SmishingCheck

Anwender-Dokumentation | Call 19 | Projekt ID 7232

Inhalt

1 Was ist SmishingCheck? 3

2 Für wen ist SmishingCheck? 3

3 Wie funktioniert SmishingCheck? 4

1 Was ist SmishingCheck?

SmishingCheck ist eine App für iOS und Android (veröffentlicht im November 2025) für österreichische Nutzer in der Sprache Deutsch, die es ermöglicht …

- … sich über Smishing und deren Ausprägungen zu informieren.
- … SMS-Nachrichten auf bekannte Betrugsfälle zu prüfen.
- … verdächtige Nachrichten an die österreichische Meldestelle (Watchlist Internet) direkt über die App zu melden.

Die App ist über die beiden Stores (iOS App-Store; Google Play-Store) kostenlos downloadbar, hier sind die Links:

- iOS: https://apps.apple.com/at/app/smishingcheck/id6741202684
- Android: https://play.google.com/store/apps/details?id=com.coastlab7.smishingCheck

Nähere Informationen zum Projekt findet man auf der Projektseite von netidee sowie der Webseite:

- netidee: https://www.netidee.at/smishingcheck
- Website: https://smishingcheck.app/

2 Für wen ist SmishingCheck?

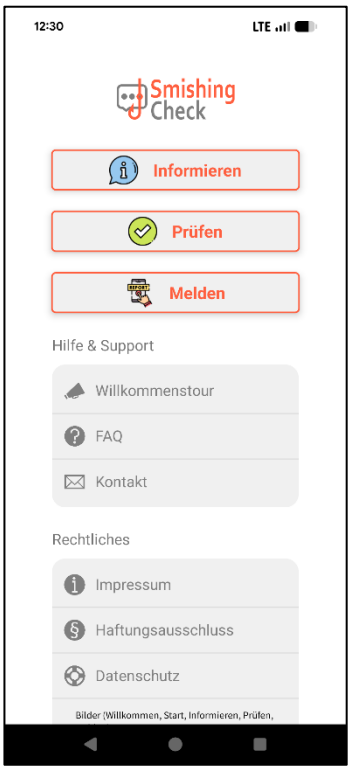
Die App SmishingCheck ist für all jene Smartphone-Nutzer (Android oder iOS) gedacht, die direkt am Handy Informationen zu Smishing erhalten wollen, SMS-Inhalte auf bekannte Smishing-Betrugsfälle prüfen wollen und Betrugsfälle direkt am Handy melden wollen. Die App kann in Österreich heruntergeladen werden, ist kostenlos und werbefrei nutzbar und ist in der Sprache Deutsch verfügbar.

Außerdem ist SmishingCheck durch die Melde-Funktion vorteilhaft für Watchlist Internet, da durch den Anreiz, Meldungen auf einfache Art und Weise über die App absenden zu können, die Dunkelziffer von bekannten Betrugsfällen reduziert wird. Es können aktuelle Trends und neue Wellen frühzeitig erkannt und dahingehend Warnungen ausgesprochen werden.

Und zu guter Letzt ist SmishingCheck auch für all jene gedacht, die das Projektergebnis weiterverwenden und mit weiteren Ideen ergänzen möchten.

3 Wie funktioniert SmishingCheck?

Nachfolgend werden die Funktionen von SmishingCheck erläutert, in dem auf die einzelnen App-Screens eingegangen wird:



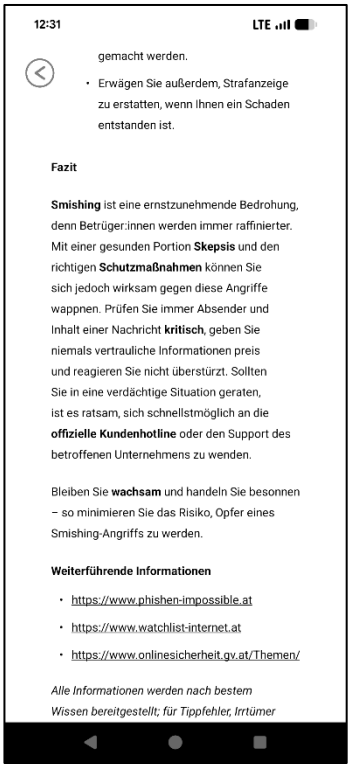
Der **Hauptschirm** beinhaltet an prominenter Stelle Schaltflächen für die drei Hauptfunktionen der App:

- Informieren,
- Prüfen
- und Melden.

Ein Klick auf einen der Schaltflächen führt zur jeweilen Funktion, die in den weiterführenden Screens erläutert wird.

Darunter befindet sich ein kleines Menü unterteilt in die Bereiche

- „Hilfe & Support“: Hier kann die Willkommenstour erneut gestartet werden, sowie sind hier die „Frequently Asked Questions (FAQ)“ und die Kontaktdaten verlinkt.
- „Rechtliches“: Mit Links zum Impressum, zum Haftungsausschluss sowie zur Datenschutzbestimmung.

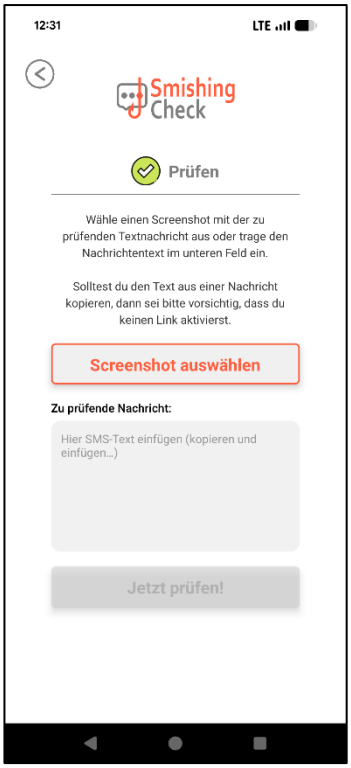


Der **Informieren**-Bereich klärt generell über Smishing auf und schildert, welche Formen von SMS-Phishing existieren. Außerdem wird darauf eingegangen, was übliche Strategien von Täter sind, auf welche Warnzeichen man achten sollte und wie man sich am besten davor schützen kann.

Es werden Smishing-Beispiele angeführt und weiterführende Informationen als Links dargestellt.

Der Informieren-Bereich ist technisch so umgesetzt, dass sehr rasch und ohne nötiges Update der App, die dargestellten Informationen erweitert oder geändert werden können. Dies ermöglicht ein rasches Reagieren auf aktuelle Trends in diesem Bereich.

Jede Unterseite der App enthält links oben eine Zurück-Schaltfläche („<“), über die man zum vorherigen Screen gelangt.



Wenn wir in den **Prüfen**-Bereich der SmishingCheck-App blicken, dann öffnet sich zuerst dieser Screen. Eine Einleitung hilf dem Nutzer, sich zurecht zu finden.

Verdächtige Texte (aus SMS- oder WhatsApp-Nachrichten) können hier als Screenshot ausgewählt werden. Das Erstellen des Screenshots muss zuvor mit den Standardfunktionen des Smartphones getätigt werden.

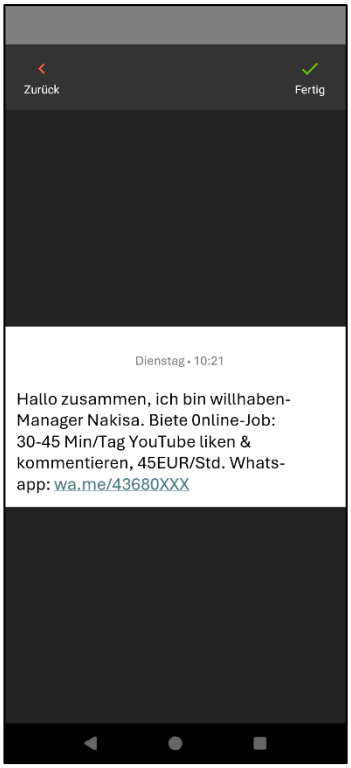
Die weitere Abfolge schildern die nachfolgenden Screens.

Sobald man ein Bild (den **Screenshot**) aus der Smartphone-internen Galerie ausgewählt hat, erscheint automatisch die Möglichkeit des Ausschneidens.

Hier kann (und sollte) dieser Teil des Screenshots ausgewählt werden, der den wesentlichen Text, welcher überprüft werden soll, beinhaltet.

Was kann und sollte so gemacht werden:

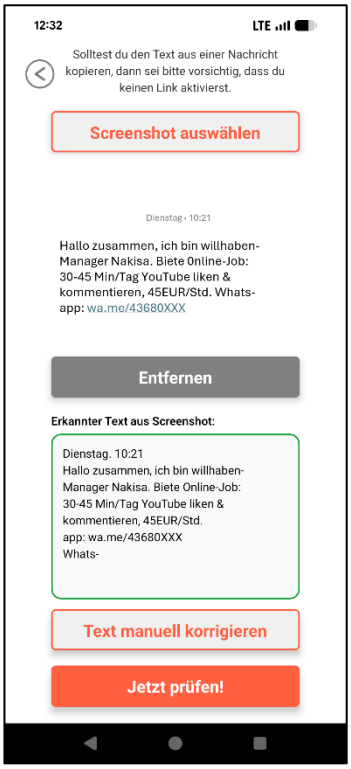
- Ein Verschieben des gesamten Rechtecks dient zum korrekten Positionieren am gewünschten Textbereich.
- Mit Hilfe der weißen Ecken des Rechtecks kann der Bereich vergrößert bzw. verkleinert werden.
- Mittels „Fertig“ (rechts oben) wird der Vorgang bestätigt.



Das ausgeschnittene **Ergebnis** des Nachrichten-Screenshots wird darauffolgend automatisch präsentiert, wie am Beispiel hier links dargestellt.

Wenn man damit zufrieden ist, ist mittels „Fertig“ (rechts oben) erneut zu bestätigen.

Möchte man den Vorgang des Ausschneidens wiederholen, so kann dies durch Betätigen von „Zurück“ (links oben) erneut durchgeführt werden.



Nach dem positiven Bestätigen des ausgeschnittenen Nachrichten-Bereichs wird automatisch der **Text aus dem Bild** ermittelt und als editierbaren Text extrahiert.

Man sieht dies hier links in der grün umrandeten Box.

Dieser Screen ermöglicht folgende Funktionen:

- Screenshot auswählen: Ein neuerliches Wählen eines Screenshots inkl. der nachfolgenden, bereits erläuterten Schritte, kann getätigt werden.
- Entfernen: Der aktuell gewählte Screenshot kann entfernt werden.
- Text manuell korrigieren: Falls die Texterkennung nicht korrekt gearbeitet hat, ist hier ein manuelles Nachkorrigieren möglich. Durch Betätigen dieser Schaltfläche wird das Bearbeiten des grün umrandeten Textfeldes ermöglicht.
- Jetzt prüfen: Der ermittelte Text wird auf Smishing-Kennzeichen überprüft (mehr dazu im nachfolgenden Screen).

Die **Prüfung** des zuvor gewählten Textes erfolgt nun – was etwas Zeit in Anspruch nimmt (wenige Sekunden, in der Regel).

Was hier passiert:

Der Textinhalt wird mit folgenden Daten verglichen (mittels Ähnlichkeitsanalyse anhand einer Gewichtungsformel):

- Watchlist Internet (https://www.watchlist-internet.at) → Unseriöse Webseiten → Phishing-Alarm: Listungen mit dem Kennzeichen „SMS“.

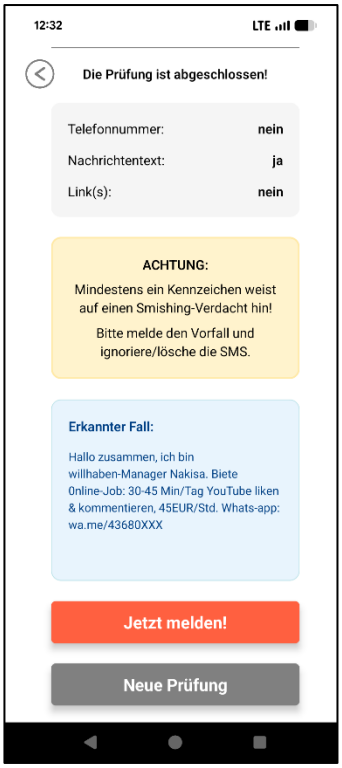
Außerdem werden Links, die im Text vorkommen, gegen folgende Listungen geprüft:

- Watchlist Internet → Unseriöse Webseiten:
  - Betrügerische Online-Shops
  - Problematische Online-Shops
  - Abo-Fallen
  - Immobilien-Agenturen
  - Urlaubsbuchung
  - Handwerksdienste
  - Speditionen
  - Jobangebote
  - Finanzbetrug
  - Automatisierte Warnungen

Außerdem werden Telefonnummern, die im Text vorkommen, gegen alle Vorkommnisse geprüft, die auf folgender Spam-Auflistung enthalten sind:

- https://spamcalls.net/de/

Wichtig: All diese Daten werden nächtlich abgerufen und zwischengespeichert, um diese in der SmishingCheck-App nutzen zu können. Daher kann es vorkommen, dass ganz aktuelle Listungen erst am nächsten Tag anschlagen.



Nachdem die **Prüfung abgeschlossen** ist, erscheint diese Hinweisseite.

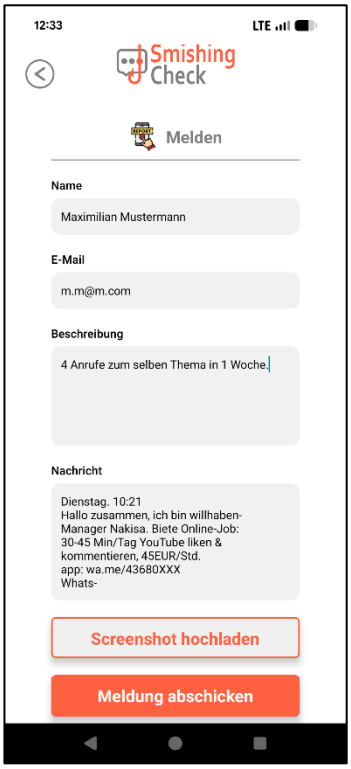
Unterteilt in die Bereiche „Telefonnummer“, „Nachrichtentext“ und „Link(s)“ werden Treffer mittels „ja/nein“ gekennzeichnet.

Wenn mindestens ein Bereich anschlägt, dann erfolgt eine Warnmeldung.

Sollte der Nachrichtentext als Verdachtsfall erkannt werden, so wird in einem blauen Bereich auch der erkannte Fall dargestellt.

Wichtig: Auch wenn kein Verdachtsfall anschlägt, heißt das nicht, dass es sich nicht trotzdem um Phishing handeln kann! Es ist daher in jedem Fall ratsam, achtsam zu sein!

Man hat nun die Möglichkeit, den Fall zu melden (mittels Schaltfläche „Jetzt melden!“), oder eine neue Prüfung durchzuführen (mittels Schaltfläche „Neue Prüfung“).



Werfen wir nun einen Blick auf die Funktion „**Melden**“.

Hier besteht die Möglichkeit, einen Betrugs- oder Verdachtsfalls an die Meldestelle von Watchlist Internet zu melden.

Wenn man direkt aus dem vorherigen Fenster „Prüfung abgeschlossen“ zum Melden gelangt, dann wird der Nachrichtentext automatisch übernommen.

Es ist nun noch notwendig, den Namen, die eigene E-Mailadresse (z.B. für Rückfragen seitens Watchlist Internet) und eine Beschreibung (bspw. ergänzende Informationen zur Nachricht) einzutragen.

Neben dem Nachrichtentext kann auch ein Screenshot übermittelt werden (mittels „Screenshot hochladen“). Hier passiert wieder eine automatische Extraktion des Textes aus dem gewählten Screenshot-Bereich (gleiches Vorgehen wie zuvor bereits geschildert).

Mittels der Schaltfläche „Meldung abschicken“ wird eine E-Mail mit den eingetragenen Daten und Informationen an die Meldestelle von Watchlist Internet geschickt.

Eine Bestätigungsmeldung signalisiert den erfolgreichen Versand.

Beim allerersten App-Start (sowie beim Betätigen des Menüeintrages „Willkommenstour“) erscheint eine kleine **Welcome-Tour** mit drei Screens.

Beim ersten der drei Screens müssen außerdem der Haftungsausschluss sowie die Datenschutzbestimmungen bestätigt werden, in dem die beiden Checkboxen aktiviert werden. (Die jeweiligen rechtlichen Inhalte sind dort selbstverständlich verlinkt.)

Die Willkommenstour erläutert bild- und textlich die wesentlichen Funktionen der App.

Mittels „Weiter“ und „<“ (Zurück) sowie durch ein Swipen nach links bzw. rechts kann durch die Willkommenstour durchnavigiert werden.

Der Menüeintrag „FAQ“ (**Frequently Asked Questions**) ist mit der folgenden Unterseite der SmishingCheck-Webseite verlinkt:

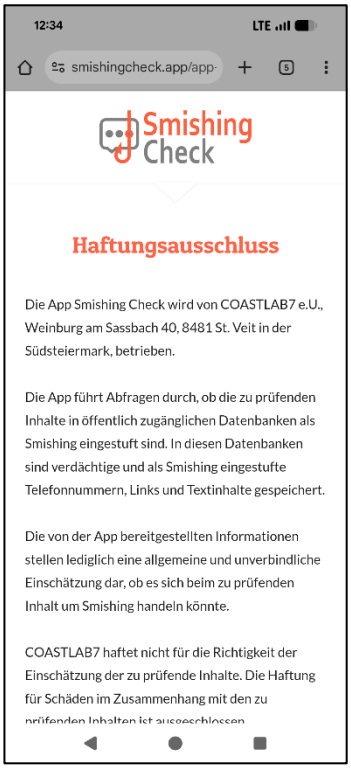
https://smishingcheck.app/faq

Hier werden wesentliche Informationen zu Smishing und natürlich zur SmishingCheck-App durch Fragen und Antworten präsentiert.

Da sich der Bereich auf der extern liegenden Webseite befindet, wirken sich Aktualisierungen direkt aus.

Der Menüeintrag „**Kontakt**“ ist mit der folgenden Unterseite der SmishingCheck-Webseite verlinkt:

https://smishingcheck.app/impressum-und-kontakt



Der Menüeintrag „**Haftungsausschluss**“ (sowie auch der Link auf der ersten Seite des Welcome-Screens) ist mit der folgenden Unterseite der SmishingCheck-Webseite verlinkt:

https://smishingcheck.app/app-haftungsausschluss

Der Menüeintrag „**Datenschutz**“ (sowie auch der Link auf der ersten Seite des Welcome-Screens) ist mit der folgenden Unterseite der SmishingCheck-Webseite verlinkt:

https://smishingcheck.app/app-datenschutzerklaerung