Initiative Deutsche Zahlungssysteme e.V.

SICHERHEIT
PASSWÖRTER
SPIONAGE
BETRUG
RISIKO

SOCIAL ENGINEERING

Schutz vor Betrug

Eine angebliche Verwandte, die in Schwierigkeiten steckt und Sie am Telefon um Geld bittet? Ein Prinz, der Ihnen per Mail bei einer Vorauszahlung eine große Summe Geld verspricht? Bei der Betrugsmasche „Social Engineering“ nutzen Cyberkriminelle menschliche Schwächen aus, um an Passwörter oder persönliche Informationen zu gelangen oder von Ihnen Geld zu erbeuten. Vor allem im digitalen Zeitalter steigt das Risiko, als Verbraucher:in Opfer von Betrug zu werden. Um diese Gefahren rechtzeitig erkennen und reduzieren zu können, gibt es Schutzmaßnahmen, die Verbraucher:innen ergreifen können. In diesem Dokument werden die gängigsten Praktiken und mögliche Maßnahmen beschrieben.

Wir beantworten die wichtigsten Fragen zu Social Engineering:

Was ist Social Engineering?

Welche Arten von Social Engineering gibt es?

Wie können Sie sich vor Social Engineering schützen?

Weiterführende Materialien

Social Engineering
Bundesamt für Sicherheit in der Informationstechnik

Online-Konten vor Hacking-Angriffen schützen
Verbraucherzentrale

Aktuelle Informationen
Kartensicherheit

Ihre Ansprechpartnerin: Heike Lange | E-Mail: heike.lange@initiative-dz.de
Initiative Deutsche Zahlungssysteme e.V. | Jägerstraße 54-55 | 10117 Berlin | Tel. (0 30) 439 732-803
www.initiative-deutsche-zahlungssysteme.de

Initiative Deutsche
Zahlungssysteme e.V.

Was ist Social Engineering?

Betrügerische Aktivitäten rund um das Bezahlen nehmen stetig zu – insbesondere im digitalen Umfeld. Laut dem Bundesamt für Sicherheit und Informationstechnik (BSI) stellen technische Sicherheitslücken jedoch nur einen Teil der Risiken dar. Scheitern Kriminelle an technischen Hürden wie aktueller Software, Firewalls und Virenscannern, versuchen sie, Verbraucher:innen mittels Social Engineering zu täuschen. Dabei nutzen die Betrüger:innen gezielt menschliche Eigenschaften wie Vertrauen oder Respekt vor Autoritäten aus, indem sie eine falsche Identität vortäuschen. Häufig setzen Betrüger:innen ihre Opfer dabei mit einer künstlichen Dringlichkeit unter Druck und bauen emotionalen Stress auf. Auf diesem Wege sollen Verbraucher:innen dazu verleitet werden, vertrauliche und sensible Daten schnell weiterzugeben, Sicherheitsfunktionen auszusetzen oder sogar Überweisungen zu tätigen.

Welche Arten von Social Engineering gibt es?

Social Engineering ist ein Überbegriff für eine Reihe verschiedener Betrugsmaschen, die multimedial – per Telefon, E-Mail oder Textnachricht über eine App – ablaufen können. Auf diese Art und Weise haben sich Kriminelle im digitalen Raum mittlerweile breit aufgestellt. Die Art des Betrugs kann verschiedene Formen annehmen:

Die bekannteste ist das **Phishing.** Dabei manipulieren Kriminelle Webseiten, Briefe oder E-Mails so, dass sie den Anschein erwecken, von bekannten und vertrauenswürdigen Organisationen zu kommen – wie etwa Banken, Behörden oder sozialen Netzwerken. Opfer bekommen dann beispielsweise den Hinweis, dass ihr Passwort ablaufen würde und werden dazu aufgefordert, dies mit einem Klick auf einen Link oder dem Besuch auf einer Website zu aktualisieren. Dabei landen sie jedoch auf einer gefälschten Webseite, mit der Folge, dass ihre sensiblen Daten und Informationen an Daten-Broker verkauft, ihre Online-Accounts gehackt oder ihre Bankkonten belastet werden.

Das **Spear-Phishing** geht noch gezielter vor: Ziel der Kriminellen sind hier insbesondere Mitarbeiter:innen einer Organisation, die eine Position im Management oder der IT ausüben. Ihnen wird von anderen Mitarbeiter:innen leichter geglaubt, wenn sie eine vermeintlich dringende E-Mail mit der Aufforderung zur Aktualisierung der Zugangsdaten schicken. Diese Form kommt auch im familiären Umfeld in Form von Personen, die sich als Verwandte ausgeben, vor.

Vishing beschreibt die Manipulation der Opfer über das Telefon. Dabei können die Täter:innen mithilfe einer Software ihre Nummer beim Anruf fälschen, sodass Opfer glauben, es handele sich um die Nummer einer offiziellen Stelle, wie zum Beispiel der Polizei oder einer Bank.

In den letzten Jahren sind auch so genannte **Deepfakes** zu einem immer größeren Problem geworden. Mithilfe von Künstlicher Intelligenz erstellen die Betrüger:innen Bilder, Videos und Tonaufnahmen von realen Menschen, die täuschend echt wirken, und versuchen so, an die sensiblen Daten von ihren Opfern zu kommen oder diese zu einer Zahlung zu bewegen.

Wie können Sie sich vor Social Engineering schützen?

Beim Schutz vor Social Engineering kommt es vor allem auch auf das eigene Verhalten an. Dabei gilt es in erster Linie Ruhe zu bewahren und nicht übereilt zu reagieren – auch wenn es vermeintlich schnell gehen muss. Um Ihnen dabei eine Hilfestellung zu geben, finden Sie auf der nächsten Seite eine Checkliste.

Initiative Deutsche
Zahlungssysteme e.V.

CHECKLISTE

Ist diese Nachricht betrügerisch?

Prüfen Sie den bzw. die Absender:in auf Korrektheit

Der angezeigte Name entspricht nicht immer der echten E-Mail-Adresse. Ein Klick auf den Namen zeigt oftmals die vollständige Adresse an. In einigen Fällen befinden sich auch in den E-Mail-Adressen Tippfehler bzw. Ziffern. Ist die Mailadresse untypisch und enthält beispielsweise lange Zahlenfolgen oder unbekannte Domains kann es sich um einen Betrugsversuch handeln.

Überprüfen Sie den Inhalt der Nachricht sowie Rechtschreibung und Grammatik

Phishing-E-Mails waren früher oft voller Fehler. Allerdings werden Betrüger:innen geschickter und es gibt zunehmend Nachrichten, die kaum noch oder gar keine Fehler aufweisen. Daher: Auch bei ungewöhnlichen Formulierungen besonders aufmerksam sein.

Lassen Sie Achtung walten bei dringenden Aufforderungen

Phishing-E-Mails setzen oft auf Dringlichkeit und versuchen, Druck auszuüben. Wer Druck aufbaut, möchte selten etwas Gutes. Aufforderungen, insbesondere Zahlungsaufforderungen, sollten in Ruhe überprüft werden.

Überprüfen Sie Links, ohne direkt draufzuklicken

Bewegen Sie Ihren Mauszeiger über den Link, offenbart sich in der Regel die vollständige URL. Auf mobilen Geräten wird der Link angezeigt, wenn man diesen länger gedrückt hält. Klicken Sie im Zweifelsfall lieber keinen Link, sondern navigieren Sie sich lieber selbstständig zu der entsprechenden Webseite.

Seien sie vorsichtig beim Öffnen von Anhängen

Anhänge können Malware enthalten. Dateien mit Endungen wie .exe, .zip oder .docm sollten nur geöffnet werden, wenn Sie diese erwarten oder Ihnen der bzw. die Absender:in bekannt ist. Fragen Sie im Zweifelsfall nach, ob es sich um einen legitimen Anhang handelt.

Geben Sie sensible Daten niemals weiter

Egal ob per E-Mail, Textnachricht oder Telefon – seriöse Unternehmen fordern nie dazu auf, Login-Daten, PINs, TANs oder ähnliches preiszugeben.

Zu schön, um wahr zu sein?

Angebote mit extremen Rabatten oder Versprechungen von hohen Gewinnen sind oft eine Falle. Wenn es zu gut klingt, um wahr zu sein, ist es wahrscheinlich ein Betrugsversuch.

Fragen Sie im Zweifelsfall immer nach

Verunsichert Sie ein Brief, eine E-Mail oder Textnachrichtsuchen Sie am besten direkt Kontakt zur eigenen Hausbank, Familie und/oder dem IT-Support. Dort wird Ihnen zuverlässig und seriös Hilfe angeboten.