CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Täuschungsversuche über Fake-Webseiten und Fake-Shops

Angreifende nutzen für Täuschungsversuche häufig gefälschte Webseiten und sogenannte Fake-Shops, um sensible Informationen wie Passwörter, E-Mail-Adressen und Bankdaten zu erbeuten. Häufig lassen sich gefälschte Webseiten und Fake-Shops auf den ersten Blick nur schwer erkennen, da es sich um täuschend echte Kopien von realen Webseiten handelt.

Tipps zum Erkennen gefälschter Webseiten

Was ist eine gefälschte Webseite?

Cyberkriminelle nutzen gefälschte Webseiten zur Erbeutung von personenbezogenen Daten, Zugangsdaten, Geldbeträgen aber auch zur Auslieferung von Schadsoftware (sog. Malware).

Es lassen sich drei Arten von betrügerischen Webseiten identifizieren, die unterschiedliche Absichten verfolgen:[1]

- **Seiten mit Werbeeinblendungen** generieren mit Klicks auf die Werbung Geld oder werden für die Auslieferung von Schadsoftware über Downloads genutzt.
- **Fake-Shops** sind täuschend echt aussehende Online-Shops, die häufig Produkte zu vorteilhaften Preisen anbieten. Zur Bezahlung der Bestellung muss ein Geldbetrag auf meist ausländische Konten überwiesen werden oder die Bank-/Kreditkartendaten werden erbeutet.
- **Phishing-Webseiten** ahmen die Anmelde- und Login-Webseiten von bekannten Diensten (z. B. Online-Händler, Kreditinstitute) nach. Ziel eines solchen Täuschungsversuchs ist die Eingabe von sensiblen Informationen wie beispielsweise Passwörter oder Kreditkartendaten.

Täuschungsversuche über Fake-Webseiten und Fake-Shops

Wie gelangt man auf gefälschte Webseiten?

Es gibt verschiedene Wege, um auf gefälschte Webseiten zu gelangen.
Phishing-E-Mails: Häufig werden Links zu gefälschten Webseiten, insbesondere zu Fake-Shops, per Phishing-E-Mails verteilt. Ziel ist es, Ihre Zugangsdaten für die echte Shop-Website abzugreifen oder Geld zu erbeuten.
SEO Poisoning: SEO Poisoning wird auch als manipulierte Suchmaschinenoptimierung bezeichnet. Gemeint sind damit kriminelle Techniken, mit denen gefälschte Webseiten in einer Suchmaschine höher gerankt (d.h. weiter oben in der Ergebnisliste angezeigt) werden. Suchmaschinen wie z.B. Webseiten, die weit oben in der Ergebnisliste stehen, werden mit wesentlich höherer Wahrscheinlichkeit von Internetnutzenden geklickt als weniger hoch gerankte Webseiten. Von Suchmaschinen gesponserte Seiten, die als Werbung angezeigt werden, können ebenfalls davon betroffen sein.
Tippfehler in der URL: Tippfehler in der URL (Webseiten-Adresse) können Sie ebenfalls auf eine gefälschte Webseite führen. Cyberkriminelle nutzen häufig URL-Adressen, die den URL-Adressen echter Webseiten zum Verwechseln ähnlich sehen.

Quellen:
[1] https://www.uni-muenster.de/Informationssicherheit/schutzen/Betruegerische_Webseiten.html
[2] https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/abzocke-online-wie-erkenne-ich-fakeshops-im-internet-13166

Tipps zum Schutz vor betrügerischen Webseiten:[2]

Updates: Halten Sie Ihre Internet-Browser durch regelmäßige Updates stets auf aktuellem Stand.
URL-Adresse überprüfen: Überprüfen Sie die URL-Adresse Ihres Internetbrowsers auf folgende Auffälligkeiten:

- Prüfen Sie, ob die Domain zu der Webseite passt, die aufgerufen werden soll.
- Achten Sie auf Rechtschreibfehler und vertauschte Buchstaben.
- Prüfen Sie die URL-Endung – üblich ist „.de“ oder „.com“.
- Überprüfen Sie den Trustscore der Webseite.
- Achten Sie auf eine sichere Verbindung, erkennbar durch das „https://“ in der Adresszeile und ggf. ein Schlosssymbol.
- Prüfen Sie das Sicherheitszertifikat einer Webseite. Klicken Sie hierzu auf das „Schlosssymbol“ neben der Adressleiste Ihres Browsers. Ihnen werden nun Informationen über das verwendete Zertifikat (z.B. die Gültigkeit) und den Betreiber der Webseite angezeigt. Diese Informationen können Sie auf Richtigkeit prüfen.
- Links in E-Mails oder Werbebanner überprüfen Sie, in dem Sie das sog. Mouse-Over nutzen. Fahren Sie hierzu mit dem Mauszeiger über den Link (ohne zu klicken). In der Fußzeile Ihres Browsers wird nun angezeigt, wohin der Link führt. Prüfen Sie auch diesen Link auf Plausibilität und Auffälligkeiten.

Gesundes Misstrauen: Hinterfragen Sie die Echtheit von Webseiten und interagieren Sie nicht mit diesen, wenn Sie eine der genannten Auffälligkeiten bemerken.

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Für weitere CSBW-Factsheets QR-Code scannen:

www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de

Stand: 01.2025