Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

29. Januar 2024

Anti-Phishing Bericht 2023

Einleitung

Seit fast 10 Jahren betreibt der Bund die Plattform «antiphishing.ch». Die Plattform wurde 2014 von der Melde- und Analysestelle Informationssicherung (MELANI) lanciert und wird seit 2020 vom Nationalen Zentrum für Cybersicherheit (NCSC), das am 1.1.2024 zum Bundesamt für Cybersicherheit (BACS) wurde, betrieben. Die Plattform bietet der Schweizer Bevölkerung aber auch Organisationen, Behörden und KMUs die Möglichkeit, verdächtige Webseiten und E-Mails zu melden. Ziel ist es, Webseiten zu identifizieren, welche versuchen, unter Vortäuschung eines falschen Sachverhaltes, an sensible Daten wie Zugangsdaten zu E-Mail-, E-Banking- oder Social-Media-Konten oder aber auch an Kreditkarten-Informationen zu gelangen (sogenanntes «Phishing»). Die Betrüger nutzen dabei die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen E-Mails mit (häufig) gefälschten Absenderadresse und Firmenlogos zustellen.

Verdächtige E-Mails oder Webseiten können auf der Website antiphishing.ch gemeldet werden. Verdächtige E-Mails können aber auch direkt an reports@antiphishing.ch weitergeleitet werden. Diese Mailbox wird nicht gelesen, sondern maschinell verarbeitet. Es erfolgt daher keine Antwort an den Absender. Absenderinnen und Absender, welche eine Rückmeldung vom BACS wünschen, können Phishing-E-Mails und verdächtige Webseiten über das Meldeformular[1] dem BACS melden. Dank den zahlreichen Meldungen von Bevölkerung, KMUs und Betreiberinnen und Betreiber kritischer Infrastrukturen konnte der Bund gemeinsam mit Partnerorganisationen bis heute über 55'000 Phishing-Webseiten identifizieren und geeignete Gegenmassnahmen einleiten.

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

Was macht das BACS mit den Phishing-Meldungen?

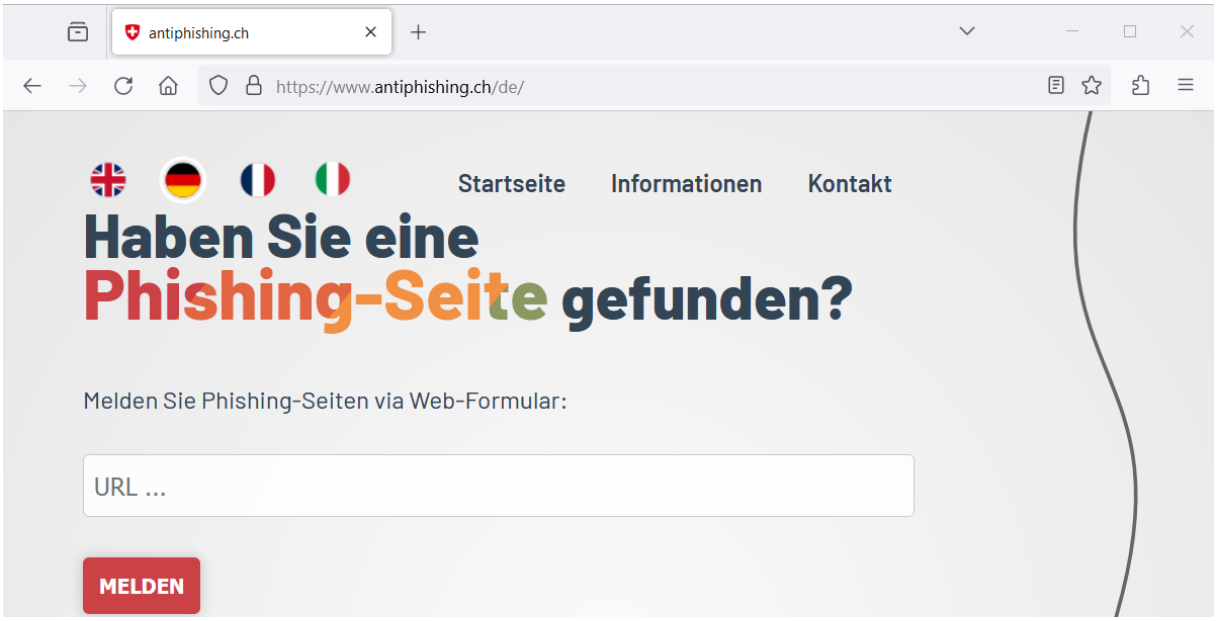

Abbildung 1 - Plattform «antiphishing.ch» des BACS

Meldungen auf antiphishing.ch werden einer maschinellen Vorprüfung unterzogen. Viele Webseiten werden dem BACS mehrmals gemeldet, weshalb als erstes eine Deduplizierung der mehrfach gemeldeten Webseiten stattfindet. Danach werden öffentlich zugängliche Metadaten erhoben, beispielsweise bei welchem Anbieter die mutmassliche Phishing-Webseite betrieben wird. Des Weiteren wird automatisch ein Screenshot der gemeldeten Webseite erstellt. Dies hilft den Analysten bei der Beurteilung, ob es sich bei der gemeldeten Webseite tatsächlich um eine Phishing-Webseite handelt oder nicht. Am Ende des Prozesses wird jede Meldung von Analysten manuell begutachtet.

Wird eine Webseite durch den Analysten als Phishing identifiziert, so wird in der Regel per E-Mail eine Benachrichtigung gesendet. Anschliessend wird diese, wenn immer möglich, an den Webhosting-Anbieter, Domain-Registrar sowie den Domain-Inhaber («Registrant») versendet. Zusätzlich informiert das BACS, wenn immer möglich, auch den Inhaber der Marke, welche von den Cyberkriminellen für die Phishing-Kampagne missbraucht wird.

Wie bei vielen Cyberbedrohungen, ist auch bei Phishing der nationale und internationale Austausch ein wichtiger Faktor. Das BACS stellt deshalb technische Informationen zu aktuellen Phishing-Webseiten Internetanbietern, Spam-Filter-Hersteller sowie Hersteller von Web-Browsern zeitnah zur Verfügung. Auch der Austausch in der internationalen Anti-Phishing Working Group (APWG)[2] ist ein wichtiger Grundpfeiler im Kampf gegen Phishing.

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

Die wichtigsten Zahlen 2023

Im Jahr 2023 wurden über die Plattform «antiphishing.ch» total **544’367 Meldungen** abgesetzt. Zusätzlich gingen über das Meldeformular im gleichen Zeitraum 9395 Meldungen zu Phishing ein. Nach der Deduplizierung konnten **10’007 Webseiten als Phishing-Webseiten identifiziert** werden. Dies entspricht einer Steigerung um 10% gegenüber dem Vorjahr (2022). Mit 1’380 Phishing-Webseiten wurden im Monat Dezember die meisten Phishing-Webseiten des Jahres 2023 identifiziert. 99% der Meldungen stammten von der Bevölkerung und KMUs. 1% von Betreibenden kritischer Infrastrukturen. Hierbei gilt es jedoch zu bemerken, dass es sich bei einem Grossteil der durch kritische Infrastrukturen gemeldeten Webseiten tatsächlich auch um Phishing handelt. Demgegenüber stehen Meldungen von der Bevölkerung und KMUs, bei welchen es sich grösstenteils nicht um Phishing selber, sondern um Spam oder beispielsweise legitime Newsletter handelt. Es besteht somit ein grosser Unterschied zwischen den Meldungen von der Bevölkerung und jenen von Betreibenden kritischer Infrastrukturen, in Bezug ob es sich tatsächlich um Phishing-Webseiten handelt.

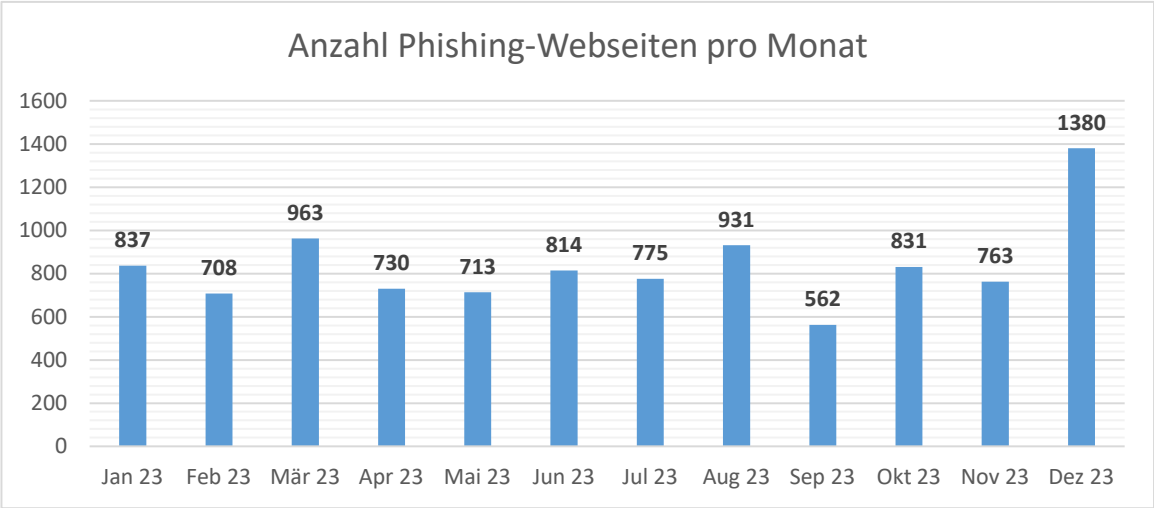

Abbildung 2 – Anzahl Phishing-Webseiten pro Monat

Die 2023 identifizierten Phishing-Webseiten missbrauchten **260 verschiedene Markennamen**, wobei **61.1% der gemeldeten Phishing-Webseiten Schweizer Markennamen** und 33,1% Namen von ausländischen Marken missbrauchten. 5,8% der Phishing-Webseiten hatten keine expliziten Markennamen missbraucht. Hierbei handelt es sich grösstenteils um generische Phishing-Webseiten, welche das Opfer dazu verleiten wollen, dessen E-Mail-Zugangsdaten preiszugeben.

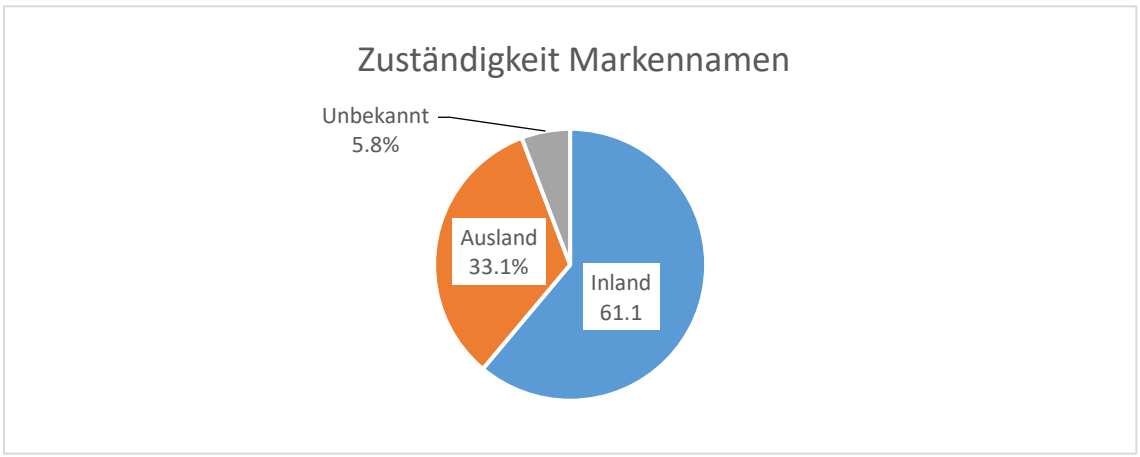

Abbildung 3 – Zuständigkeit der missbrauchten Markennamen

Mit 21% wurde 2023 der Markenname der Schweizerischen Post am meisten von Cyberkriminellen für Phishing missbraucht. Zusammen mit ausländischen Anbietern kommen Phishing-Webseiten, welche Markennamen von bekannten Brief- und Paket-Zulieferern missbrauchen, auf über 40%. Dabei sind in der Regel aber nicht die Plattformen dieser Anbieter das Ziel der Cyberkriminellen. Vielmehr werden deren Markennamen als Köder benutzt, um angebliche Paketzustellungs- oder Zollgebühren einzukassieren. Diese Gebühren sollen dann mittels Kreditkarte beglichen werden. Tatsächlich begleicht das Opfer dabei aber keine Gebühren, sondern wird Opfer von Kreditkarten-Phishing.

Ebenfalls beliebt bei Cyberkriminellen ist die Marke SwissPass, auf welchen 14% der Phishing-Webseiten entfallen, gefolgt von Markennamen von bekannten Internet- und Mobilfunkanbietern (8%).

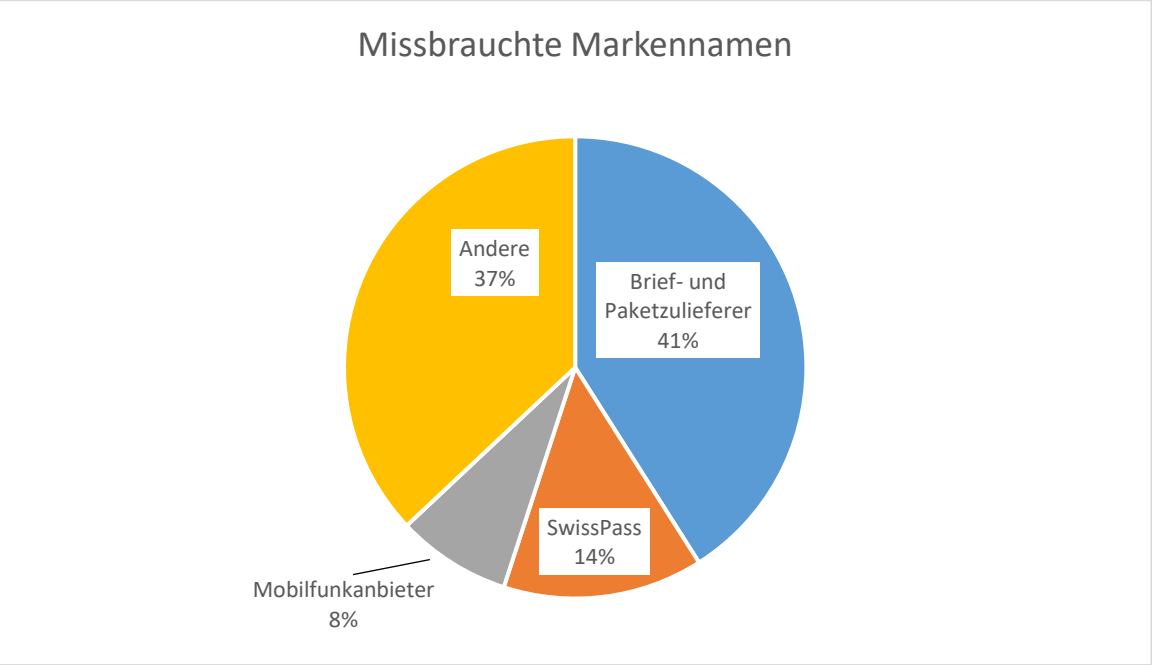

Abbildung 4 - Missbrauchte Markennamen

Ein Grossteil der Phishing-Webseiten wird auf ausländischen Top-Level-Domains (TLDs) betrieben. Fast die Hälfte aller identifizierten Phishing-Webseiten wurden auf den gTLDs3 «.com» und «.net» betrieben. Anders als bei der ccTLD4 «.ch» ist hier die Verordnung über Internet-Domains (VID)5 nicht anwendbar, wodurch dem BACS sowie auch anderen Behörden in der Schweiz die Möglichkeit fehlt, aktiv gegen die Phishing-Webseite vorzugehen.

[3] Generic Top-Level-Domain

[4] Country Code Top-Level-Domain

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

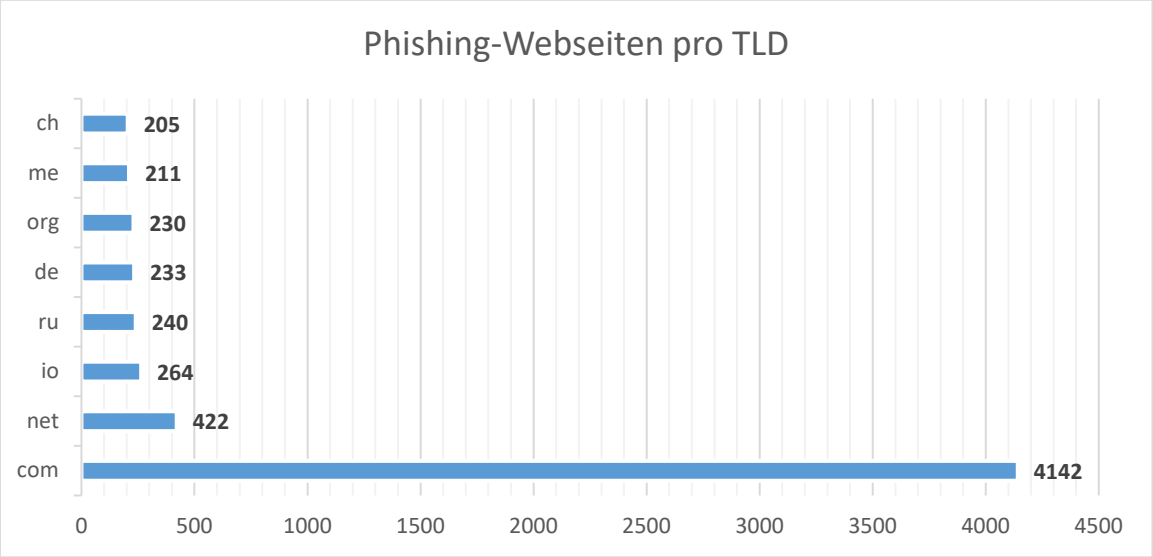

Abbildung 5 - Top Level Domain (TLD) mit den meisten Phishing-Webseiten

Für die Bereitstellung von Phishing-Webseiten greifen die Cyberkriminellen unter anderem auf gehackte Webseiten zurück. Oftmals registrieren diese aber auch dedizierte Domain-Namen direkt selber mit dem ausschliesslichen Zweck, die Phishing-Webseiten bereitzustellen. **205 Phishing-Webseiten wurde auf der ccTLD «.ch» betrieben. Davon wurden 25 Domain-Namen mutmasslich direkt von Cyberkriminellen für ausschliesslich betrügerische Absichten registriert.** Diese Domain-Namen wurden gestützt auf die Verordnung über Internet-Domains (VID) Art. 15 auf Antrag des NCSC technisch und administrativ bei der Registerbetreiberin (Domain-Registry) blockiert.

Bei Cyberkriminellen ebenfalls beliebt sind Anbieter von Internetplattformen. Die folgende Tabelle zeigt die Internetplattformen sowie deren Betreiber, auf welchen das NCSC 2023 die meisten Phishing-Webseiten identifiziert hat.

Rang	Phishing-Seiten	Domain-Name	Betreiber	Land
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	Russland
10	72	dweb.link	Protocol Labs	USA
11	71	sviluppo.host	n/a	n/a
12	71	cleverapps.io	Clever Cloud	Frankreich
13	54	wpengine.com	WP Engine	USA
14	53	builderallwppro.com	n/a	n/a
15	51	r2.dev	Cloudflare	USA

Weitere Phishing-Varianten

Smishing – Phishing per SMS

Im vergangenen Jahr konnte das NCSC eine Zunahme von «Smishing» feststellen. Anders als beim herkömmlichen Phishing erfolgen die Betrugsversuche dabei via SMS oder dem SMS-Nachfolger RCS, der bei vielen Messenger-Diensten eingesetzt wird. Dabei wurden im vergangenen Jahr grösstenteils Markennamen von Brief- und Paketzulieferer missbraucht, um den Empfänger auf eine Phishing-Webseite zu ködern, welche diesem dann versucht Kreditkarten-Informationen zu entlocken.

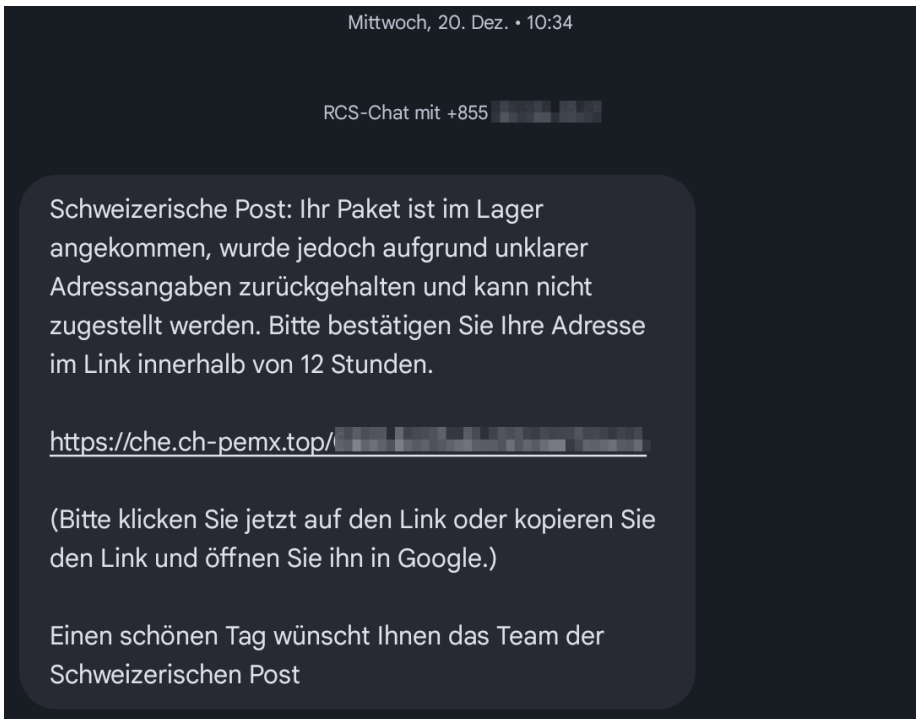

Abbildung 6 - Beispiel einer Smishing-Nachricht (SMS/RCS)

Anders als bei E-Mail basiertem Phishing lassen sich verdächtige oder betrügerische SMS nicht einfach an antiphishing.ch weiterleiten, was eine Erfassung sowie das Einleiten geeigneter Gegenmassnahmen durch das BACS erschwert. Die Anwender müssen sich auf die Schutzmassnahmen des jeweiligen Telekomanbieters oder Betriebssystem-Herstellers verlassen.

Wenn Suchmaschinen zur Phishing-Falle werden

Suchmaschinen sind heute aus dem digitalen Alltag nicht mehr wegzudenken. Sie erlauben uns, innert Kürze Informationen im World-Wide-Web zu finden, sei dies über eine Feriendestination, eine/n Künstler/in oder einer Information, welche wir bei unserer Arbeit benötigen. Am häufigsten genutzt werden in der Schweiz die Suchmaschinen Google (Alphabet) und Bing (Microsoft).

Das Angebot von Suchmaschinen ist gratis. Damit der Anbieter den Dienst jedoch gratis anbieten kann, ist dieser auf Einnahmen angewiesen. Ein weitverbreitetes und zugleich lukratives Geschäftsmodel ist der Werbemarkt. Dabei vermieten die Anbieter von Suchmaschinen die ersten Plätze für Suchresultate an Werbende. So kann es sein, dass wenn Internetnutzende

nach einem Hotel suchen, nicht die tatsächliche Webseite des gesuchten Hotels zuoberst in den Suchresultaten erscheint, sondern vielleicht ein Hotel der Konkurrenz. Dies, weil der Konkurrent den Suchmaschineanbieter für eine solche Werbeeinblendung bezahlt.

Für Unternehmen, welche solche Werbungen aufschalten, sind Suchmaschinen sehr lukrativ. Durch das sogenannte «Profiling» lassen sich Werbungen gezielt an das gewünschte Zielpublikum ausrichten. Die Werbeeinblendungen bekommen dann nur diejenigen Benutzenden zu sehen, welche dem Zielpublikum entsprechen. Hier sind die Möglichkeiten beinahe unbegrenzt: Alter, Geschlecht, Interessen aber auch das Land, aus welcher die Suchanfrage gestellt wird, oder die vom Web-Browser verwendete Sprache. Diese Möglichkeiten sind jedoch nicht nur für Unternehmen mit legitimen Interessen attraktiv. Auch Cyberkriminelle haben bereits vor längerer Zeit erkannt, dass solche Werbeeinblendungen eine verlässliche Möglichkeit bieten, um potenzielle Opfer auf Phishing-Webseiten zu locken.

In der zweiten Hälfte 2023 hat das NCSC vermehrt Meldungen zu schädliche Werbeeinblendungen auf Suchmaschinen erhalten – sogenannte «Rogue Ads». Aktuell werden vergleichsweise viele davon auf Bing (Microsoft) geschaltet. Dabei mieten Cyberkriminelle mit Hilfe von gehackten Publisher-Konten oder gestohlenen Identitäten Werbefläche für ein Stichwort auf Bing. Als Stichworte verwenden die Cyberkriminellen dabei Namen von bekannten Schweizer Finanzinstituten oder Kreditkartenausteller. Sucht nun ein potenzielles Opfer auf Bing nach dem E-Banking seiner Hausbank, kriegt dieses als oberstes Suchresultat die Werbeeinblendung der Cyberkriminellen zu sehen. Die Werbeeinblendung ist so konstruiert, dass diese suggeriert, dass es sich um das tatsächliche Suchresultat für das E-Banking System der Bank handelt. Klickt das Opfer auf die Werbung, führt diese das Opfer auf eine Phishing-Webseite der Cyberkriminellen. Mittels «Real-Time-Phishing» ist die Phishing-Webseite in der Lage, auch auf mittels Multi-Faktor-Authentifizierung (MFA) abgesicherte E-Banking Systeme zuzugreifen.

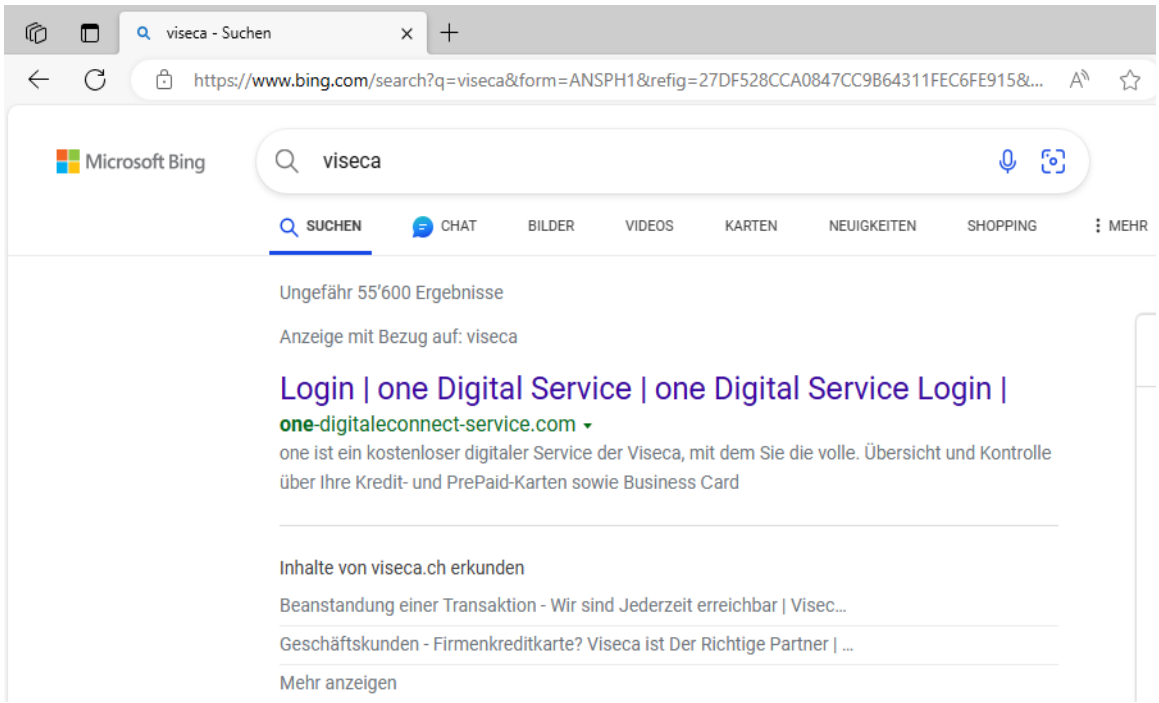

Abbildung 7 - Beispiel einer «Rogue Ad» auf einer Suchmaschine, welche zu einer Phishing-Webseite führt

Für Cyberkriminelle ist dieser Modus Operandi in vielerlei Hinsicht vorteilhaft. Einerseits können diese gezielt auswählen, wer die schädliche Werbung angezeigt bekommt (für eine Kantonalbank in der Romandie können die Cyberkriminellen das Ausliefern der Werbung auf «Schweiz» und die Sprache «Französisch» einschränken). Andererseits müssen diese, anders als bei Phishing via E-Mail, sich nicht mit Spam-Filtern herumschlagen, welche die Phishing-E-Mail möglicherweise als Spam klassifizieren.

Gleichzeitig birgt der Modus Operandi Probleme für Sicherheitsdienstleister und Behörden wie das BACS, welche gegen Phishing im Cyberraumvorgehen. So gibt es seitens Suchmaschinenanbieter keine Transparenz darüber, wer welche Werbung geschaltet hat. Eine Früherkennung ist daher nicht möglich. Das BACS kann somit erst dann aktiv werden, wenn die schädliche Werbung bereits geschaltet ist und von Bürgerinnen und Bürger oder von einer kritischen Infrastruktur gemeldet wird. Aus diesem Grund ist das BACS sehr dankbar, wenn es Meldungen dazu aus der Bevölkerung, von Unternehmen, Behörden und Organisationen erhält.

Empfehlungen

Seien Sie grundsätzlich skeptisch gegenüber E-Mails und SMS, welche Sie dazu verleiten möchten, auf einen Link zu klicken. Zusätzlich empfiehlt das BACS folgendes:

- **Meldung an das BACS:** Melden Sie verdächtige E-Mails oder Webseiten dem BACS auf antiphishing.ch. Falls Sie eine Rückmeldung zu Ihrer Meldung wünschen verwenden Sie als Alternative das Meldeformular auf https://www.report.ncsc.admin.ch/

- **Seien Sie skeptisch**: Keine Bank und kein Kreditkarteninstitut wird Sie jemals per E-Mail oder SMS auffordern, Passwörter zu ändern oder Kreditkartendaten zu verifizieren.

- **Multi-Faktor-Authentisierung (MFA):** Aktivieren Sie auf Ihren Online-Konten wie beispielsweise E-Mail oder Social Media wenn immer möglich eine Multi-Faktor-Authentisierung (MFA). Prüfen Sie Ihre Kontoeinstellung Ihres Anbieters, ob MFA angeboten wird und aktivieren Sie diese Option.

- **Mehrfachverwendung von Passwörtern:** Verwenden Sie niemals dasselbe Passwort für mehrere Online-Konten. Verwenden Sie einen Passwort-Manager für die Verwaltung Ihrer Zugangsdaten.

- **Kreditkartenabrechnung:** Prüfen Sie regelmässig Ihre Kreditkartenabrechnung auf Unstimmigkeiten und wenden Sie sich bei unbekannten Transaktionen sofort an Ihren Kreditkartenanbieter.

- **SMS-Filter:** Aktivieren Sie den SMS-Filter Ihres Betriebssystems auf Ihrem Smartphone, um verdächtige SMS zu filtern.

- **Verwendung von Favoriten:** Verwenden Sie für den regelmässigen Zugriff auf Online-Konten wie beispielsweise E-Banking, Social-Media oder E-Mail die Favoriten («Bookmarks»)-Funktion Ihres Web-Browsers.

- **Spoofing:** Bedenken Sie, dass Absender von E-Mails und SMS aber auch Rufnummern von eingehenden Telefonanrufen einfach zu fälschen sind. Verlangen Sie im Zweifelsfalle, dass Sie den Anrufenden zurückrufen können.