Technische Universität München
Fakultät für Informatik

Seminararbeit
im Rahmen des Seminars
“Der Staat als Hacker”
(SOT82533)

Social Engineering und Phishing

Jens Fröhlich

12. Juni 2025

Inhaltsverzeichnis

1 Einleitung

1.1 Social Engineering und Phishing

"Hallo Mama/Papa, ich bin's. Ich habe mein Handy verloren und brauche dringend Geld. Kannst du mir bitte 100 Euro überweisen? Ich kann dir später alles erklären." - Diese Art von Nachricht wird wohl kaum einem neu vorkommen und ist ein gutes Beispiel für eine Thematik, die uns heutzutage immer häufiger begegnet: **Social Engineering**.

Dabei liegt der komplette Fokus auf dem Mensch als Schwachstelle, um durch gezielte psychologische Manipulation an vertrauliche Informationen zu gelangen. Dabei wird oft das Vertrauen des Opfers ausgenutzt, um es dazu zu bringen, sensible Daten preiszugeben oder bestimmte Handlungen vorzunehmen (wie zum Beispiel eine Geldüberweisung).[1]

Phishing im Speziellen ist eine besonders verbreitete Form des Social Engineerings. Hierbei handelt es sich um den Versuch, sich mittels gefälschter E-Mails, Telefonanrufe, Webseiten oder andere Personen auszugeben, um die Opfer zu manipulieren.[2]

1.2 Relevanz des Themas

Die praktische Relevanz dieser Angriffsmethoden lässt sich anhand aktueller Studien eindrücklich belegen.

1.2.1 Fallzahlen

Aufgrund der hohen Erfolgsquote stehen Social Engineering bzw. Phishing zurecht sehr häufig im Rampenlicht. Laut HoxHunt sind knapp zwei von drei Datenschutzverletzungen auf den Faktor Mensch zurückzuführen, von denen wiederum mehr als 80% als Phishing eingestuft werden können. Zudem ist laut SlashNext die Anzahl der Phishing-Angriffe seit 2021 um ungefähr 49% gestiegen. Besonders hervorzuheben hierbei hier, dass seit der Veröffentlichung von ChatGPT die Anzahl der Phishing-Angriffe um mehr als 4000% angestiegen ist.[3]

Allerdings hat IBM analysiert, dass etwa 15% aller Datenschutzverletzungen auf Phishing und damit auch Social Engineering zurückzuführen sind.[4] Dieser

[1] *Social Engineering – der Mensch als Schwachstelle* 2025.
[2] *Spam, Phishing & Co* 2025.
[3] *Phishing Trends Report (Updated for 2025)* 2025.
[4] *Cost of a Data Breach | Report 2024* 2025.

Unterschied kann dadurch erklärt werden, dass Phishing in Studien oft unterschiedlich definiert wird. So hat IBM höchstwahrscheinlich nur die Fälle aufgenommen, in denen Phishing eine zentrale Rolle gespielt hat, während HoxHunt auch Fälle mit einbezieht, in denen Phishing bzw. Social Engineering Teil des Angriffs, aber nicht (nur) die Hauptursache war.

1.2.2 Wirtschaftliche Schäden und Auswirkungen auf Unternehmen und Privatpersonen

Laut einer Studie von IBM verursachten größere Phishing-Angriffe im Jahr 2024 durchschnittlich einen Schaden von etwa 4,88 Millionen US-Dollar pro Vorfall.[5] Gerade Unternehmen sind besonders gefährdet, da die klaren Hierarchien es Angreifern ermöglichen, gezielt bestimmte Personen zu imitieren und bei Unternehmen generell mehr Profit erzielt werden kann.

Ein sehr bekanntes Beispiel dafür ist der Hackerangriff auf die US-amerikanische Einzelhandelskette Target aus dem Jahre 2013, der ungefähr 162 Millionen US-Dollar Schaden verursachte (wenn auch nur indirekt).[6]

2 Definition von Social Engineering

2.1 Grundprinzipien und Psychologie des Social Engineerings

Bei **Social Engineering** steht die Ausnutzung von menschlichen Eigenschaften wie Vertrauen, Angst, Autorität und Hilfsbereitschaft im Vordergrund. Durch gezielte Manipulation oder Erpressung werden unzählige Opfer (oftmals ohne ihr Wissen) dazu gebracht, Geldsummen für vermeintliche Dienstleistungen zu überweisen, sensible Daten anzugeben oder gezielt Schutzmechanismen (z.B. 2-Faktor-Authentifizierung) außer Kraft zu setzen.[7]
Im Mittelpunkt steht hierbei nicht die Umgehung von technischen Schutzmaßnahmen, sondern die gezielte Täuschung und Manipulation des Menschen als Schwachstelle, sodass technische Barrieren oft irrelevant werden. Angreifer verfeinern ihre Methoden kontinuierlich durch erprobte Angriffstechniken. Dadurch gelingt es ihnen immer schneller und häufiger, Menschen zu beeinflussen. Ein wirksamer Schutz gegen diese Angriffe kann daher nur durch **Aufklärung** der potenziellen Opfer erreicht werden.

[5] *Was ist Phishing?* 2025.
[6] *The Target Breach: A Historic Cyberattack with Lasting Consequences* 2025.
[7] *Social Engineering – der Mensch als Schwachstelle* 2025.

2.2 Gängige Methoden

Die Methoden des Social Engineerings können vielfältiger nicht sein. Bei der als **Quid pro Quo** bekannten Taktik bieten Angreifer ihren Opfern scheinbar attraktive Dienstleistungen an, um im Gegenzug an Geld (oder in manchen Fällen auch sensible Daten) zu gelangen. Diese Strategie wurde im Netz vor allem durch den YouTuber *Jim Browning* bekannt. Durch seine Videos, in denen er sogenannte Call-Center aufdeckt, und diese sukzessive **infiltriert** und am Ende an die lokalen Behörden übergibt, wird deutlich, wie einfach es ist, Menschen zu manipulieren.[8]

Oft verbunden mit Quid pro Quo ist die sogenannte **Scareware**, bei der Angreifer versuchen, ihre Opfer durch Angst dazu zu bringen, **Schadsoftware**, verkleidet als Sicherheitssoftware, herunterzuladen. Dies kann durch einfache **Pop-up Fenster** geschehen, die behaupten, das System sei infiziert, oder durch gezielte Anrufe, bei denen sich die Angreifer als Mitarbeiter bekannter Firmen ausgeben und behaupten, das Konto vom Nutzer wäre kompromittiert worden.[9]

Honeytrapping ist eine gängige Methode, um sich mit Menschen, die auf diversen Dating-Plattformen nach einem Partner/einer Partnerin suchen, anzufreunden und dadurch einen finanziellen Vorteil zu erlangen. Vor allem der Aufschwung von künstlicher Intelligenz und Dating-Portalen hat es den Angreifern umso leicht gemacht **gefälschte Profile** zu erstellen und falsche Versprechen zu geben.[10]

3 Definition von Phishing

3.1 Definition und Abgrenzung als Teilbereich des Social Engineerings

Obwohl Social Engineering und Phishing oft fälschlicherweise als Synonyme verwendet werden, ist dies allerdings nicht korrekt. Tatsächlich ist Phishing eine Form des Social Engineering, aber nicht jeder Social-Engineering-Angriff ist zugleich ein Phishing-Angriff. Phishing beschreibt den konkreten Versuch, Opfer über bestimmte Kommunikationskanäle - wie E-Mails, Webseiten oder Formen an Kurznachrichten - zu manipulieren. Social Engineering hingegen ist lediglich der Überbegriff von der Herangehensweise, bei der psychologische

[8] *Jim Browning - YouTube* 2025.
[9] *What Is Scareware?* 2025.
[10] Villavicencio 2022.

Manipulationstechniken genutzt werden, um die angestrebten Ziele zu erreichen.[11]

3.2 Die Verschiedenen Arten von Phishing

Phishing kann in zahlreiche Unterkategorien eingeteilt werden.

Eine besonders destruktive Form stellt **Spear Phishing** dar. Bei dieser Taktik werden sowohl der Empfängerkreis als auch die Inhalte der versendeten E-Mails präzise aufeinander abgestimmt. Richtig umgesetzt können solche Angriffe daher besonders glaubwürdig wirken.[12]

Eine technisch anspruchsvollere Form stellt das **Pharming** dar. Hierbei wird die Zuordnung von Webseitname zu IP-Adressen (die sogenannte DNS-Auflösung) manipuliert, sodass die Opfer zwar den korrekten Domainnamen aufrufen, aber dennoch auf eine gefälschte Webseite geleitet werden. Gegen diese Methode können sich selbst erfahrener Nutzer nur schwer schützen.[13]

Smishing ist die Form, die bereits in der Einleitung erwähnt wurde. Hier werden Opfer per SMS oder über Messenger-Dienste wie WhatsApp oft dazu verleitet, Geld zu überweisen. Ein bekanntes Beispiel hierzu ist die “Mama/Papa, ich habe mein Handy verloren und brauche Geld”-Nachricht, welche heute vermehrt zu finden ist.[14]

4 Bekannte Phishing-Skandale und ihre Folgen

4.1 Democratic National Committee (DNC)-Hack

Ein prominentes Beispiel für einen Phishing-Angriff ist der DNC-Hack der Jahre 2015 und 2016, bei dem die demokratische Partei der USA Opfer eines Spear-Phishing-Angriffs wurde. Dabei wurden E-Mails an 300 Mitarbeiter der Partei und der Clinton-Kampagne verschickt, die von russischen Hackergruppen “Fancy Bear” und “Cozy Bear” stammten. Insgesamt wurden 70GB an Daten von den Servern der Clinton-Kampagne und 300GB von den DNC-Servern gestohlen. Diese Daten wurden zusammen mit knapp 20.000 E-Mails auf WikiLeaks veröffentlicht.[15]

[11] *Sind Phishing und Social-Engineering das Gleiche?* 2025.
[12] *Was ist Phishing?* 2025.
[13] *Täuschend echte Webseiten: Wie schützt man sich vor Pharming?* 2025.
[14] Villavicencio 2022.
[15] *How The DNC Hack Changed the 2016 Presidential Election Results* 2025.

Im Januar 2017 untersuchten sowohl das FBI, als auch die CIA, NSA und mehrere andere US-Geheimdienste, ob die russische Regierung mit diesem Angriff die Präsidentschaftswahl 2016 zugunsten von Donald Trump beeinflussen wollte.[16]

Obwohl es also keine klaren Beweise gibt, wird angenommen, dass der Angriff eine signifikante Rolle bei der öffentlichen Meinungsbildung spielte. Der Fall dient somit nicht nur als Beispiel für die Umsetzung von Social Engineering und Phishing, sondern verdeutlicht auch die weitreichenden politischen und gesellschaftlichen Folgen, die solche Angriffe haben können.

4.2 Twitter Spear Phishing Attack (2020)

Ein weiterer bekannter Vorfall ist der Twitter-Skandal aus dem Jahr 2020, bei dem es einer Gruppe mittels Spear-Phishing gelang, die Accounts von bekannten Personen wie Elon Musk, Barack Obama, Joe Biden und Bill Gates zu übernehmen. Dabei wurden mehrere Mitarbeiter durch E-Mails dazu gebracht, ihre Zugangsdaten preiszugeben, sodass sich der damals 17-jährige Graham Ivan Clark Zugriff auf die internen Systeme von Twitter verschaffen konnte. Dadurch gelang es ihm die Support-Tools von Twitter zu nutzen, um die einige berühmte Accounts zu übernehmen.

Insgesamt wurde von 45 Konten aus getweeted, wobei die Angreifer bei 36 Konten auch auf private Nachrichten zugreifen konnten. Von diesen Accounts wurde während der Covid-19-Pandemie ein Bitcoin-Betrug gestartet, bei dem die Angreifer fälschlicherweise versprachen, alle erhaltenen Bitcoins zu verdoppeln und zurückzugeben. Dadurch wurden insgesamt ca. 12,86 BTC (damals umgerechnet rund 100.000 Euro) erbeutet.[17]

Abbildung 1: Screenshot von Bill Gates' Twitter Account während des Hacks[18]

[16] *Intercepted Russian Communications Part of Inquiry Into Trump Associates* 2025.
[17] *What Happened During The Twitter Spear-Phishing Attack?* 2025.

Genauere Details zu den Umständen des Hacks wurden von Twitter aufgrund von Sicherheitsrisiken nicht veröffentlicht.

Im August 2021 wurden dann vier Personen verhaftet, darunter der damals noch 17-jährige Graham Ivan Clark, der die Spear-Phishing-Attacke initiiert hatte. Ein 19-jähriger führte zusammen mit einem 22-jährigen den Bitcoin-Scam aus, während ein weiterer 22-jähriger Clark bei der Umsetzung des Angriffs unterstützte.[19]

5 Bezug zum Ethischen Hacking

Nach den vorangegangenen Definitionen und Beispielen stellt sich die naheliegende Frage: Wenn diese Taktiken so schädlich sind, warum werden sie dann von Sicherheitsexperten eingesetzt? Die Antwort liegt im Konzept des **Ethischen Hackings**. Der erste Schritt zum Verständnis dieser Praxis führt über das sogenannte **Penetration Testing** (auch **Pentesting** genannt).

5.1 Pentesting von Social Engineering

Beim Pentesting geht es darum, die Sicherheit eines Systems durch simulierte Angriffe auf die Probe zu stellen. Hierbei geht es nicht darum, Schaden anzurichten, sondern potenzielle Schwachstellen noch vor Angreifern zu identifizieren und weitestgehend zu beheben.

Dazu beauftragen Unternehmen Sicherheitsexperten, die die eigenen Systeme auf Schwachstellen untersuchen. Dazu nutzen sie die gleichen Methoden und Werkzeuge, welche auch Angreifer verwenden würden. Pentesting kann in verschiedenen Formen erfolgen, wie etwa das Ausnutzen von Schwachstellen in Software oder Hardware, allerdings auch sehr häufig in Form von Social Engineering und Phishing.

Ein Beispiel hierfür wäre, wenn ein Pentester eine E-Mail, die vermeintlich von der IT-Abteilung stammt, mit einem Link an die Mitarbeiter des Unternehmens schickt. Jedoch führt der Link zu keiner schädlichen Webseite, sondern zu einer Informationsseite, in welcher erklärt ist, dass es sich um einen Test handelt. Dadurch wird den Mitarbeitern gleichzeitig verdeutlicht, wie leicht solche Angriffe umsetzbar sind, ohne wirtschaftlichen Schaden anzurichten. Im Anschluss an solche Tests werden alle Daten ausgewertet und, falls nötig, mehrere Schulungen angeboten.

[18] Shah 2020.
[19] *What Happened During The Twitter Spear-Phishing Attack?* 2025.

5.2 Rolle von Ethik und Moral

Durch die harmlose Intention hinter Pentesting könnte man auf den ersten Blick annehmen, Menschen als Versuchsobjekte zu benutzen wäre moralisch und ethisch vertretbar. Allerdings muss hier beachtet werden, dass der einzige Unterschied zwischen einem ethischen Hacker und einem Angreifer der **Kontext** ist. Ethisch betrachtet täuscht man hier wissentlich Menschen, nur um einem guten Zweck zu dienen.

Hierzu gilt es, das **Prinzip des minimalen Schadens** als oberste ethische Regel zu betrachten. So sollten Personen, die in dem Test geprüft werden, keineswegs gedemütigt werden. Zudem soll keine Angst oder Panik verbreitet werden. So sollte die E-Mail keine gefälschte Kündigung enthalten, sondern zum Beispiel die Ankündigung eines neuen Sicherheitssystems. Zudem sollte durch die Tests kein Datenverlust entstehen.

In der Herangehensweise lassen sich auch gewisse Züge des **Utilitarismus** erkennen. Diese Lehre besagt, dass eine Handlung exakt dann moralisch richtig ist, wenn das höhere Wohl aller Beteiligten dadurch gefördert wird. Aus dieser Perspektive lassen sich Social-Engineering-Tests an Menschen gut rechtfertigen, da sie genau diese Absicht verfolgen: Das kurzfristige Behagen Einzelner im Gegenzug zu dem langfristigen Schutz des Unternehmens. Dadurch lassen sich Pentests an Menschen sehr leicht rechtfertigen, da genau diese Absicht verfolgt wird.

Eine vollständige **Aufklärung** ist nach den Tests unabdingbar. Alle Beteiligten sollen danach erfahren, dass es sich um einen Test gehandelt hat, was das Ziel hinter diesen war und welche Maßnahmen jeder Einzelne ergreifen kann, damit er nicht Opfer eines tatsächlichen Angriffs wird. Die Mitarbeiter sollen sich nach den Tests sicherer und informierter fühlen, anstatt verunsichert und verängstigt.

Die Auswertung der Tests sollte auch unter allen Umständen anonymisiert erfolgen. Es geht nur um die statistische Auswertung, nicht um die Beurteilung jedes Einzelnen.

5.3 Rechtliche Rahmenbedingungen

Nachdem die ethischen Aspekte dargelegt wurden, stellt sich noch die Frage, in welcher Form solche Pentests legal durchgeführt werden können. In Deutschland gilt grundsätzlich das Hacking-Verbot und wird im Strafgesetzbuch (StGB) unter Strafe gestellt. Für ethische Hacker sind vor allem die sogenannten **Hackerparagraphen** von Bedeutung, die in § 202a bis § 202c StGB und § 303 StGB zu finden sind.

Während § 202a StGB das Ausspähen von Daten, § 202b StGB das Abfangen von Daten und § 202c StGB die Vorbereitung auf das Ausspähen und Abfangen von Daten unter Strafe stellt, sehen diese Paragraphen zunächst erstmal keine Ausnahmen für ethische Hacker vor. Von entscheidender Relevanz ist hierbei die **Einwilligung des Betroffenen**. Diese ist unerlässlich, damit ethische Hacker legal arbeiten können. Alle ethischen Hacker müssen sich also vorab jeglicher Arbeit vertraglich absichern, sodass sie im Falle eines Rechtsstreits beweisen können, dass sie die Erlaubnis des Betroffenen hatten. Dort werden alle Rahmenbedingungen wie Prüfungsumfang, Dauer, Art der Tests, Zielgruppe oder Verschwiegenheit, an die sich der Hacker unter allen Umständen halten muss, festgehalten.

Abschließend lässt sich also festhalten, dass man ohne Vertrag kein Pentesting durchführen darf. Erst die vorherige schriftliche und präzise Einwilligung des Rechteinhabers legalisiert das ethische Hacken. Und diese Einwilligung bildet somit die juristische Trennlinie, welche sogenannte **Black-Hat-Hacker** von **White-Hat-Hackern** trennt.

6 Ausblick

6.1 Bedeutung von Präventionsmaßnahmen und Sensibilisierung

Jeder denkt, er würde niemals auf solche Angriffe hereinfallen. Doch die Realität sieht aus statistischer Perspektive anders aus. IT-Schutzmechanismen helfen nur bedingt, also muss die Sicherheitslücke beim Menschen geschlossen werden. Im Mittelpunkt der Abwehr stehen daher Präventionsmaßnahmen in Form von regelmäßigen Schulungen, um die Sensibilisierung potenzieller Opfer zu fördern. Solche Schulungen sollten unter anderem vermitteln, dass nur Links aus vertrauenswürdigen Quellen angeklickt werden sollen und persönliche Daten nicht leichtfertig weitergegeben werden dürfen. Zudem ist gezielte Aufklärung besonders gefährdeter Gruppen, beispielsweise älterer Menschen durch Institutionen wie Banken oder den Behörden, von essenzieller Bedeutung, um auch diese vor gängigen Betrugsmaschen zu schützen.

6.2 Zukünftige Entwicklungen und Herausforderungen

Eine der größten Herausforderungen stellt der Fortschritt künstlicher Intelligenz dar, die es potenziellen Opfern erschwert, Angriffe zu erkennen. Stimmen

können täuschend echt imitiert werden und Texte können so verfasst werden, als stammen sie von der vertrauten Person. Zudem können Angriffe durch KI-Tools automatisiert werden, sodass das Gesamtvolumen an Angriffen voraussichtlich weiter steigen wird. Angesichts dieser Entwicklungen wird es umso wichtiger, dass sich die Gesellschaft intensiv mit der Thematik auseinandersetzt. Eine kontinuierliche Aufklärung und das präventive Erlernen von Schutzmaßnahmen sind der Schlüssel, um der wachsenden Bedrohung durch Social Engineering entgegenzuwirken.

Literaturverzeichnis

Cost of a Data Breach | Report 2024. URL: https://www.ibm.com/reports/data-breach (besucht am 23. 05. 2025).

How The DNC Hack Changed the 2016 Presidential Election Results. URL: https://www.idstrong.com/sentinel/the-dnc-hack (besucht am 25. 05. 2025).

Intercepted Russian Communications Part of Inquiry Into Trump Associates. URL: https://www.nytimes.com/2017/01/19/us/politics/trump-russia-associates-investigation.html (besucht am 25. 05. 2025).

Jim Browning - YouTube. URL: https://www.youtube.com/@JimBrowning (besucht am 21. 05. 2025).

Phishing Trends Report (Updated for 2025). URL: https://hoxhunt.com/guide/phishing-trends-report#part-i-phishing-trends-amp-statistics (besucht am 22. 05. 2025).

Shah, C. *Tweet über gehackte Accounts*. 15. Juli 2020. URL: https://x.com/adv_chandnishah/status/1283517681459589122 (besucht am 04. 06. 2025). Tweet veröffentlicht am 15. Juli 2020, zeigt mehrere Screenshots von gehackte Twitter-Accounts.

Sind Phishing und Social-Engineering das Gleiche? URL: https://www.keepersecurity.com/blog/de/2023/09/05/are-phishing-and-social-engineering-the-same/ (besucht am 06. 06. 2025).

Social Engineering – der Mensch als Schwachstelle. URL: https://www.bsi.bund.de/dok/11287460 (besucht am 21. 05. 2025).

Spam, Phishing & Co. URL: https://www.bsi.bund.de/dok/507910 (besucht am 21. 05. 2025).

Täuschend echte Webseiten: Wie schützt man sich vor Pharming? URL: https://www.vis.bayern.de/geld_versicherungen/konten_zahlungsverkehr/pharming.htm (besucht am 06. 06. 2025).

The Target Breach: A Historic Cyberattack with Lasting Consequences. URL: https://www.frameworksec.com/post/the-target-breach-a-historic-cyberattack-with-lasting-consequences (besucht am 23. 05. 2025).

Villavicencio, A. *10 Arten von Social-Engineering-Angriffen*. 2022. URL: https://www.crowdstrike.com/de-de/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ (besucht am 21. 05. 2025).

Was ist Phishing? URL: https://www.ibm.com/de-de/think/topics/phishing (besucht am 23. 05. 2025).

What Happened During The Twitter Spear-Phishing Attack? URL: https://teampassword.com/blog/what-happened-during-the-twitter-spear-phishing-attack (besucht am 02. 06. 2025).

What Is Scareware? URL: https://www.keepersecurity.com/blog/2023/07/28/what-is-scareware/ (besucht am 25. 05. 2025).