clicks on this rogue ad, they are led to a fake website set up for phishing purposes. Using 'real-time phishing' the phishing website can even access online banking systems secured with multi-factor authentication (MFA).



https://www.bing.com/search?q=viseca&form=ANSPH1&refig=27DF528CCA0847CC9B64311FEC6FE915&...

viseca

Ungefähr 55'600 Ergebnisse

Anzeige mit Bezug auf: viseca

Login | one Digital Service | one Digital Service Login |

one-digitaleconnect-service.com

one ist ein kostenloser digitaler Service der Viseca, mit dem Sie die volle. Übersicht und Kontrolle über Ihre Kredit- und PrePaid-Karten sowie Business Card

Inhalte von viseca.ch erkunden

Beanstandung einer Transaktion - Wir sind Jederzeit erreichbar | Visec...

Geschäftskunden - Firmenkreditkarte? Viseca ist Der Richtige Partner | ...

Mehr anzeigen

Figure 7 – Example of a rogue ad on a search engine leading to a phishing website

This technique is convenient for cybercriminals in many respects. For one thing, they can specifically select who this malicious advertising is displayed to (e.g. for a cantonal bank in French-speaking Switzerland, cybercriminals can restrict display of the advert to users for which the location is 'Switzerland' and the language 'French'). Also, unlike with phishing via email, they do not need to get around spam filters that might classify the email as junk.

At the same time, this technique poses problems for security providers and authorities such as the NCSC trying to counter phishing in cyberspace. For example, search engine providers are not always transparent about who has placed which advertisements, so early detection is not possible. The NCSC can only intervene once the malicious advertisement has already been placed and reported by the public or a critical infrastructure. The NCSC is therefore very grateful when it receives messages from the public or from companies, authorities or organisations.

Recommendations

Always be sceptical about emails and SMS telling you to click on a link. The NCSC also recommends the following:

- **Report to the NCSC:** Report suspicious emails or websites to the NCSC at antiphishing.ch. Alternatively, if you want confirmation of your report, use the report form on https://www.report.ncsc.admin.ch/

- **Be sceptical:** No bank or credit card institution will ever ask you to change passwords or verify credit card details by email or SMS.

- **Multi-factor authentication (MFA):** Wherever possible, activate multi-factor authentication (MFA) on your online accounts such as email or social media. Check your provider's account settings to see if MFA is offered and activate this option.

- **Multiple use of passwords:** Never use the same password for different 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 if you find any unknown transactions.

- **SMS filter:** Activate the SMS filter of your operating system on your smartphone to filter out any suspicious SMS.

- **Using favourites:** Use the Favourites (or 'bookmarks') function in your web browser for accounts you access regularly, such as online banking, social media and email.

- **Spoofing:** Remember that sender addresses of emails and SMS and the caller ID of incoming calls are easy to fake. If you are in doubt, ask the person calling if you can call them back.