



# netidee

PROJEKTE

Vorsicht Falle!

Endbericht | Call 16 | Projekt ID 5736

Lizenz CC-BY

# Inhalt

Einleitung.....	3
Projektbeschreibung.....	3
Verlauf der Arbeitspakete.....	4
Arbeitspaket 1 – Detailplanung und Formales am Projektstart.....	4
Arbeitspaket 2 – Konzeption.....	4
Arbeitspaket 3 – Betrugsfallen.....	9
Arbeitspaket 4 – Einbettung in die Watchlist Internet.....	13
Arbeitspaket 5 – Dissemination.....	15
Umsetzung Förderauflagen.....	19
Liste Projektendergebnisse.....	19
Verwertung der Projektergebnisse in der Praxis.....	19
Öffentlichkeitsarbeit/ Vernetzung.....	21
Eigene Projektwebsite.....	21
Geplante Aktivitäten nach netidee-Projektende.....	21
Anregungen für Weiterentwicklungen durch Dritte.....	22

## Einleitung

Seit dem Jahr 2015 fußen die Präventionsaktivitäten der Watchlist Internet vor allem auf Newsartikel zu aktuellen Betrugsfällen und Warnlisten. Die Initiative setzt darauf in Suchmaschinen gut gereiht zu sein, um von österreichischen Konsument:innen rasch gefunden zu werden – im Idealfall noch bevor jemand in eine Falle getappt ist. Die Website erreichte im Jahr 2022 über drei Millionen Personen, ein bisheriger Rekord der Reichweite.

Trotzdem ist sich die Initiative bewusst, dass es laufend innovative Überlegungen braucht, um mehr Menschen zu erreichen – nicht nur mit der Information zu sicherem Verhalten im Netz, sondern vor allem mit dem situativen Handwerkszeug für die konkret im Umlauf befindlichen Fallen.

Aus dieser Motivation ist das Projekt „Vorsicht Falle!“ entstanden: Die Präventionserfahrung hat gezeigt, dass vor allem aus der schlechten Erfahrung gelernt wird. Diesen Lerneffekt zu erreichen, ohne dass dabei Schaden entsteht, ist das Ziel von simulierten Fallen. Sie erlauben es Betrugsfällen nicht abstrakt erklären zu müssen, sondern konkret vorzeigen zu können und noch dazu eröffnen sie die Möglichkeit Erfahrung zu simulieren.

## Projektbeschreibung

*Beschreibung der Projektziele / Zielgruppe und inhaltlicher Überblick über das Projektergebnis (max. 5 Seiten)*

Im Projekt „Vorsicht Falle!“ war das Ziel realistische Betrugsfälle nachzubauen, um einen höheren Präventionseffekt zu erzielen. Konkret ging es uns darum für die Watchlist Internet zu erproben, welchen Aufwand diese Methode birgt und inwiefern sich Fake-Fallen künftig als ergänzendes Element in die Watchlist Internet einbauen lassen. Das Nachbauen von Fake-Fallen erweist sich für manche Fälle als besonders einfach, für andere ist mit einem höheren Aufwand zu rechnen. Als die größte Herausforderung stellte sich die Verbreitung der Fälle heraus. Es wurde insofern gerade in diese Arbeitsschritte viel Zeit investiert, denn die Reichweite ist ein wichtiger Indikator des Erfolgs von Präventionsmaßnahmen.

Entwickelt wurde ein Fake-Fake-Shop sowie zwei Fake-Gewinnspiele – sie werden jedenfalls über das Projektende hinaus von der Watchlist Internet genutzt werden und es zeigten sich bereits in der Projektlaufzeit zahlreiche externe Personen bzw. Organisationen, die an den Simulationen interessiert sind, sowohl auf nationaler als auch auf internationaler Ebene.

## Verlauf der Arbeitspakete

### Arbeitspaket 1 – Detailplanung und Formales am Projektstart

Es wurden alle Tasks von AP1 abgeschlossen, dazu zählt u. a.: Vertrag unterschrieben, Detailprojektplan erstellt und abgenommen, Liste der Projektergebnisse erstellt und abgenommen.

### Arbeitspaket 2 – Konzeption

In AP2 vorgesehen ist die Konzeption der Betrugsfallen-Simulation. Das Projektkonzept beruht darauf, die etablierten Wege der Wissensvermittlung der Watchlist Internet zu nutzen, um diese durch Fallen als spielerische Elemente zu ergänzen. User:innen erhalten die Möglichkeit, statt einen Newsartikel, eine simulierte Falle zu teilen. Sie tragen so zu einer effektiven Prävention bei. In der Konzeption haben wir ein 5-Phasen-Modell entwickelt, um die vorgesehene User-Journey zu systematisieren (siehe Zwischenbericht): (1) Erstkontakt, (2) Narrativ, (3) Falle, (4) Schockmoment und (5) Auflösung.

## 5-Phasen-Modell der simulierten Online-Fallen



Abbildung 1: Das Konzept – 5-Phasen-Modell der simulierten Onlinefallen

Im Zwischenbericht ausführlich beschrieben wurde das erste erstellte Konzept einer Falle, für ein Amazon-Gewinnspiel. Die UX-Wireframes wurden mit dem Tool UXpin erstellt (siehe Zwischenbericht für Screenshots). Im Zeitraum seit Zwischenbericht, wurden angelehnt an die Amazon Gewinnspiel Falle eine weitere Falle konzipiert und entwickelt – ein ÖBB-Gewinnspiel.

Ein wichtiges weiteres Konzept war die Erstellung eines Fake-Shops. Das Ziel dabei war möglichst nahe an einem aktuellen Fake-Shop eine Falle zu entwickeln. Es zeigten sich dabei die folgenden Herausforderungen:

- **Produktfotos:**

Zahlreiche Fake-Shops nutzen Fotos zur Bewerbung von Produkten, für die sie keine Rechte haben. Dabei handelt es sich um von legitimen Shops kopierten Produktfotos oder gerade im Modebereich, um Fotos deren Inhaber:innen-Status ungeklärt ist. Folgende Möglichkeiten kamen in Frage, um Bilder entsprechend des geltenden Rechts verwenden zu können:

- Kooperationen mit Rechte-Inhaber:innen
- Akquirierung der Bildrechte
- Nutzung von lizenzfreien Fotos
- Anfertigung eigener Fotos

Da eine Unternehmenskooperation in diesem frühen Stadium des Projekts als unrealistisch erschien, gingen wir den Optionen b, c und d nach. Um umfassende Produktkataloge bereitstellen zu können, eignen sich lizenzfreie Fotos kaum – es konnten nicht genügend Produkte, die demselben Stilschema folgen bzw. auch der gleichen Produktkategorie zuzuordnen sind, gefunden werden. Die eigene Anfertigung von Produktfotos ist mit einem erheblichen finanziellen Aufwand verbunden und wurde deshalb ebenfalls ausgeschlossen. Angedacht wurde hinsichtlich einer eigenen Erstellung von Fotos die Nutzung von KI-generierten Produktbildern. Die damit zu erreichende Qualität eignet sich für den Nachbau von Fake-Shops mit Modeprodukten oder sehr breiten Produktpaletten, die mit sehr schlechten Fotos arbeiten, die ebenfalls teilweise automatisch generiert wirken. Es bleiben Fehler in der Darstellung offensichtlich vorhanden und insofern wurde im Projekt entschieden diesen Weg vorerst außen vor zu lassen. Er bleibt als Option für künftige Fake-Shops erhalten.



Abbildung 2: 1. Von der KI Crayon (damals DALLE mini) erstellte Produktbilder

Die Überlegungen drehten sich also um den Erwerb von Produktfotos und nach Recherche in Stock-Foto-Archiven eröffneten sich zwei Möglichkeiten für Shops: Zu finden sind zahlreiche Fotos, die für einen Shop mit Einrichtungsmöbeln genutzt werden könnten, zu finden sind auch zahlreiche Fotos von No-Name Produkten zum Beispiel Parfums, Kleidungsstücke, Getränkedosen, technische Geräte. Wir entschieden uns für die Wahl eines Themas, das derzeit besondere Aufmerksamkeit erhält und bei dem die Shops mit geringen Produktpaletten und relativ generischen (Marken-freien) Produkten gefüllt sind: Onlineshops, die auf das Thema Survival, Vorsorge bzw. Blackout-Prävention setzen. Es wurden Bilder gekauft und adaptiert.

- **Schockmoment:**

Anders als bei den Fake-Gewinnspielen, bei denen das Versprechen eines möglichen Gewinns bereits ausreichende Motivation für viele sein kann, um ein Formular auszufüllen, ist diese Niederschwelligkeit bei einem Fake-Shop nicht gegeben. Vielmehr stellt sich bei Fake-Shops die Frage, zu welchem Zeitpunkt eines Einkaufs die Warnung stattfinden sollte. Als Optionen kamen in Frage, dass die Nutzer:innen erst nach dem versuchten Einkauf darüber informiert werden, dass sie in einem nicht-existenten, aber zum Glück durch Präventionsexpert:innen aufgebauten Fake-Shop eingekauft hätten. Vorteil an dieser Lösung wäre, dass der Schockmoment, definiert als ein wichtiger Lernmoment, groß sein könnte. Der Nachteil wäre, dass zum einen die von den User:innen geteilten Daten umfassend und sensibel sind, zum anderen die Rückführung auf die Website sich technisch kompliziert gestalten könnte. Entschieden wurde, dass sobald jemand beginnt das Bestellformular auszufüllen, anzunehmen ist, dass eine Kaufabsicht besteht. Um das Problem rund um geteilte Daten zu umgehen, wird insofern schon bei den ersten eingegebenen

Buchstaben ein Pop-Up ausgelöst – der Schreckmoment ist geringer, insofern noch nicht bezahlt wurde, dafür stellen sich Probleme rund um die geteilten Daten nicht.

- **Auflösungen**

Die Auflösungen tragen die folgende Problematik: Ist der Schockmoment groß, ist die Entwarnung gleichsam wenig vertrauenserweckend. Bei den Fake-Gewinnspielen ist der Schock über das Overlay sehr groß – entsprechend war die Sorge, dass Personen einer Entwarnung kaum Glauben schenken könnten. Es wurde insofern auf die Integration vertrauensbildender Elemente Wert gelegt – die Einbettung in die Watchlist Internet, der Veweis auf Fördergeber:innen etc. wurde als prioritär angesehen.

Auch bei dem simulierten Fake-Shop wurde zunächst eine Weiterleitung auf die Website der Watchlist Internet eingerichtet. Auf dieser waren Informationen zum Projekt im Sinne der Vertrauensbildung, sowie die Möglichkeit zu einer Tour zurück auf den Fake-Shop geleitet zu werden. Die Praxis zeigte allerdings, dass an dieser Stelle viele User:innen verloren gingen – die bis zur Watchlist, allerdings nicht mehr zurück auf die Tour gelangen. Weil die Tour ein integraler Bestandteil der Aufklärungsarbeit ist, wurde deshalb entschieden direkt der Kassa auf die Tour der Website zu leiten.

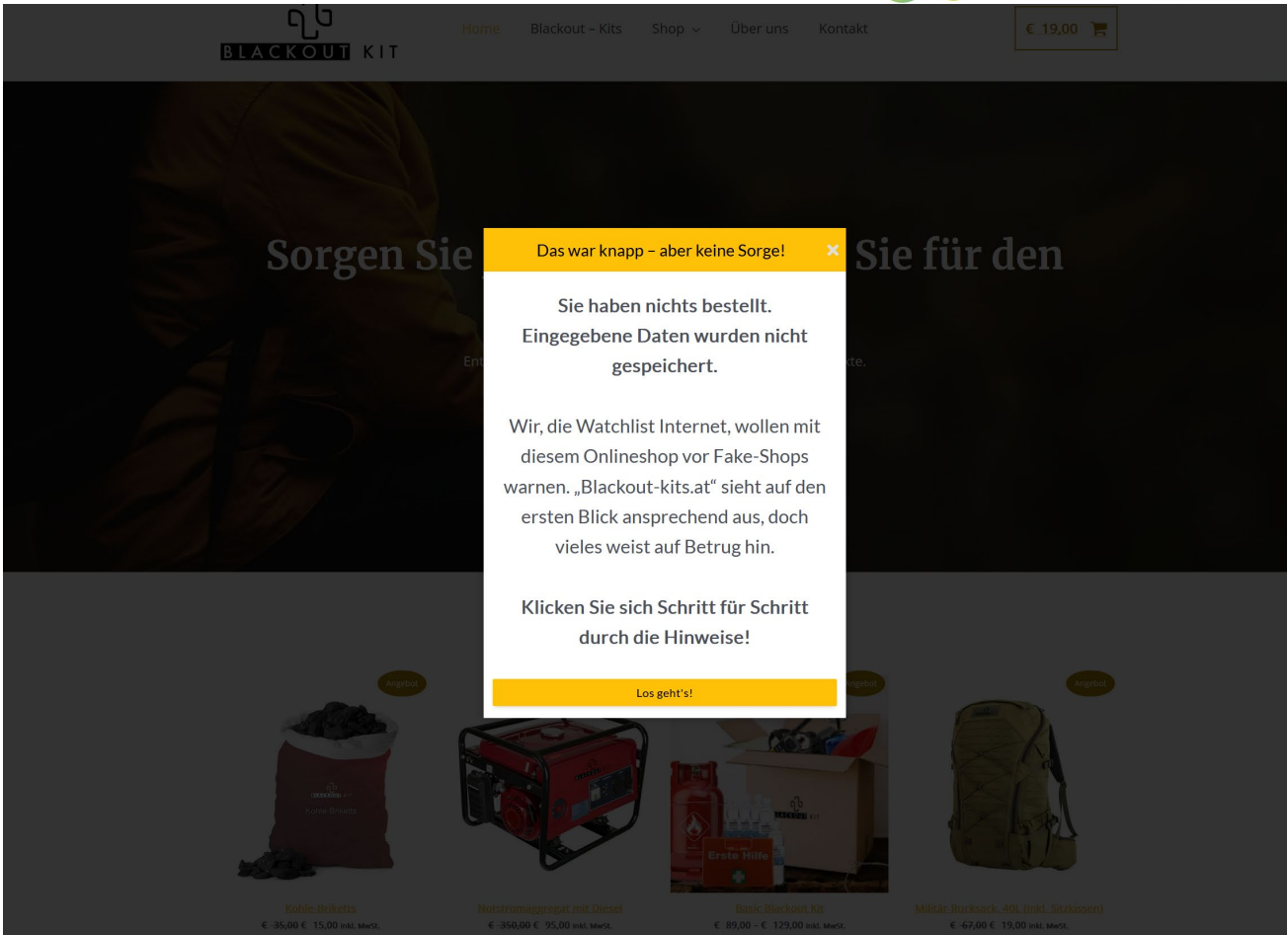


Abbildung 3: 1. Screenshot der Tour durch www.blackout-kits.at

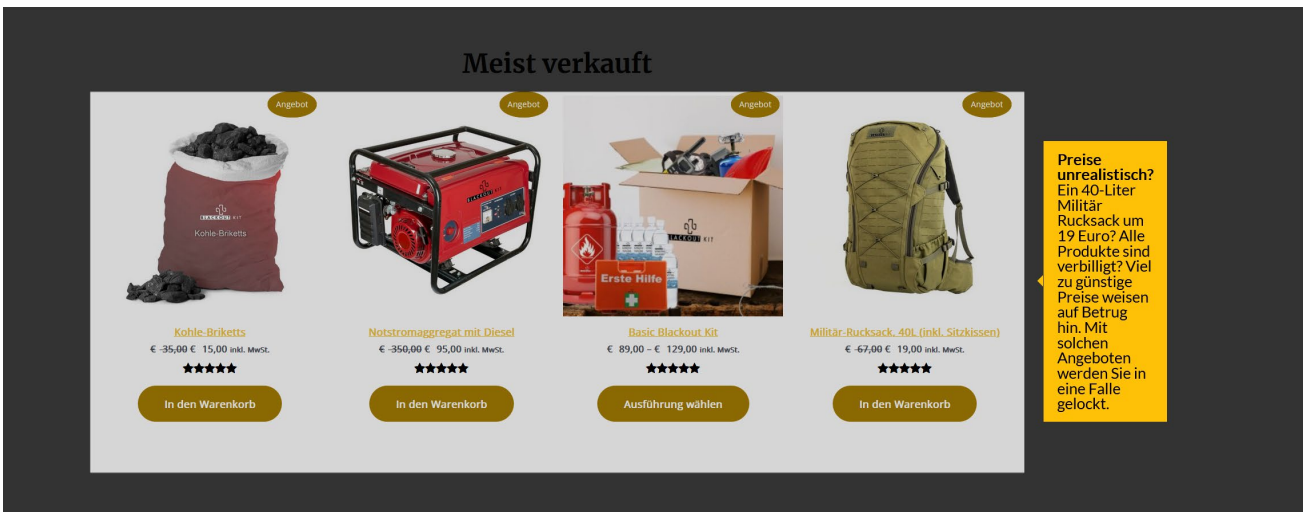


Abbildung 4: 2. Screenshot der Tour durch www.blackout-kits.at.



### Arbeitspaket 3 – Betrugsfallen

Im Arbeitspaket 3 wurden drei Betrugsfallen entwickelt: Ein Fake-Gewinnspiel zu einem Amazon- und zu einem ÖBB-Jubiläum sowie einen Fake-Shop rund um das Thema Black-Out. Die technische Erstellung der Fake-Gewinnspiele konnte intern vom ÖIAT umgesetzt werden. Bevor es an die tatsächliche Erstellung der Fallen ging, wurde die Registrierung einer Domain diskutiert. Die Entscheidung fiel schließlich auf die Domain gewlnnspiel.at, da diese mit Hilfe von Subdomains für mehrere Fallen verwendet werden kann. Zusätzlich orientiert sich so die Domain bereits an zwei beliebten Tricks von Betrüger:innen. Die Top-Level-Domain .at soll vertrauenswürdig wirken, das gleiche gilt für das Typosquatting. Beim letzteren werden Domains mit kleinen Fehlern registriert – meist um Webseiten bekannter Unternehmen nachzuahmen. Die Fehler fallen nur bei genauerer Betrachtung auf: So wie bei gewlnnspiel.at, das mit einem l und nicht mit einem i geschrieben wird.

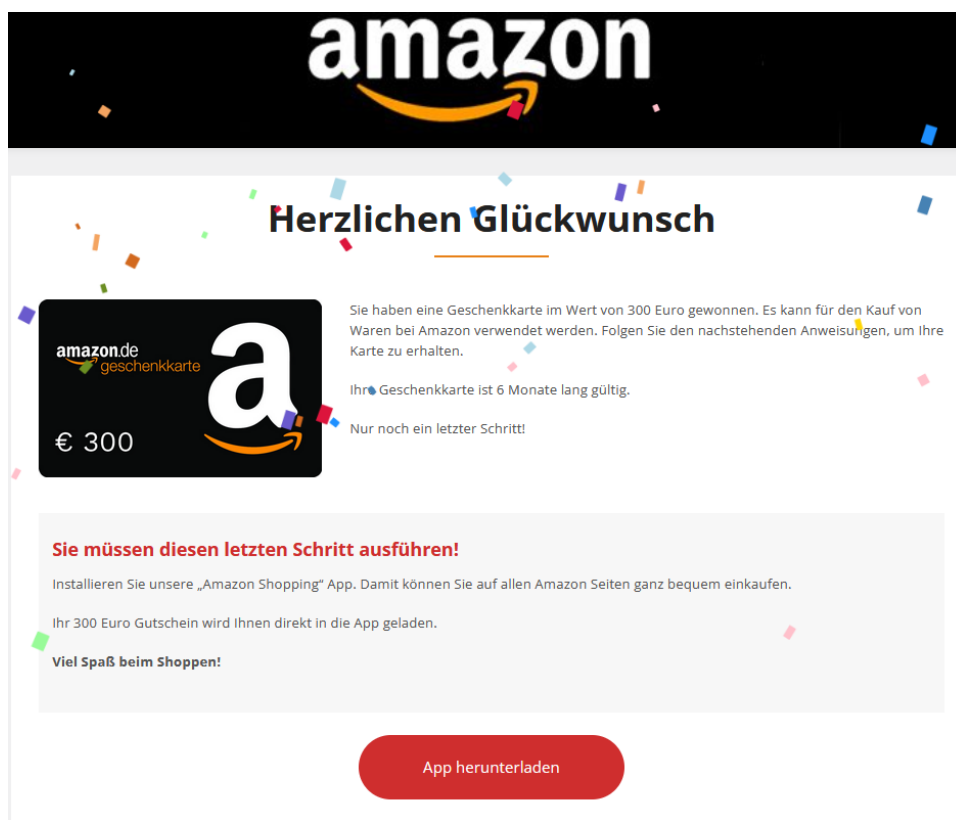


Abbildung 5: 2. Screenshot der Amazon-Falle



## Gewinnen Sie 2.000 Euro!

🕒 ÖBB – 100 Jahre Staatliche Verkehrsförderung! Gewinnspiel nur noch **29 Minuten** online ⚡

Für unser Jubiläum, haben wir uns etwas besonderes einfallen lassen!

Machen Sie bei unserem kleinen Spiel mit und mit etwas Glück erhalten Sie ÖBB-Gutscheine im Wert von bis zu 2.000 Euro.

Klicken Sie auf die Logos und finden Sie alle Paare. Wir drücken die Daumen!



Abbildung 6: 2. Screenshot der ÖBB-Falle

Die Erstellung der Fallen läuft über das Content-Management-System Wordpress. Innerhalb dieses Backend wurden verschiedene Themes, Plugins und weitere Tools erprobt, die dabei helfen sollen, die jeweiligen Fallen möglichst so zu gestalten, dass sie jenen der Betrüger:innen ähneln. Bei der Auswahl der jetzt verwendeten Tools und Plugins waren vor allem Datenschutzkonformität sowie die Einfachheit in der Handhabung zentrale Kriterien. Letzter Punkt soll gewährleisten, dass der Aufwand und die Komplexität für die Erstellung der Fake-Gewinnspiele möglichst gering ist, damit das Watchlist Internet Team auch künftig im Zuge der laufenden Redaktionsarbeit solche Fallen gestalten kann. Eine entsprechende Dokumentation, die vom Team genutzt werden kann, wurde bereits erstellt.

Ein wichtiges Element der Betrugsfallen ist zudem die Auflösung – diese wurde für den Anwendungsfall Fake-Gewinnspiel folgendermaßen gelöst: Wer in eine Falle tappt, wird auf die Watchlist Internet weitergeleitet, wo in Kürze das Projekt erklärt wird und die Möglichkeit zu einer Tour durch die Falle gegeben wird. Da die Watchlist Internet über das Content-Management-System Typo3 läuft und existierende Plugins nicht den Bedürfnissen der Auflösungsseiten gerecht werden, wurde ein eigenes Tour-Tool entwickelt, das es ermöglicht

Screenshots der jeweiligen Falle auf watchlist-internet.at hochzuladen und an diesen zu erklären, wie man die jeweilige Falle erkennen kann.

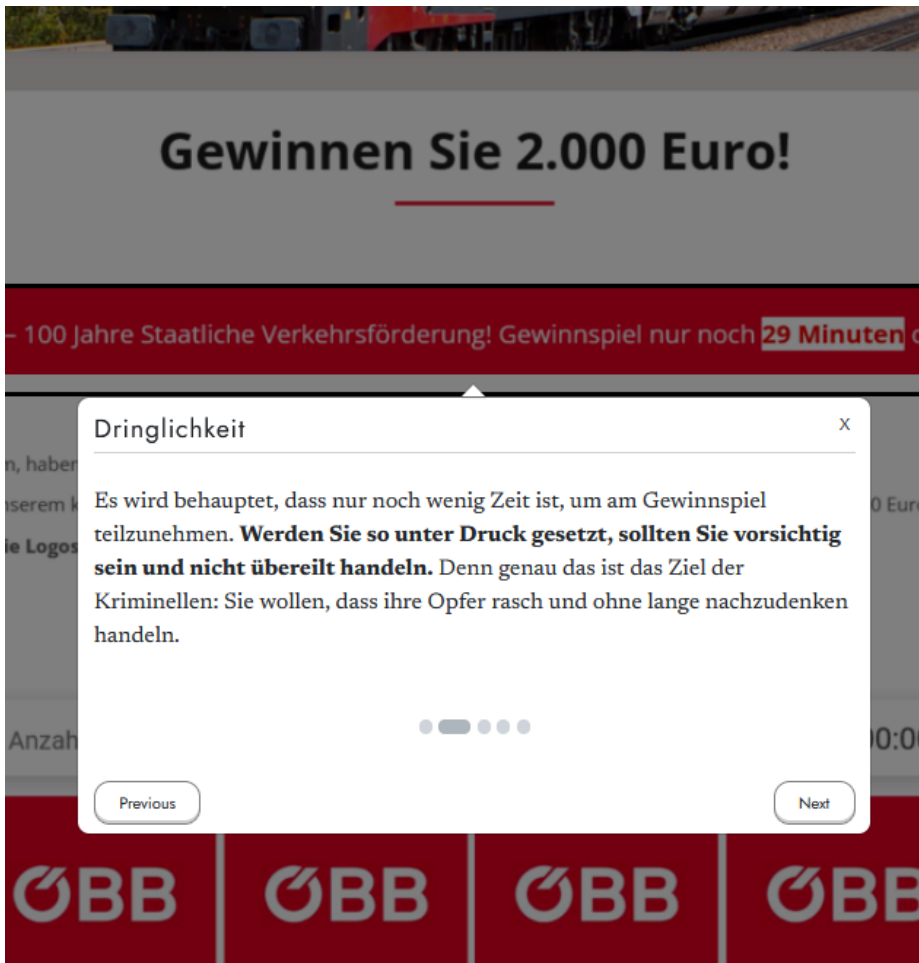


Abbildung 7: 2. Screenshot der Tour auf watchlist-internet.at.

Als komplexer stellte sich die Erstellung eines Fake-Shops heraus. Zwar können Shop-Systeme inzwischen genutzt werden, die eine rasche Erstellung erlauben – jedoch ist der Zeitaufwand zur vollständigen Befüllung eines Webshops mit Produkten, Produktbeschreibungen, Reviews, sowie der weiteren zu erstellenden Texte wie Datenschutz oder Rückversandbedingungen hoch. Entschieden wurde deshalb eine erfahrene Webshop-Agentur in die Erstellung des Shops einzubeziehen. Die Agentur LimeSoda konnte dafür gewonnen werden, dies im Sinne eines CSR-Projekts umzusetzen. Erstellt wurde der erste Prototyp des Fake-Fake-Shops durch ihre Unterstützung. Die erworbenen Produktfotos wurden vom ÖIAT entlang eines eigens für den Shop entwickelten Logos angepasst und es wurden Reviews durch angebliche Käufer:innen sowie Produktbeschreibungen verfasst. Der Aufwand für die Entwicklung dieser Falle war deutlich höher als für die Gewinnspiel-Fallen.



Abbildung 8: 2. Screenshot des Fake-Fake-Shops *blackout-kits.at*.

Als zusätzliche Herausforderung beim Betrieb des Fake-Fake-Shop stellte sich die Auflösung heraus: Entscheidend war hier nicht nur den Zeitpunkt der Auflösung, sondern Fragen technischer Natur. Zunächst war geplant die User:innen auf eine Auflösungsseite der Watchlist Internet zu führen, um ihr Vertrauen wieder herzustellen – und sie dann für eine Tour zur Seite zurückzuführen. Auch nach längerer Recherche wurden jedoch weder kostenfreie noch kostenpflichtige Plugins gefunden, die eine Tour anbieten, die auf einer externen Seite eingebettet werden kann. Die Alternative: Die Nutzer:innen werden auf die Watchlist Internet geführt, dort kurz über das Projekt aufgeklärt und anschließend wieder auf den Shop verwiesen, um die Tour mit den Betrugshinweisen durchzuspielen. Zwar funktionierte die Tour nun mit Hilfe eines kostenpflichtigen Plugins, dennoch stellte sich diese Lösung als wenig praktikabel heraus – zu viele Nutzer:innen klickten von der Watchlist Internet nicht mehr auf den Link zur Tour. Der Präventions- und Lerneffekt war dementsprechend niedriger. Der Schritt über die Watchlist Internet wurde daher weggelassen, stattdessen öffnet sich nun bei der Eingabe der Daten direkt die Tour – wobei im ersten Tour-Schritt erklärt wird, dass es sich um ein Projekt der Watchlist Internet handelt. Da der Schockmoment beim Fake-Fake-Shop geringer ist als bei den Fake-Gewinnspielen, ist die vertrauenswürdige Umgebung der Watchlist Internet nicht unbedingt notwendig. Es reicht, die Nutzer:innen erst am Ende der Tour auf die Website der Watchlist Internet zu führen.

## Arbeitspaket 4 – Einbettung in die Watchlist Internet

Das Ziel des Arbeitspakets 4 war die Einbettung der Fallen in die Watchlist Internet sowie die Möglichkeit, dass diese von den User:innen selbst umgestaltet werden können. Letzteres wurde aufgrund rechtlicher Probleme (bspw. Bildrechte) verworfen. Stattdessen lag der Fokus auf der Verbreitung der Fallen, interessierte User:innen wurden als Disseminationsagent:innen eingebunden. Auf der Projektwebsite werden User:innen dazu angeleitet mittels vor-formulierter Textbausteine die Fallen an Bekannte, Freund:innen oder Familienmitglieder weiterzuleiten. Ebenfalls als Option angeführt ist, dass die Fallen auch transparent im Sinne von Fake-Fallen verbreitet werden können.

### Wie können Sie mitmachen?

- Sehen Sie sich unsere Fake-Fallen an und wählen Sie eine aus.
- Kopieren Sie den dazugehörigen Link und überlegen Sie sich einen Text dazu oder nutzen Sie unsere Textvorschläge als Inspiration.
- Senden Sie Link und Text an die Person, die Sie – mit den besten Absichten, versteht sich – in die Falle locken wollen. Dafür fügen Sie Link und Text einfach in eine E-Mail, eine SMS oder eine Messenger-Nachricht (zum Beispiel WhatsApp oder Signal) ein oder klicken auf eines der Symbole, um beides direkt zu versenden.

⚠ Sie wollen Ihre Familie oder Freund:innen nicht ohne deren Wissen in die Falle locken? Kein Problem! Weisen Sie in Ihrer Nachricht einfach darauf hin, dass es keine echte Falle ist. Allein das Durchspielen hilft, Hinweise auf Internetbetrug besser zu erkennen.

Gibt es Probleme oder benötigen Sie Hilfe? Schreiben Sie uns unter [kontakt@watchlist-internet.at](mailto:kontakt@watchlist-internet.at).

*Abbildung 9: Screenshot der Projektwebsite Vorsicht Falle - Anleitung für die Weiterleitung von Fallen.*

Die jeweiligen Fallen werden ansprechend vorgestellt – zur Verfügung gestellt wird ein Textvorschlag, aber auch der Link zur Original-Falle sowie die Möglichkeit der Weiterleitung über soziale Medien bzw. per E-Mail. Alle bisher erstellten Fallen erscheinen untereinander – dieser Aufbau ermöglicht den weiteren Ausbau der Fallen und eröffnet die Möglichkeit die Fallen in unterschiedlichen Settings zu nutzen.

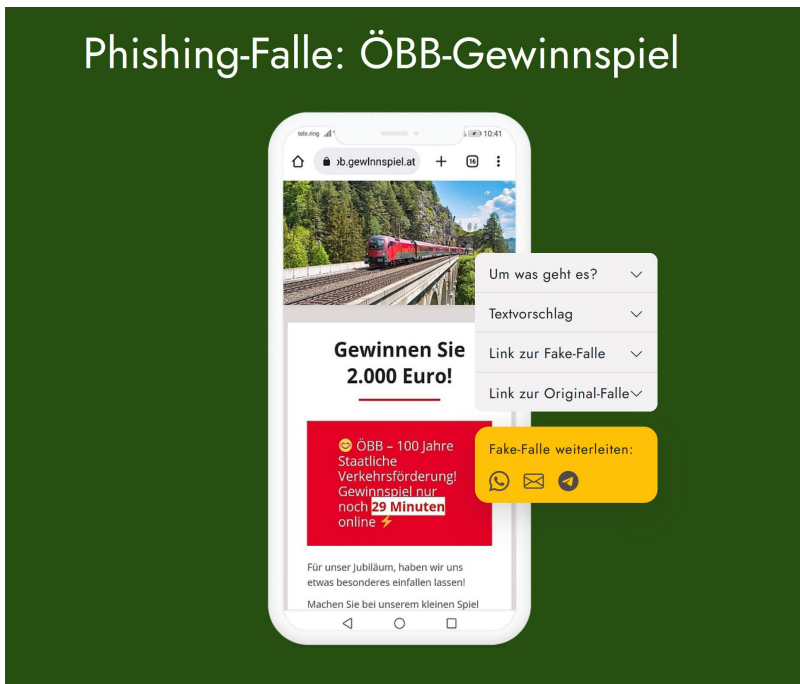


Abbildung 10: Screenshot der vorgestellten Falle.

Zentral im Verwertungskonzept ist, dass die Fake-Fallen an aktuellen Fallen orientiert sind und entsprechend kann in den Warnartikeln zu den jeweiligen Fallen auch die erstellte Fake-Falle gut beworben werden. (Siehe: <https://www.watchlist-internet.at/news/kettenbrief-alarm-angebliches-amazon-gewinnspiel-macht-auf-whatsapp-die-runde/> und <https://www.watchlist-internet.at/news/gefaelschtes-oebb-gewinnspiel-auf-whatsapp/>). Diese Form der Verlinkung hat bislang noch keine große Reichweite gebracht. Zur Veranschaulichung: Der Artikel zum ÖBB-Gewinnspiel (inkl. Hinweis auf Vorsicht, Falle!) wurde am 21.09.2022 veröffentlicht. Die Besucher:innen-Zahl lag an diesem Tag bei 17 Personen und änderte sich auch in den nächsten Tagen kaum. Ein ähnliches Szenario ließ sich auch bei der Amazon-Falle beobachten. Es wurde dennoch entschieden den Zugang zu behalten, dabei sollen die Formen der Verlinkungen und Darstellung der einzelnen Fallen ansprechender gestaltet werden.

Gleichzeitig wird die Verbreitung der Fallen, um weitere Formen der Verwertung ergänzt. Als Alternativkonzept wurde die Kooperation mit Saferinternet.at verstärkt – einer EU-Initiative mit Schwerpunkt Kinder und Jugendliche, die vom ÖIAT geleitet wird. Gerade die Fake-Gewinnspiele sind ein zunehmendes Problem für die Zielgruppe Kinder und Jugendliche – diese sind jedoch derzeit noch nicht eine Kernleser:innen-Gruppe der Watchlist Internet und nutzen andere Kanäle. (Siehe Kapitel 6 für die Verwertungs Ideen in diesem Zusammenhang).

Im Kontext dieser Kooperation als auch bei der Verbreitung über die Watchlist Internet, kam die Diskussion auf, dass die Verwendung von seriösen Unternehmen (ÖBB, Amazon) sich negativ auf

die Verbreitung der Fake-Gewinnspiele auswirken könnte. Um dem entgegenzusteuern, entschied das Team zu Projektende, die Fallen zu ändern und No-Name-Unternehmen bzw. gar keine Unternehmen zu nennen. Aus oebb.gewltnspiel.at wurde daher your-trip.gewltnspiel.at – die Amazon-Gewinnspiele wurden zu elektromarktxl.gewltnspiel.at bzw. elektromarkt-xl.gewltnspiel.at abgeändert.

## Arbeitspaket 5 – Dissemination

**Änderung zu geplanten Aktivitäten:** Im Plan vorgesehen war eine Presseaussendung als klassische Form der Dissemination der Fallen – dies wurde jedoch verworfen, um stattdessen den Fake-Shop über klassische Werbung auf der Produktsuchmaschine Google Shopping zu bewerben. Die damit erzielte Reichweite für die entwickelte Falle geht weit über die Erwartungen hinaus und dieser Erfolg ermöglichte uns auch die weitere Verwertung der Ergebnisse durch Partner sicherzustellen.

- Es sind im Projektzeitraum 12 Blogeinträge auf [www.netidee.at/vorsicht-falle](http://www.netidee.at/vorsicht-falle) erschienen.
- Die Watchlist Internet (Website, Newsletter und Social Media Kanäle) wurden genutzt, um die Falle zu bewerben und User:innen für den ersten Testzeitraum zu gewinnen. Siehe zum Beispiel: <https://www.watchlist-internet.at/news/vorsicht-falle-wir-brauchen-ihre-hilfe-fuer-ein-neues-projekt/>

### **Neuer Disseminationsansatz – die Bewerbung des Fake-Shop auf Google Shopping:**

Der simulierte Fake-Shop ist zwar auch auf der Projektwebsite auf der Watchlist Internet angeführt, allerdings ist die Einbettung in einen Newsartikel nur teilweise als sinnvoll erachtet worden, um nicht nur einzelne, sondern viele User:innen zu erreichen. Der Aufwand zur Erstellung eines Webshops ist ungleich höher als für andere Fallen und der Gedanke, dass jemand über ein Teilen der Fake-Falle jemandem zu einem so spezifischen Einkauf bringt, unrealistisch. Daher entschieden wir Werbekanäle zu testen und den Fake-Fake-Shop, wie es auch bei tatsächlichen Fake-Shops üblich ist, in der Produktsuchmaschine Google listen zu lassen. Es wurde eine Zahl an unterschiedlichen Bewerbungsmöglichkeiten diskutiert, unter anderem Social Media Seiten (vor allem Facebook), jedoch fiel die Wahl schlussendlich auf eine Bewerbung über Google. Zahlreiche Meldungen von Betroffenen an die Watchlist Internet beschreiben, wie die Opfer zu tatsächlichen Fake-Shops gekommen sind, die Google Suche, bzw. Produktsuche rangiert hier auf dem ersten Platz.

## **Die Erstellung des Google-Werbekontos**

Zur optimalen Verbreitung der simulierten Falle Blackoutkits.at, wurde ein Google Merchant sowie ein Google Ads Konto erstellt. Die Erstellung dieser beiden Konten wurde dokumentiert. Hier wurde deutlich, wie barrierefrei Werbung für betrügerische Produkte und Services auf Google geschaltet werden kann. In wenigen Minuten und nach ein paar Klicks, konnte ein Google Konto auf den Namen Blackoutkits Vienna registriert werden. Alle erforderlichen Daten, waren eine gmail-E-Mail-Adresse sowie eine valide Kreditkarte. Weder ein Klarname musste angegeben werden noch eine gültige Adresse. Die angegebene Adresse wurde nicht überprüft, ebenso wurde nicht darauf geachtet, ob diese mit dem Registrar der Kreditkarte übereinstimmt. Einzig ein „Überprüfungs-SMS“ wurde an eine zuvor angegebene Nummer gesendet, die danach nicht wieder abgefragt wurde. Googles Sicherheitsvorkehrungen wurden hier eindeutig im Namen der Usability und User:innen-Freundlichkeit hinten angereicht.

Das Google Merchant und Google Ads Konto wurden miteinander verknüpft, und der Produktfeed von Blackoutkits.at eingespielt. Hierbei wurde mit erfundenen Produkt-IDs gearbeitet, um möglichst viele der Vorgaben von Google für eine optimale Produktauspielung zu erfüllen. Nach einer kurzen Verifikationsperiode (ca. 24h) wurden die zuerst kostenlosen Produktanzeigen (Product Listing Ads - PLA) von Google genehmigt und ausgespielt.

## **Die Anzeigenschaltung**

Um ein möglichst breites Publikum zu erreichen, wurden Produkteinträge für die Google Produktsuchmaschine Google Shopping erstellt, ebenso wie Textanzeigen, die bei einer Stichwortsuche ausgespielt werden. In mehreren Phasen wurde Werbung ausgerollt, um die Anzahl an Impressionen und später auch Klicks zu optimieren. In einer ersten Phase im November 2022, wurden unbezahlte Produktanzeigen (PLAs) geschaltet. Diese erwiesen sich als erfolgreicher als angenommen und erzielten in zwei Wochen mehrere hundert Klicks auf die im Fake-Fake-Shop angebotenen Produkte. Im Zeitraum vom 02. bis zum 27. November wurden kostenlose Produktanzeigen auf Google Shopping geschaltet. Da nur entweder kostenlose oder bezahlte Anzeigen geschaltet werden können, aber nicht kostenlose und bezahlte Anzeigen zum gleichen Zeitpunkt, wurden die kostenlosen Anzeigen ab dem 28.11. von bezahlten Anzeigen abgelöst. Im Zeitraum vom 28.11.2022 bis zum 19.12.2022 wurden mit den bezahlten Produktanzeigen, sowie den bezahlten Textanzeigen 333.600 Impressionen von User:innen und 9.399 Klicks erreicht.



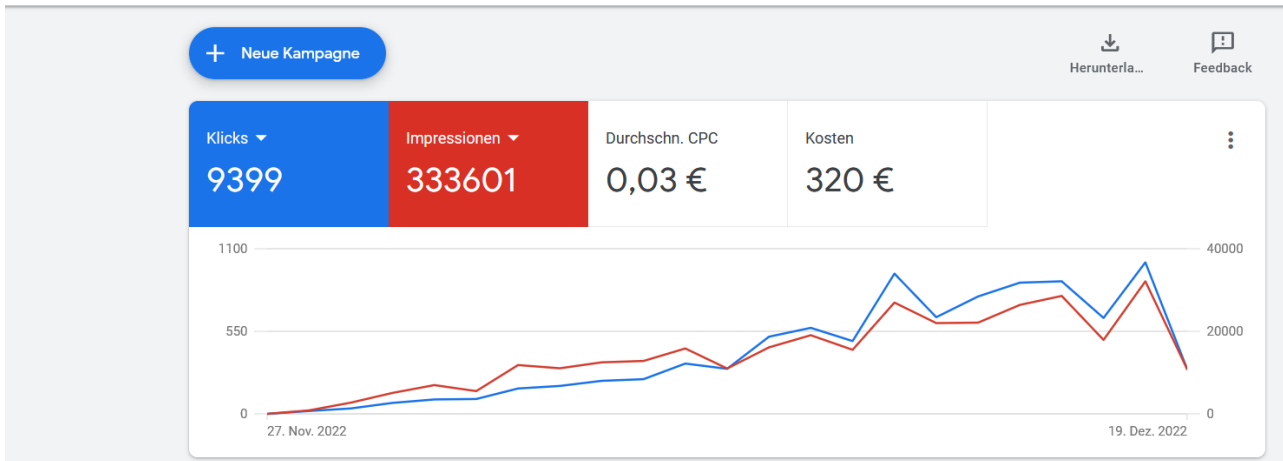


Abbildung 11: Die Anzeigen erzielten eine beeindruckende Anzahl an Impressionen, für einen vergleichsweise geringen Kostenaufwand. Die durchschnittlichen Kosten per Klick betragen nur 0,03 €.

Mit einem Kostenaufwand von ungefähr 320 € im gesamten Zeitraum der Kampagnenschaltung, konnte so eine erhebliche Reichweite mit relativ geringem Kostenaufwand generiert werden. Im gleichen Zeitraum verzeichneten wir 9.940 Besuche sowie 35.552 Seitenansichten. Immerhin 8,5% aller Besucher:innen begannen die Formularfelder auf der Kassa-Seite auszufüllen und gelangten anschließend zur Auflösung (Tour-Seite). Insgesamt klickten sich seit dem Online-Stellen der bezahlten Anzeigen 840 Personen in einem Zeitraum von drei Wochen durch unsere Auflösungs-Tour.

Mit dem gebündelten Werbeaufwand konnte also eine erheblich breitere Schnittmenge der Bevölkerung erreicht werden und insbesondere eine Zielgruppe, die nicht zur traditionellen Leser:innenschaft der Watchlist Internet zählt.

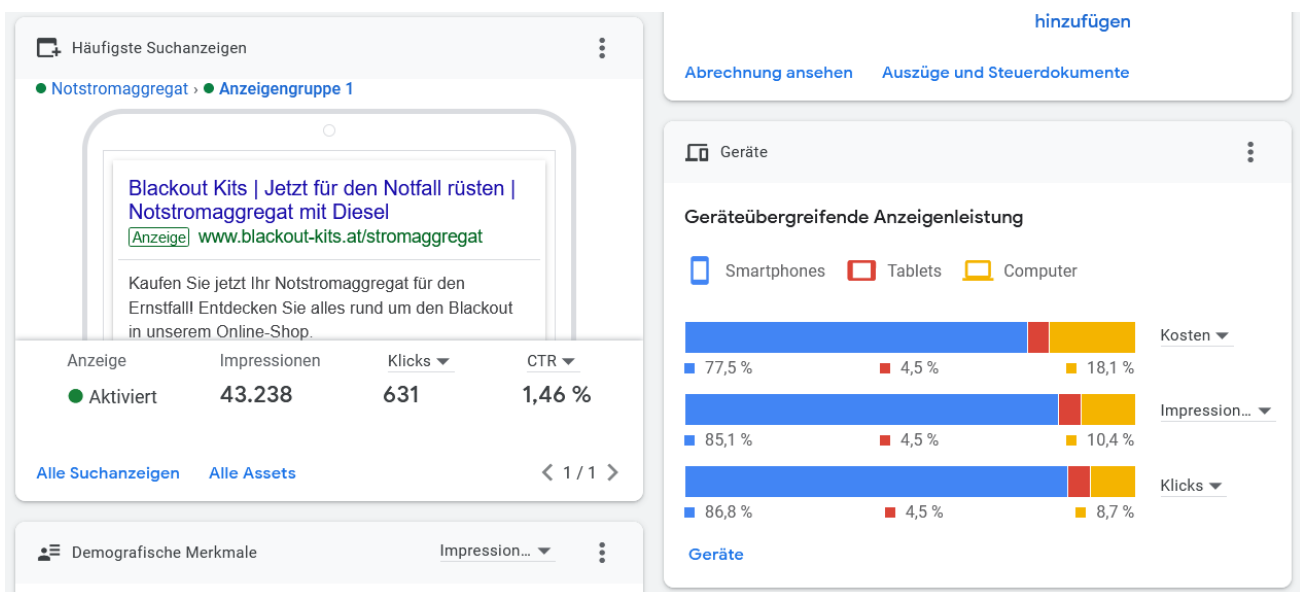


Abbildung 12: Links ein Beispiel der Google-Suchanzeige. Rechts die Anzeigenleistung der Werbeanzeigen insgesamt.

Google Ads erlaubt ebenfalls einen genaueren Einblick in die Demographie der Personen, die von dem Effekt der simulierten Fallen profitierten: Die meisten Impressionen (Personen denen die Anzeigen gezeigt wurden) kamen von Männer zwischen 35 und 54 Jahren, die Anzeigen wurden vorwiegend mit Smartphones oder anderen mobilen Geräten aufgerufen, jedoch ist die Conversion Rate (Anzahl der Personen die auf die Tour Seite kamen) relativ hoch für Laptops und PCs.

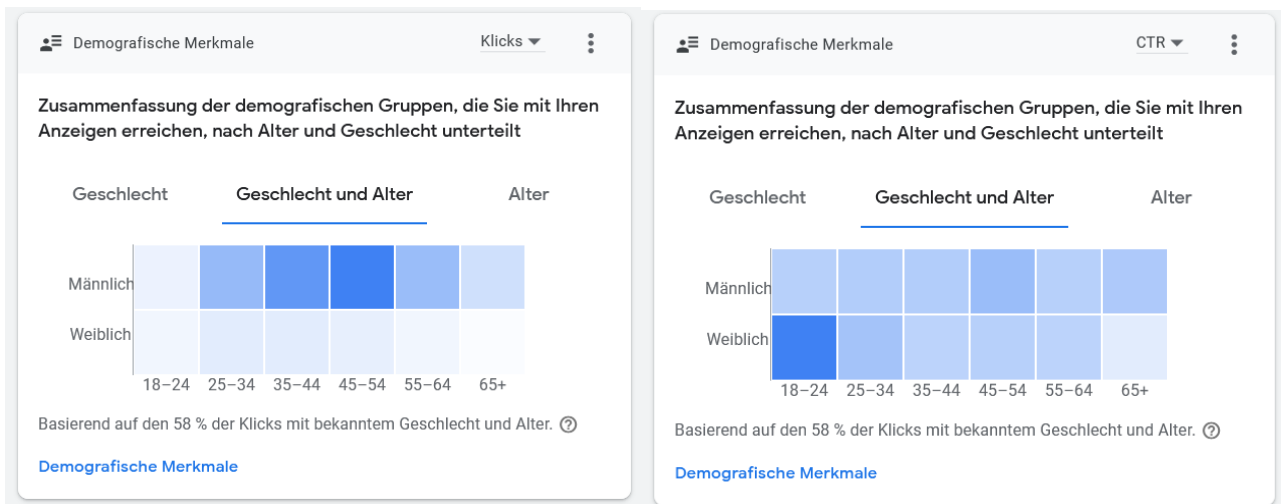


Abbildung 13: Die Verteilung von Geschlecht und Alter der Personen die auf die Anzeigen klicken (links) sowie die Klicks in Relation zu den Impressionen (Click-Through-Rate, rechts).

Interessant ist, dass die Anzeigen vorwiegend Männern zwischen 35 und 54 ausgespielt wurden, allerdings die Click-Through-Rate (Anzahl der Klicks auf die Anzeige) zeigt, dass Männer wie Frauen sehr ausgeglichen auf die Anzeigen geklickt haben. Der Ausreißer in der Gruppe (weiblich 18-24) könnte damit zusammenhängen, dass dieser Gruppe erheblich weniger häufig die Werbeanzeigen ausgespielt wurden.

Die Ansprache neuer Zielgruppen und die Verteilung der simulierten Fallen über Werbeanzeigen, insbesondere Google Ads, erwies sich als äußerst erfolgreich. Es zeigt sich, dass simulierte Fallen als Präventivmaßnahme gut in den organischen Content einfügen und nicht sofort als Simulationen erkannt werden.

## Umsetzung Förderauflagen

Keine Auflagen

## Liste Projektergebnisse

1	Projektzwischenbericht	CC-BY-3.0 AT	netidee.at/vorsicht-falle
2	Projektendbericht	CC-BY-3.0 AT	netidee.at/vorsicht-falle
3	Entwickler:innendokumentation	CC-BY-3.0 AT	netidee.at/vorsicht-falle
4	Anwender:innendokumentation	CC-BY-3.0 AT	netidee.at/vorsicht-falle
5	Veröffentlichungsfähiger Einseiter	CC-BY-3.0 AT	netidee.at/vorsicht-falle
6	<i>Dokumentation Externkommunikation in Endbericht</i>	CC-BY-3.0 AT	netidee.at/vorsicht-falle
7	Konzeption	CC-BY-3.0 AT	netidee.at/vorsicht-falle
8	Fake-Gewinnspiele	CC-BY-3.0 AT	amazon.gewlInnspiel.at oebb.gewlInnspiel.at
9	Fake-Gewinnspiel mit Zielgruppe Jugendliche	CC-BY-3.0 AT	amaz0n.gewlInnspiel.at
10	Fake-Shop	CC-BY-3.0 AT	blackout-kits.at
10	Angepasstes Wordpress-Backend inkl. begleitende Dokumentation für das Watchlist Internet Team (siehe Entwickler:innendoku)	GNU General Public License (GPLv2)	amazon.gewlInnspiel.at oebb.gewlInnspiel.at blackout-kits.at
11	Tour-Plugin für Typo3 (siehe Entwickler:innendoku)	MIT License	<a href="https://github.com/yaras6/bs5-intro-tour">https://github.com/yaras6/bs5-intro-tour</a> netidee.at/vorsicht-falle
12	Verwertungskonzept	CC-BY-3.0 AT	netidee.at/vorsicht-falle
13	Dokumentation Werbung (statt Presseaussendung)	CC-BY-3.0 AT	netidee.at/vorsicht-falle

## Verwertung der Projektergebnisse in der Praxis

*Angaben zur Verwertung der Projektergebnisse in der Praxis*

- **Fake-Gewinnspiele – weitere Nutzung und weitere Entwicklungen durch die Watchlist Internet:** Die entwickelten Fallen werden von der Watchlist Internet weiter betrieben, im Detail: Die Fake-Gewinnspiele sind online und können weitergeschickt werden, die Informationsartikel zu den jeweiligen echten Betrugsfällen verlinken ebenfalls auf die Fallen und sofern diese Betrugsformen nochmals aufkommen, wird weiterhin darauf verlinkt werden. Der intern abzudeckende, relativ geringe Aufwand zur Entwicklung von Fake-Gewinnspielen ermöglicht, dass jedenfalls im Rahmen der Initiative weiterhin solche Fallen künftig erstellt werden. In Arbeit ist zum Beispiel bereits ein Fake-Gewinnspiel der Post.
- **Nutzung der Fake-Gewinnspiele im Saferinternet.at Kontext:** Zusätzlich wurde im Gespräch mit Saferinternet.at entschieden, dass diese Fallen sich vor allem an die Zielgruppe der Jugendlichen richtet – sowohl bezüglich der üblichen Verbreitung über Social Media als auch durch den Ansatz von „Prank your Friends“. Eine erste Falle, die sich speziell an Jugendliche richtet, wurde bereits entwickelt, dabei handelt es sich um eine abgewandelte Version des Amazon-Gewinnspiels. Zu finden ist das Gewinnspiel mit der Zielgruppe Jugendliche unter: [elektromarktxl.gewinnspiel.at](http://elektromarktxl.gewinnspiel.at). Um die Reichweite des Gewinnspiels zu vergrößern, wurde ein WhatsApp-Share Button hinzugefügt - inklusive der Behauptung, das Weiterleiten wäre notwendig, um überhaupt gewinnen zu können (auch dieser Trick wird von Kriminellen genutzt, um an möglichst viele potentielle Opfer zu kommen). Miteinbezogen werden soll dieses Gewinnspiel sowie die Jugend-Kampagne „Prank your Friends“ rund um den Europäischen Safer Internet Day, der von Saferinternet.at den gesamt Februar 2023 gefeiert wird. Das Thema für 2023 ist „Fake News“ – in diesem Kontext werden Schulklassen dazu angeregt eigene Projekte umzusetzen. In diesem Rahmen wurde entschieden Fake-Fallen hineinzunehmen. In Arbeit ist in diesem Zusammenhang bereits ein Stundenbild von Saferinternet.at (PowerPoint-Foliensatz), das dafür Verwendung finden soll.
- **Fake-Fake-Shop:** Aufgrund des Erfolgs bei der Verbreitung des Fake-Shops ist es geplant im Jahr 2023 diese Falle weiterzuführen. Die Analyse der Daten aus Dezember zeigen, dass je nach investiertem Werbebudget die Reichweite der Präventionsaktivität substantiell erhöht werden kann, jedoch auch mit geringem Aufwand der Weiterbetrieb jedenfalls gesichert werden kann.

## Öffentlichkeitsarbeit/ Vernetzung

- Vorstellung des Projekts und ersten Prototyps einer Falle beim Konsumentenpolitischen Forum am 09. Mai 2022 durch Bernhard Jungwirth
- Austausch mit der AK Niederösterreich und Sebastian Schrittwieser (Universität Wien) zu ihrem netidee-Projekt simulierter Phishing-Fallen
- Vortrag am E-Day der Wirtschaftskammer Wien am 14. September
- Vortrag beim ersten Anti-Scam Meeting der Global Anti Scam Alliance am 21 September 2022 zur Vorstellung der Fallen vor internationalem Publikum. Siehe: <https://www.gasa.org/global-anti-scam-summit-2022-gass>
- Vorstellung des Projekts bei der Beiratssitzung der Watchlist Internet im November 2022, unter Beisitz von Vertreter:innen von u. a. BKA, BMSGPK und der Cybercrime Oberstaatsanwaltschaft Bamberg.
- Austausch mit N26 im Dezember 2022 über mögliche Kooperationen – Vorstellung der entwickelten Fake-Fallen.

## Eigene Projektwebsite

Auf der Watchlist Internet wurde eine Überblicksseite für die entwickelten Fallen eingerichtet:

<https://www.watchlist-internet.at/vorsicht-falle/>

## Geplante Aktivitäten nach netidee-Projektende

Alle Fallen werden einerseits über das laufende Watchlist Internet Budget weiter gedeckt werden, dass der Fake-Shop sowie auch die Fake-Gewinnspiele weiter betrieben werden können.

Andererseits laufen bereits erfolgreiche Gespräche mit interessierten Stakeholdern für mögliche Teil-Finanzierungen der Bewerbung des Shops sowie der Gewinnspiele, sowie die Erstellung weiterer Fallen z. B. Urlaubsbuchungsplattformen – im Jänner/Februar 2023 wird eine Entscheidung zu dieser weiteren Finanzierung erwartet.

## Anregungen für Weiterentwicklungen durch Dritte

Aus unserer Sicht ist vor allem die Anpassung des Backends eine Herausforderung. Wir würden es insofern besonders begrüßen, wenn Dritte ein Interesse daran zeigen würden an der weiteren Vereinfachung des Backends und der Entwicklung von passenden Plugins zu arbeiten, die eine noch raschere Erstellung der Fallen erlauben und so ermöglichen, tagesaktuelle Betrugsmaschen zu Fake-Fallen umzubauen und effektiv davor warnen zu können. Anzudenken sind auch weitere Feedback-Elemente für User:innen oder die Kopplung der Fallen an ein Quiz und andere bestehende Elemente. Wir sehen jedenfalls aufgrund des Erfolgs, den wir bei der Verbreitung der Fallen und der Rezeption der Fallen feststellen konnten, ein großes Potenzial für Weiterentwicklungen und freuen uns über Kontaktaufnahmen bzw. unterstützen gerne Dritte bei ihren Plänen.