Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Face/Off – Täuschung von Verbraucherinnen und Verbrauchern bei Internetdiensten

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel: +49 22899 9582-0
E-Mail: certbund@bsi.bund.de
Internet: https://www.bsi.bund.de

1 Inhalt

2 Einleitung

Unter Internetdiensten versteht man Anwendungen, die über das Internet genutzt werden können, z. B. Suchmaschinen und E-Mail. Viele Verbraucherinnen und Verbraucher nutzen regelmäßig solche Internetdienste, um sich beispielsweise in Nachrichten-Portalen zu informieren, über Messenger-Dienste oder soziale Netzwerke miteinander zu kommunizieren oder um in Online-Shops ihre Einkäufe zu tätigen.

Jedoch sind damit auch verschiedene Gefahren verbunden: Kriminelle entwickeln immer wieder neue Betrugsmethoden, um sich auf Kosten von Verbraucherinnen und Verbrauchern einen Vorteil zu verschaffen. Dafür manipulieren sie Webseiten, erstellen Fake-Webseiten, Fake-Shops und Fake-Accounts (in sozialen Netzwerken). Allen gemeinsam ist die vorsätzliche Täuschung von Nutzerinnen und Nutzern. Diese Täuschung könnte man auch als „Face/Off“ bezeichnen.

In diesem Dokument wird der Aspekt der Täuschung von Verbraucherinnen und Verbrauchern durch Defacement (die unberechtigte Manipulation von Webseiten), Fake-Webseiten, Fake-Shops und Fake-Accounts genauer betrachtet und Verbraucherinnen, Verbrauchern und Webseiten-Betreibern werden einige Kriterien an die Hand geben, worauf bei der Nutzung der entsprechenden Internetdienste (z. B. Einkauf im Internet oder Nutzung sozialer Netzwerke) geachtet werden sollte.

3 Defacement

Bei einem Defacement („Verunstaltung“) wird eine bestehende Webseite durch einen Angreifenden manipuliert, um die Reputation einer Organisation zu beschädigen oder um das Vertrauen der Nutzerinnen und Nutzer zu erschüttern. Häufig besteht die Motivation des Angreifenden auch darin, Ansehen in der Defacement-Szene zu erlangen.

Szenario

Die Webseite eines Unternehmens (z. B. das Content-Management-System (CMS)) enthält eine oder mehrere Sicherheitslücken. Dies können beispielsweise fehlende Sicherheitsupdates oder leicht zu erratende Zugangsdaten sein. Angreifende nutzen diese Sicherheitslücken, um die Inhalte der Webseite teilweise oder sogar vollständig zum Nachteil des Unternehmens zu verändern.

Beispiel

Hacker manipulieren im Kontext einer politischen Wahl die Webseite der politischen Gegnerinnen und Gegner.

Empfehlungen

für Verbraucherinnen und Verbraucher

- Seien Sie kritisch: Wenn Ihnen Inkonsistenzen in der Darstellung einer Person oder eines Unternehmens auffallen, können das Hinweise auf Defacement sein.
- Verbraucher-Empfehlung: "Spam, Phishing & Co"
- Verbraucher-Empfehlung: "Sicher im digitalen Alltag"

für Webseiten-Betreiber

- Cyber-Sicherheitsempfehlung: "Prävention und Erste Hilfe bei Website Kompromittierung oder Defacement"
- Cyber-Sicherheitsempfehlung: "Absicherung von Telemediendiensten nach Stand der Technik"

4 Fake-Webseiten

Basierend auf einer bestehenden legitimen Webseite wird eine neue (Fake-) Webseite teilweise nachgebaut oder fast vollständig kopiert, um mit Phishing an sensible Daten (z. B. Passwörter oder Kreditkartendaten) von Verbraucherinnen und Verbrauchern zu gelangen.

Szenario

Nutzerinnen und Nutzer werden dazu verleitet, über einen Link auf die Fake-Webseite zuzugreifen. Sie wähnen sich – durch das täuschend echte Erscheinungsbild der Webseite – auf der Originalseite und geben bedenkenlos persönliche Daten ein oder laden sich unbemerkt Schadprogramme auf ihre Geräte. Angreifende lassen dabei oft eine Internet-Adresse ("Domain") registrieren, deren Name fast identisch ist mit dem Namen der Webseite, die sie kopieren möchten, z. B. "bsi.bunt.de" statt "bsi.bund.de". Zusätzlich besorgen sie sich ein valides SSL-Zertifikat, um die zu kopierende Webseite täuschend echt nachzubilden bzw. um Zertifikatswarnungen im Browser zu umgehen.

Beispiel

Angreifende verschicken eine SMS oder E-Mail im vorgetäuschten Design eines Kreditinstituts an Nutzerinnen und Nutzer. Um Druck auszuüben wird auf eine angeblich bevorstehende Kontosperrung verwiesen. Der in der SMS oder E-Mail enthaltene Link zur Eingabe der Zugangsdaten verweist jedoch auf eine Fake-Webseite der Angreifenden.

Empfehlungen

für Verbraucherinnen und Verbraucher

- Seien Sie kritisch: Fragen Sie sich, ob die Anfrage zur Preisgabe von sensiblen Daten glaubhaft und plausibel scheint.
- Verbraucher-Empfehlung: "Onlinebanking, Onlineshopping und mobil bezahlen"
- Verbraucher-Empfehlung: "Spam, Phishing & Co"
- Verbraucher-Empfehlung: "Wie erkenne ich Phishing-E-Mails und -Webseiten?"
- "Aktuelle Beispiele für Phishing-Angriffe"
- "Wie schützt man sich gegen Phishing?"

5 Fake-Shops

Ein Fake-Shop ist ein (betrügerischer) Online-Shop, der mit Lockangeboten Nutzerinnen und Nutzer zum Einkauf animiert. Die Zahlung erfolgt häufig gegen Vorkasse. Die Ware wird anschließend gar nicht oder nur in schlechter Qualität ausgeliefert. Dadurch entsteht den Verbraucherinnen und Verbraucher ein finanzieller Schaden.

Szenario

Ein Online-Shop bietet teure Marken- und Consumer-Produkte, z. B. Smartphones, Notebooks, weit unter dem üblichen Marktpreis an. Um die Besucherinnen und Besucher zum Kauf zu animieren, wird oftmals zusätzlich eine angeblich geringe verfügbare Stückzahl („letzter Artikel“) suggeriert.

Beispiel

Durch Internet-Suchen oder durch Klicken auf zweifelhafte Werbebanner – z. B. auch auf seriösen Webseiten, gelangen Verbraucherinnen und Verbraucher auf Fake-Shops.

Empfehlungen

für Verbraucherinnen und Verbraucher

- Seien Sie kritisch: Fragen Sie sich, ob die preisliche Gestaltung plausibel erscheint.
- Verbraucher-Empfehlung: "Woran erkenne ich sichere Onlineshops?"
- Die SOS-Karte - Schutz beim Onlineshopping
  - zusätzlich: Überprüfen Sie, ob bei der Zahlung im Fake-Shop Zugangsdaten (z. B. zum Online-Banking) preisgegeben wurden. Falls ja, ändern Sie schnellstmöglich die entsprechenden Zugangsdaten.
- LKA Niedersachsen: Fakeshops
- Liste betrügerischer Online-Shops

6 Fake-Accounts

Ein Fake-Account in einem sozialen Netzwerk wird erstellt, um bewusst andere Nutzerinnen und Nutzer zu täuschen. Häufig gibt ein solcher Fake-Account vor, eine andere reale oder fiktive Person zu sein, um in deren Namen falsche oder verfälschte Informationen zu verbreiten. Das Ziel von Fake-Accounts kann vom Abfischen sensibler Daten bis hin zum Verbreiten von Falschinformationen reichen.

Szenario

Angreifende erstellen z. B. durch Social Engineering authentisch wirkende Accounts in den sozialen Netzwerken, um eine bestimmte Person darzustellen bzw. nachzuahmen.

Beispiel

- Ein angeblicher Bekannter sendet Ihnen eine Freundschaftsanfrage, die Sie auch bestätigen. Anschließend nimmt der Angreifende, der hinter diesem Account steckt, Kontakt mit Ihnen auf, um an sensible Daten (z. B. Ihre Telefonnummer, Informationen Ihrer Freunde) zu gelangen.
- Ein legitimer Nutzer „abc_1“ veranstaltet ein Gewinnspiel in den sozialen Medien. Kriminelle legen einen ähnlich klingenden Account „abc_2“ an und schicken hierüber private Nachrichten an die Teilnehmenden des Gewinnspiels des legitimen Accounts. Darin behaupten sie, dass die Person gewonnen hat und fordern z.B. Adresse, Bankdaten, etc. oder verweisen auf einen Phishing-Link.

Exkurs "Social Bots"

Fake-Accounts werden häufig in Verbindung mit Social Bots genutzt. Bots sind Computerprogramme, die im Internet (halb-) automatisiert mit menschlichen Nutzenden in sozialen Netzwerken kommunizieren. Für Menschen ist eine Unterscheidung häufig nur schwer möglich, da diese Programme über die Fake-Accounts in den sozialen Netzwerken fast so agieren, wie ein echter Mensch. Social-Bot-Programme können durch die Nutzung der Programmierschnittstellen der sozialen Netzwerke häufig sehr einfach realisiert werden. Grundsätzlich kann man grob zwischen unbedenklichen und potentiell maliziösen Social-Bots unterscheiden:

- Unbedenkliche Social-Bots, typischerweise gekennzeichnet durch Stichworte wie "Automatisiert" o. ä., die über das aktuelle Wetter informieren oder einen bestimmten Beitrag auf mehreren sozialen Netzwerken verbreiten („Cross-Posting“).
- Maliziöse Social-Bots, typischerweise nicht gekennzeichnet, die zum Klicken auf bestimmte (potentiell schadhafte) Links verleiten oder tendenziöse Informationen zu brisanten Themen verbreiten.

Empfehlungen

für Verbraucherinnen und Verbraucher

- Verbraucher-Empfehlung: "Exkurs: Social Bots und Chat Bots"
- Verbraucher-Empfehlung: "Sicherheitseinstellungen bei Facebook, Twitter, Instagram, WhatsApp & TikTok"
- Verbraucher-Empfehlung: "Sicher durch die sozialen Medien"
- Verbraucher-Empfehlung: "Tipps zum sicheren Umgang mit sozialen Netzwerken"
- Basistipps zur IT-Sicherheit: Für alle Nutzenden sozialer Medien sind die Basisschutzempfehlungen des BSI für Verbraucherinnen und Verbraucher als Grundlage sehr empfehlenswert. Dort werden grundlegende Sicherheitsmaßnahmen vorgestellt, beispielsweise wie sichere und gut erinnerbare Passwörter oder auch die 2-Faktor-Authentisierung konzipiert werden.

- IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen: Zusätzlich bietet der IT-Sicherheitsleitfaden für Kandidierende wertvolle Hilfestellungen für alle Personen, wie sie ihren Social Media Account vor dem Zugriff von Unberechtigten schützen können.
  - Falls Sie vermuten, dass jemand Ihre Identität gestohlen hat, Ihren Namen oder Ihr Bild verwendet, denken Sie an Folgendes:
    - Erstellen Sie zwecks Beweissicherung Screenshots der Aktivitäten des Fake-Accounts.
    - Melden Sie den Fake-Account dem Betreiber des sozialen Netzwerkes.
- Verbraucher-Empfehlung: "Wie erkenne ich Phishing-E-Mails und -Webseiten?"

Was sind potentiell authentische Accounts?

- Personen, deren Namen und (Profil-) Bild Sie kennen.
- Die im Profil hinterlegten Informationen (z. B. Alter, Biografie) sind plausibel.
- Die bisher veröffentlichten Beiträge des Profils sind nachvollziehbar.
- Der Account folgt mehreren Freunden, die Sie auch kennen.
- Der Account ist von der Plattform verifiziert.
- Die Beiträge des Accounts enthalten keine verdächtigen Links.
- Die Beiträge des Accounts enthalten keine auffälligen Rechtschreib- und Grammatikfehler.

Was sind potentiell problematische Accounts?

- Fragt der Account-Inhaber nach Geld z. B. für lebenswichtige Operationen oder Reisekosten, ohne dass man sich persönlich kennt?
- Sollen Sie über eine kostenpflichtige SMS oder einen kostenpflichtigen Anruf mit dem Anderen in Kontakt treten?
- Werden Sie bereits nach kurzer Kennlernphase nach Ihrem Passwort z. B. für einen Online Shop gefragt?