

Projektziel

Die unabhängige Informationsplattform Watchlist Internet klärt seit 2013 über Internet-Betrug und betrugsähnliche Fallen auf. Entstanden als netidee-Projekt ist die Watchlist Internet mittlerweile zentrale Anlaufstelle für all jene, die sich vor Gefahren im Internet schützen wollen. Aktuell erreicht das Watchlist Internet Team monatlich bis zu 300.000 Personen.

Mit dem Projekt „Vorsicht, Falle“ wird an diesen Erfolg angeknüpft und die Präventionsarbeit durch Gamification-Methoden ausgebaut, indem realistische Betrugsfallen nachgebaut werden. Konkret geht es 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 Fallen als besonders einfach, für andere ist mit einem höheren Aufwand zu rechnen. Als die größte Herausforderung stellte sich die Verbreitung der Fallen heraus. Es wurde insofern gerade in diese Arbeitsschritte viel Zeit investiert, denn die Reichweite ist ein wichtiger Indikator des Erfolgs von Präventionsmaßnahmen. Innerhalb des Projektes entstanden zwei unterschiedliche Konzepte für Fallen: (1) Fake-Gewinnspiele und (2) ein Fake-Shop.

Fake-Gewinnspiele:

Alle Fallen wurden mit dem CMS Wordpress erstellt. Dennoch unterscheidet sich die Herangehensweise an die jeweiligen Fallen grundlegend. Um mit relativ geringem Aufwand neue Fake-Gewinnspiele erstellen zu können, hat sich die Umstellung des einfachen Wordpress-Backends auf Wordpress Multisite (Wordpress Netzwerk) bewährt. Eine genaue Dokumentation für die Einrichtung eines solchen Netzwerks stellt Wordpress zu Verfügung: <https://wordpress.org/support/article/create-a-network/>

Folgende Vorteile ergaben sich für uns durch die Umstellung auf Wordpress Multisite:

- Alle Seiten mit einem Zugang erreichbar
- Copy-Paste der Inhalte möglich (zentral, da Fake-Gewinnspiele – auch jene der Betrüger:innen – meist ähnlich aufgebaut sind)
- Netzwerkweite Aktivierung der verwendeten Plugins möglich

Folgende Plugins, Tools und Code-Snippets kommen zum Einsatz:

- **Formularelemente:** Fake-Gewinnspiele arbeiten oftmals mit Umfragen, die vertrauenswürdig wirken sollen. Die Umfragen sind dabei recht kurz und einfach gehalten, die Formularelemente des verwendeten Blockeditors (bei uns Kadence Blocks) sind daher ausreichend. Das ÖBB-Gewinnspiel nutzt zudem Formulare zur Abfrage persönlicher Daten. Dieses Formular wurde von

uns selbst geschrieben, da während der Dateneingabe eine Weiterleitung zum “Schockmoment” (Modal) stattfinden soll. Eine vereinfachte Darstellung des Code-Snippets:

```

<div class="modal-overlay">
  //Verlinkung zum Bild, das als Modal verwendet wird
  
</div>

//Formular
<div id="form-wrapper">
  <div id="formular-wrapper">
    <form id="formular">
      <label id="vorname" for="vorname">Vorname</label><input id="vornamein"
name="vorname" type="text">
      <br><br>
      <label id="nachname" for="vorname">Nachname</label>      <input
name="vorname" type="text">
      <input id="send-button" type="button" value="Senden">
    </form></div>
</div>

//Modal vorerst nicht anzeigen
<style>
.modal-overlay {
  display: none;
  position: fixed;
  z-index: 99;
  width: 100vw;
  max-width: 100vw;
  left: 0;
  right: 0;
  top: 0;
  bottom: 0;
}
</style>

//Modal wird während Dateneingabe im Feld Vorname angezeigt
<script>
var input = document.querySelector("input[name='vornamein']");

input.addEventListener("input", updateValue);

function updateValue(e) {

  if (e.target.value.length >= 3) {

    setTimeout(function () {
document.getElementsByClassName("modal-overlay")[0].style.display =
  "block";
    }, 2000);

    //Weiterleitung zu watchlist-internet.at nach 10 Sekunden
    setTimeout(function () {
      window.open("https://www.watchlist-internet.at", "_self");
    }, 10000);
  }
}
</script>

```

- **Interaktive Elemente:** Neben Umfragen werden auch kleine Minispiel von den Betrüger:innen eingesetzt (bspw. Glücksrad, Memory, Quiz). Diesbezüglich empfehlen wir die Verwendung externer Tools. Insbesondere interacty.me und genial.ly bieten hier einfache und DSGVO-konforme Möglichkeiten. Die erstellten Mini-Spiele können anschließend in den Blockeditor per html-Snippet eingebettet werden.
- **Schockmoment mit Modal:** Bei der Konzeption der Fake-Fallen wurde ein “Schockmoment” als wichtiger Bestandteil der jeweiligen Fallen definiert, um einen möglichst hohen Lerneffekt sicherstellen zu können. Bei den Fake-Gewinnspielen wird dieser Schockmoment mit einem Fullscreen-Modal ausgelöst. Das Modal besteht aus einem von uns erstelltem Bild mit Text, der vorgaukelt Opfer von Schadsoftware oder einer Phishing-Falle geworden zu sein. Eingebledet wird das Modal mit Hilfe des Plugins Popup-Builder. Wichtig bei der Auswahl des Plugins war die Möglichkeit ein kurzes Javascript-Snippet einfügen zu können. Denn das Modal soll nur kurze Zeit für die Nutzer:innen sichtbar sein und nach wenigen Sekunden automatisch zur Auflösungsseite weiterleiten. Dafür haben wir folgendes Javascript-Snippet eingesetzt:

```
setTimeout(function(){open("https://www.watchlist-internet.at","_self"),10000};
```

- **Auflösungsseite mit Tour:** Nach dem Schockmoment gilt es das Vertrauen der Nutzer:innen zurückzuholen. Daher haben wir beschlossen, die Auflösungsseite auf www.watchlist-internet.at zu platzieren und nicht auf der Seite des Gewinnspiels selbst. Hierfür wurde eine eigene Tour entwickelt, mit der sich die Nutzer:innen Schritt für Schritt durch die jeweilige Falle klicken können, um die Hinweise auf Betrug zu erforschen. Die Watchlist Internet nutzt das CMS Typo3, ein eigens entwickeltes Tour-Plugin. Dieses ist hier unter einer MIT-Lizenz zu finden: <https://github.com/yaras6/bs5-intro-tour>

Fake-Shop: Auch für den Fake-Shop haben wir uns gemeinsam mit der Agentur limesoda für Wordpress als CMS entschieden. Die Entwicklung des Fake-Fake-Shops gestaltete sich jedoch um einiges aufwändiger als die Gewinnspielseiten. Besonders hervorzuheben ist dabei die Auswahl der Produkte und damit einhergehend die Bebilderung. Zentrales Element des Fake-Shops ist das Plugin WooCommerce zur Erstellung eines Shopsystems, das uns folgende Möglichkeiten zur Verfügung stellt:

- Anlegen der Produkte
- Beschreibungstext
- Produktbild

- Preis inkl. Angebotspreis (Angebote und zu günstige Preisen sind zentrales Element von Fake-Shops)
- Varianten der Produkte (bspw. unterschiedliche Farben oder Größe)
- Bewertungen (Fake-Shops weisen oftmals eine Vielzahl gefälschter Bewertungen auf, die allesamt positiv sind)
- Warenkorb
- Kassa

Die Auflösung wurde mit Hilfe des Plugins Tours Builder erstellt. Im Gegensatz zu den Fake-Gewinnspielen haben wir uns beim Fake-Fake-Shop dafür entschieden, die Falle in Form einer Tour durch den Shop selbst aufzulösen. Grund dafür ist, dass der Schockmoment weniger stark ist und dass eine erste Analyse der Besucher:innen-Zahl gezeigt hat, dass viele Nutzer:innen bereits vor der Auflösung abspringen. Das Plugin Tour Builder ermöglicht, dass sich die Tour durch das Anklicken des ersten Formularfeldes auf der Kassa-Seite automatisiert öffnet. Mit Hilfe der Tour werden die Nutzer:innen über die Falle aufgeklärt und anschließend Schritt für Schritt durch den Shop geführt, um die Hinweise auf Betrug zu erkunden.

Verbreitung der Fallen: Wie im Endbericht des Projektes ausführlich dargelegt, verwenden wir unterschiedliche Verbreitungswege der Fallen. Dazu zählt die Schaltung von Werbung durch Google Ads im Falle des Fake-Shops, sowie die Einbettung der Fallen in die Watchlist Internet – einerseits innerhalb von Warnmeldungen zu ähnlichen Betrugsfällen, andererseits auf der Projektseite von Vorsicht, Falle. Mit Hilfe einer niederschweligen Schritt-für-Schritt-Anleitung animieren wir die Leser:innen der Watchlist Internet mitzumachen, indem Sie die Fallen verbreiten und so Freund:innen oder Familie für Betrug sensibilisieren. Die Anleitung findet sich auf www.watchlist-internet.at/vorsicht-falle.

Messung des Präventionseffekts: Um den tatsächlichen Präventionseffekt der jeweiligen Falle zu messen, empfehlen wir die Verwendung des Wordpress-Plugins matomo. Innerhalb des Plugins können Zielseiten definiert werden, die eingehend analysiert werden können. Als Zielseite haben wir die Tour-/Auflösungsseiten definiert. Wird diese aufgerufen, ist ein Lern- und Präventionseffekt anzunehmen. Befindet sich die Auflösung auf einer externen Seite, müsste auch diese mit matomo (oder einem anderen DSGVO-konformen Tracking-Tool) verknüpft sein.

Anregungen für Weiterentwicklungen durch Dritte

Weiterentwicklungsmöglichkeiten durch Dritte oder im Rahmen von Kooperationen mit Dritten sind sowohl auf technischer als auch auf konzeptioneller Ebene denkbar:

- **Weitere Anpassung des Backends:** Um den Arbeitsaufwand für die Erstellung der Fallen möglichst gering zu halten, macht eine weitere Anpassung und Vereinfachung des derzeitigen Backends Sinn. Je mehr sich das Backend an die Bedürfnisse der Fake-Fallen orientiert, desto schneller können die Fallen entwickelt werden. So kann auch die Anzahl der Fallen erhöht werden. Die Anpassung eines Backends ist sowohl innerhalb von Wordpress als auch durch andere CMS denkbar.
- **Unabhängigkeit von externen Anbieter:innen:** Die Suche nach Plugins gestaltete sich schwierig. Einerseits kamen für uns nur DSGVO-konforme Anbieter:innen in Frage, andererseits sind die Gestaltungsbedürfnisse recht untypisch. Die Programmierung eigener Tools würde uns mehr Spielraum in der Gestaltung geben und uns unabhängig von externen Anbieter:innen machen. So würde die Frage des Datenschutzes bei der Suche nach Plugins wegfallen, aber auch Plugin-Updates nichts an der Funktionalität unserer Fallen ändern.
- **Konzeption weiterer Fallen:** Internetbetrug nimmt vielfältige Formen an. Dementsprechend vielfältig sollten auch die von uns zur Verfügung gestellten Fallen sein. Wir werden auch nach der Laufzeit des Projektes weitere Fallen erstellen und konzipieren. Konzeptionelle Weiterentwicklungen können aber auch von Dritten oder in Zuge von Kooperationen vorangetrieben werden. Besonders spannend wären bspw. die Entwicklung klassischer Phishing-Fallen (im Namen bekannter Unternehmen) oder die Programmierung einer Fake-Schadsoftware zur Steigerung des Schockmoments (anstatt des derzeit verwendeten Modals).
- **Alternative Verbreitungswege:** Derzeit verwenden wir Werbung (Fake-Shop), die Watchlist Internet sowie virale Weiterleitungsketten (Gewinnspiele) für die Verbreitung der Fallen. Zudem können die Fallen in Schulungen oder in anderen pädagogischen Einsatzgebieten zur Anwendung kommen. Für einen möglichst hohen Präventions- und Lerneffekt ist die Konzeptionierung weiterer Verbreitungswege notwendig.

Wir freuen uns über Kooperationsanfragen und unterstützen gerne bei der Weiterentwicklung unserer Fake-Fallen – bitte melden Sie sich bei uns!

Louise Beltzung
beltzung@oiat.at

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