netidee

PROJEKTE

Vorsicht, Falle!

Zwischenbericht | Call 16 | Projekt ID 5736

Inhalt

1 Einleitung

Aktuell erreichen wir als Team der Watchlist Internet mit unseren Warnmeldungen zu Betrugsfallen 200.000 Personen im Monat. Diese Präventionsarbeit wollen wir im Projekt „Vorsicht, Falle!“ durch Gamification-Methoden ausbauen. Unser Ziel ist es, aktuelle Fallen für Phishing, Schadsoftware und Fake-Shops realistisch zu simulieren. Wer in diese simulierten Fallen hineinfällt, erleidet keinen Schaden, sondern erhält Erklärungen und Tipps, um in Zukunft besser gegen Internetbetrug gewappnet zu sein. Die Fallen werden in die Warnartikel der Website der Watchlist Internet eingebettet, damit User:innen nicht nur News an Ihr Umfeld senden können, sondern auch simulierte Fallen.

In der ersten Projekthälfte konnten wir bereits Fallen entwickeln und diese umfassend testen. Der Schwerpunkt für die anstehende zweite Projekthälfte liegt zum einen im Aufbau weiterer Fallen sowie zum anderen in Überlegungen zu optimalen Auflösungen für einen hohen Lerneffekt. Die entwickelten Fallen werden in die Website der Watchlist Internet eingebettet und auch direkt bei Newsartikeln, sofern passend, verlinkt.

2 Status der Arbeitspakete

2.1 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.

2.2 Arbeitspaket 2 – Konzeption

In AP2 vorgesehen ist die Konzeption der Betrugsfallen-Simulation mit punktueller Absprache mit Gamification-Expert:innen von OVOS. 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 Abbildung 1).

Der Erstkontakt: Interessierte Leser:innen der Watchlist Internet informieren sich über eine aktuelle Betrugsmasche und entdecken dort den Hinweis, dass sie auch eine simulierte Online-Falle verschicken könnten. Ihre Neugier ist geweckt, denn ihre Bekannten und Familie reagieren z. B. in letzter Zeit gar nicht oder mit Desinteresse auf von ihnen weitergeschickte Watchlist-Newsartikel.

Das Narrativ: Die interessierte User:innen klicken auf die Information zur Falle und landen auf der Projektseite von „Vorsicht Falle“. Auf dieser wird ihnen ein Überblick über alle vorhandenen Fake-Fallen gegeben, inklusive Textvorschlägen, die sie begleitend mitschicken können.

Die Falle: Die simulierten Falle orientiert sich an einer aktuellen, realen Betrugsmasche. Sie ist authentisch aufgebaut. Das überzeugt die User:innen und sie teilen eine Betrugsfalle ihrer Wahl.

Der Schockmoment: Die adressierte Person klickt auf den Link und sieht eine entlang einer aktuellen Falle überzeugend gestaltete Version einer Betrugsmasche. In dem Moment, in dem sonst der Schaden entstanden wäre – z. B. bei der Eingabe von Kreditkartendaten – wird der:die User:in für einen Moment in Schrecken versetzt. Dieser Schockmoment gilt als essenziell, damit die Erfahrung im Gedächtnis bleibt.

Die Auflösung: Nach wenigen Sekunden wird der Schockmoment von einer Auflösung abgelöst – in dieser erfährt der:die Nutzer:in, wie sie bei dieser aktuellen Falle die Hinweise auf Betrug hätte erkennen können. Am Ende hat der:die User:in die Möglichkeit die Falle mit weiteren Bekannten zu teilen.

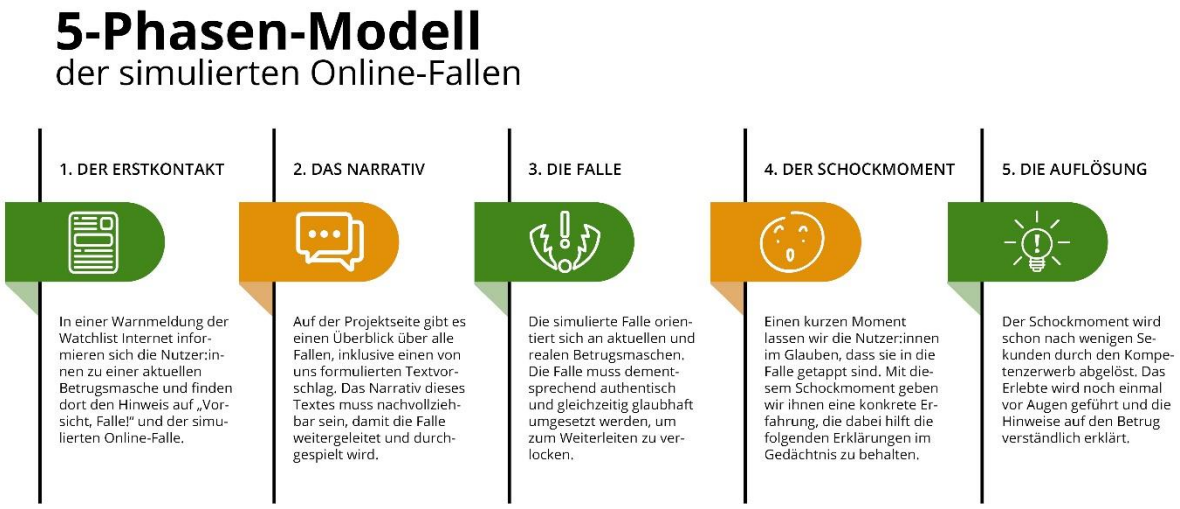


Abbildung 1: Das Konzept – 5-Phasen-Modell der simulierten Onlinefallen

Konzeption der Falle „Amazon-Gewinnspiel“

Ein aktuell kursierendes Amazon-Gewinnspiel ist die erste Falle, die nach diesem Prinzip konzipiert wurde. Auf Basis erster Konzepte wurden UX Wireframes der Falle „Amazon-Gewinnspiel“ mit dem Tool UXpin erstellt (siehe die folgenden Schreenshots):

Abbildung 2: UX-Design der Amazon-Gewinnspiel Falle, Startseite

Abbildung 3: UX-Design der Amazon-Gewinnspiel Falle, Projektseite

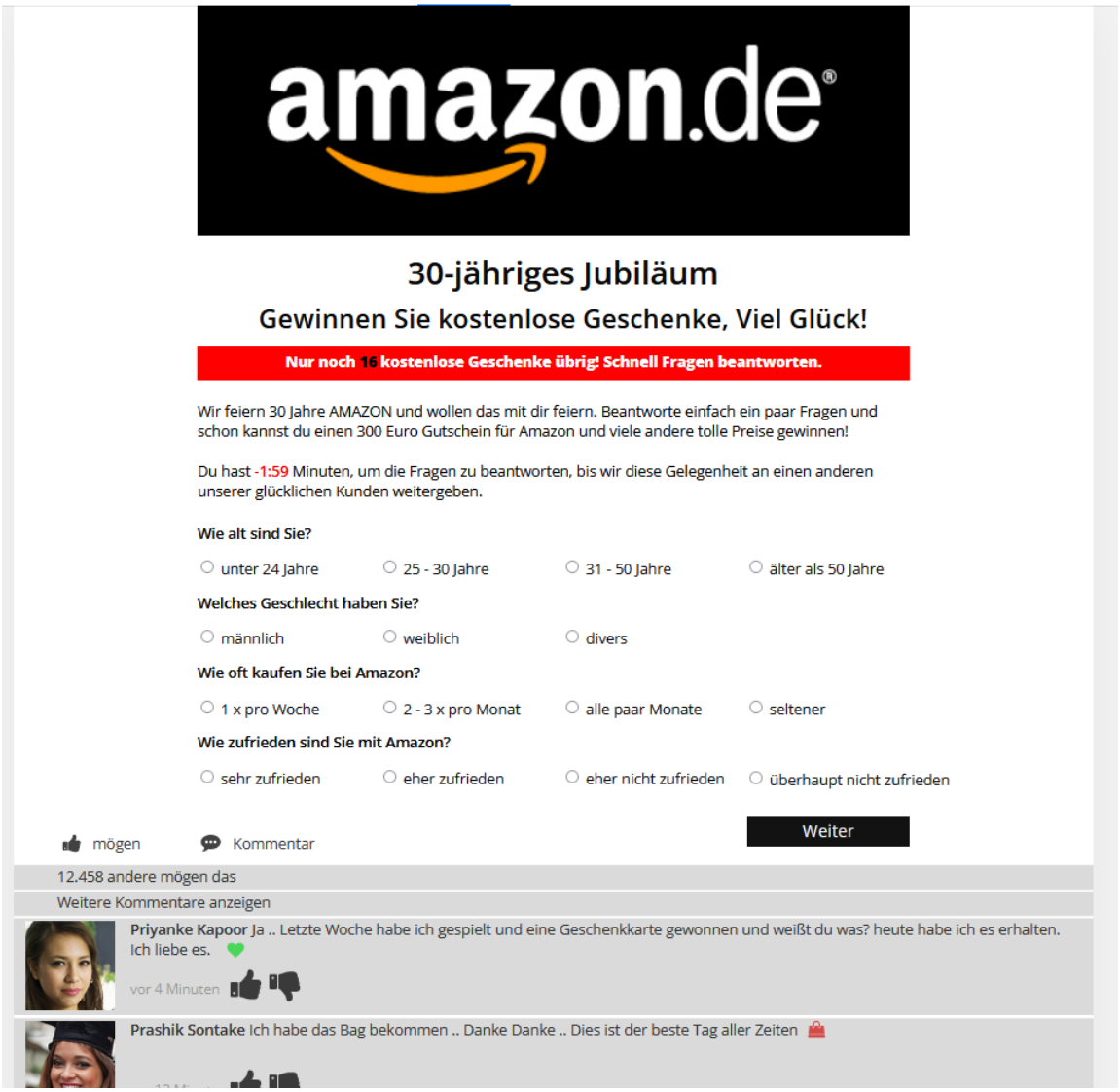


Abbildung 4: UX-Design Startseite der simulierten Falle

Abbildung 5: UX-Design der Auflösung

Die weiteren geplanten Schritte in diesem Arbeitspaket umfassen:

- Konzeption weiterer Simulationsfallen entlang des 5-Phasen-Modells
- Konzeption der Auflösungen fortsetzen
- Beratung durch Gamification-Expert:innen von OVOS

2.3 Arbeitspaket 3 – Betrugsfallen

Im Arbeitspaket 3 werden Betrugsfallen entwickelt. Der Fokus liegt dabei auf der Aufklärung und der Wissensvermittlung, insofern kommt den Auflösungen eine große Bedeutung zu.

Aufbauend auf der konzipierten Falle zum Gewinnspiel von Amazon wurde die folgende Falle entwickelt und ausgerollt (siehe: https://amazon.gewlnnspiel.at/)

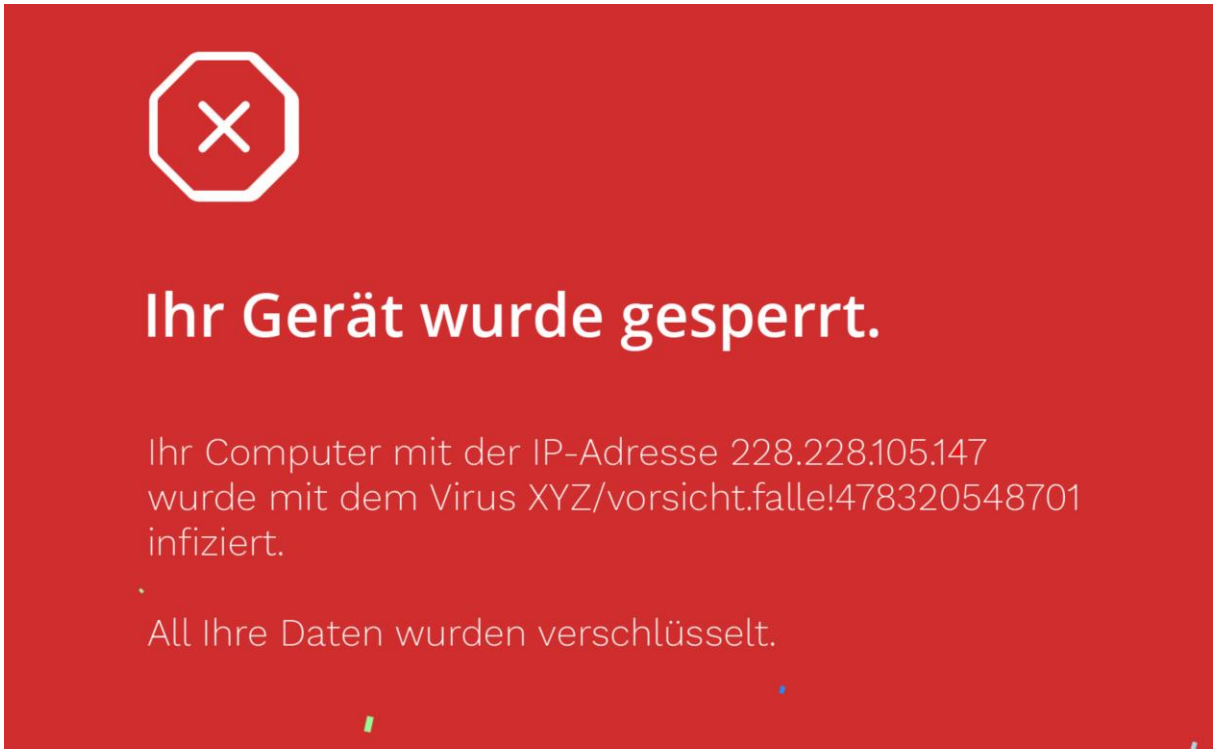


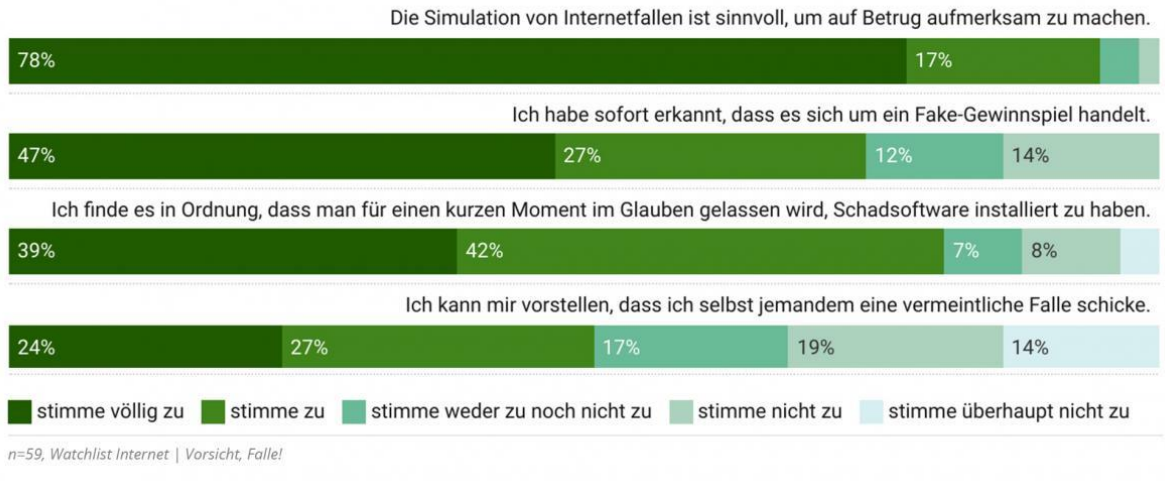
Abbildung 6: Screenshot des "Schockmoments" der Falle Amazon-Gewinnspiel.

Wer die vermeintliche Falle bis zum Ende durchspielt, wird auf der letzten Seite gebeten eine kurze Umfrage auszufüllen. Das Ergebnis des ersten Testdurchlaufs: Im Testzeitraum vom 04. Mai bis 28. Mai erhielten wir 59 ausgefüllte Fragebögen. Dabei ging es um eine Bewertung (stimme völlig zu bis stimme überhaupt nicht zu) der folgenden vier Aussagen:

- Die Simulation von Internetfallen ist sinnvoll, um auf Betrug aufmerksam zu machen.
- Ich habe sofort erkannt, dass es sich um ein Fake-Gewinnspiel handelt.
- Ich finde es in Ordnung, dass man für einen kurzen Moment im Glauben gelassen wird, Schadsoftware installiert zu haben.
- Ich kann mir vorstellen, dass ich selbst jemandem eine vermeintliche Falle schicke.

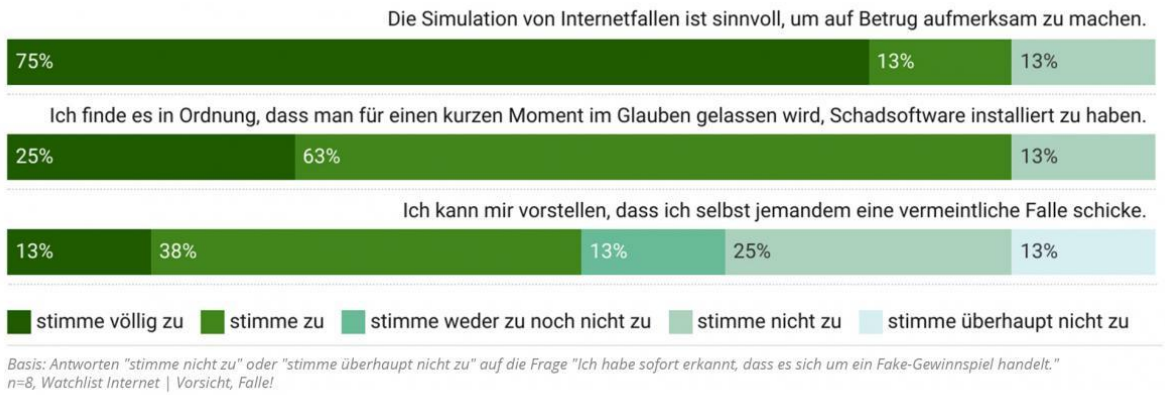
Zusätzlich stellten wir den Umfrageteilnehmer:innen ein offenes Textfeld mit der Frage „Wollen Sie uns noch etwas anderes mitteilen?“ zur Verfügung.

Das Ergebnis: 78% der Befragten stimmen völlig zu und weitere 17% stimmen zu, dass die Simulation von Internetfallen sinnvoll ist, um auf Betrug aufmerksam zu machen. Insgesamt 81% finden es in Ordnung, dass wir die Teilnehmer:innen für einen kurzen Moment im Glauben lassen, Schadsoftware installiert zu haben. Etwas Zurückhaltung gibt es lediglich bei der Frage, ob die Befragten sich vorstellen können, selbst so eine Falle weiterzuleiten. Hier stimmten „nur“ 51% (völlig) zu.



Wieso manche Teilnehmer:innen sich nicht vorstellen können, die Falle selbst weiterzuleiten, konnten wir zu einem Teil aus den Kommentaren im Textfeld eruieren. So sorgten sich einige Befragte, dass sie ihr Umfeld damit verärgern würden. Hier werden wir entsprechend nachschärfen und auch für Skeptiker:innen eine Möglichkeit anbieten, um die Falle ohne Bedenken weiterleiten zu können.

Wie die Grafik zeigt, sind nur wenige Personen in die Falle getappt – die meisten haben erkannt, dass es sich um Fake handelt - nur 14% geben an, das Fake-Gewinnspiel nicht erkannt zu haben. Eine weitere Auswertung der Umfrageergebnisse zeigt, dass auch all jene, die die Falle nicht erkannt haben, unser Projekt positiv aufnehmen. Interessant ist vor allem, dass 88% (und damit noch mehr als beim Gesamtergebnis) das Vorgaukeln der installierten Schadsoftware, in Ordnung finden.



2.4 Arbeitspaket 4 – Einbettung in die Watchlist Internet

Ziel des Arbeitspakets 4 ist die, dass die Betrugsfallen in die Watchlist Internet eingebettet werden und diese von den User:innen auch umgestaltet werden können.

Es wurde bereits eine Überblicksseite eingerichtet, die Texte wurden durch Feedback der Presseagentur Skills adaptiert. Es sind Weiterleitungen auf die aktuell schon ausgerollten Fallen eingerichtet (siehe: https://www.watchlist-internet.at/vorsicht-falle/).

Die aktuelle Falle wurde ebenfalls schon in einem Newsartikel verlinkt (siehe: https://www.watchlist-internet.at/news/kettenbrief-alarm-angebliches-amazon-gewinnspiel-macht-auf-whatsapp-die-runde/).

Die Website der Watchlist Internet wird derzeit grundlegend erneuert – die neue Version der Seite wird für Herbst 2022 erwartet. Im Hintergrund wird insofern an der Einbettung der Vorsicht-Falle-Simulationen in diese neue Umgebung gearbeitet, die u. a. zusätzliche Optionen für die ansprechendere Gestaltung mit sich bringen werden.

2.5 Arbeitspaket 5 – Dissemination

In AP5 vorgesehen sind alle Disseminationsaktivitäten, die als Zielgruppe zum einen Privatpersonen, zum anderen auch Unternehmen haben. Dafür ist neben den in Kapitel 5 beschriebenen Aktivitäten, jedenfalls noch eine Presseaussendung und die Erstellung eines Verwertungskonzepts geplant.

Bislang erschienen sind 6 Blogeinträge auf www.netidee.at/vorsicht-falle
Die Watchlist Internet (Website, Newsletter und Social Media Kanäle) wurden bereits genutzt, um die Falle zu bewerben und User:innen für den ersten Testzeitraum zu gewinnen.
https://www.watchlist-internet.at/news/vorsicht-falle-wir-brauchen-ihre-hilfe-fuer-ein-neues-projekt/

Siehe Kapitel 5 für weitere Disseminationsaktivitäten im Sinne der Öffentlichkeitsarbeit und Vernetzung

3 Umsetzung Förderauflagen

Das Projekt hat keine Förderauflagen zu beachten.

4 Zusammenfassung Planaktualisierung

Es sind keine Aktualisierungen im Plan vorgesehen.

5 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.

Geplante weitere Öffentlichkeitsarbeit:

- Zusage für einen Vortrag beim ersten Anti-Scam Meeting der **Global Anti Scam Alliance** am 21 September 2022, bei dem das Projekt „Vorsicht, Falle“ vorgestellt werden wird.

6 Eigene Projektwebsite

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