

Social Engineering

Definition

- engl. „angewandte Sozialwissenschaft“ / „soziale Manipulation“
- menschliche Interaktionen mit dem Ziel der Manipulation des Opfers
- Absicht ist der Identitäts-, Daten- oder Vermögensdiebstahl, sowie die Erschleichung von kostenpflichtigen Dienstleistungen
 - Im Extremfall auch Industriespionage und Sabotage

Formen des Social Engineerings (SE)

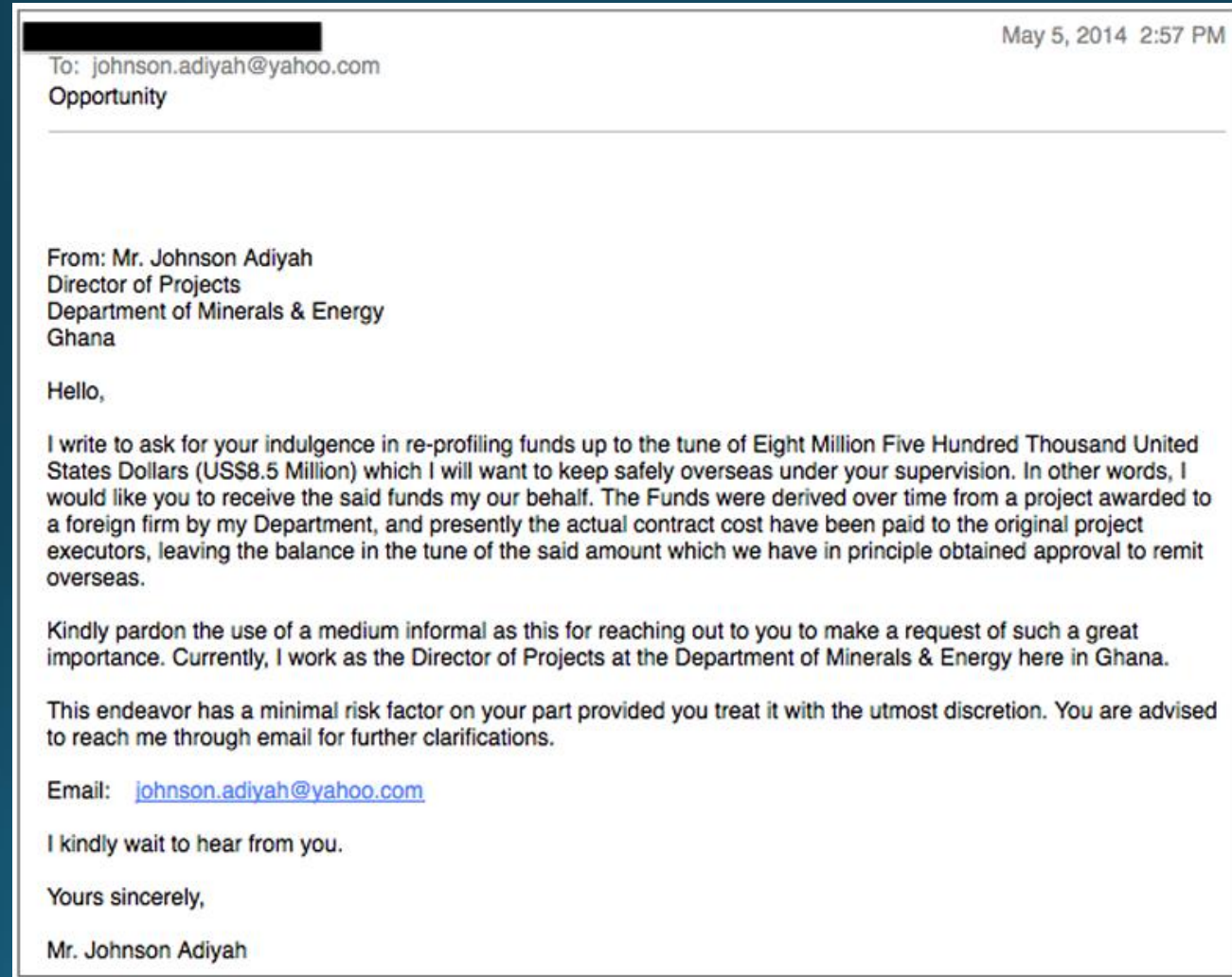
- Smishing
- Dumpster Diving
- Reverse Social Engineering
- Baiting
- Tailgating
- Vishing
- **Phishing**

**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

Phishing-Formen

- Allgemeines Phishing
 - „Masse statt Klasse“
 - Ähnlich wie Spam mit möglichst geringem Aufwand möglichst viele potentielle Opfer erreichen (z.B. „Nigerian 419“)
 - Hat eine sehr geringe Erfolgsquote (~5%), dafür aber auch minimale Kosten
 - Hochgradig automatisierbar durch z.B. Harvester/Spider, Scripte, etc.

Phishing-Formen



Phishing-Formen

- Allgemeines Phishing
 - „Masse statt Klasse“
 - Ähnlich wie Spam mit möglichst geringem Aufwand möglichst viele potentielle Opfer erreichen (z.B. Nigerian 419)
 - Hat eine sehr geringe Erfolgsquote (~5%), dafür aber auch minimale Kosten
 - Höchstgradig automatisierbar durch z.B. Harvester/Spider, Scripte, etc.
- Spear Phishing
 - Zugeschnitten auf eine kleine Personengruppe oder eine einzelne Person
 - Hohe bis maximale Erfolgsquote (~50-70%)
 - Gewissermaßen hoher Aufwand (viel Handarbeit, Automatisierung kaum möglich)

Phishing-Phasen

- Planung + Reconnaissance
- Setup
- Informationssammlung
- Ausnutzung der gewonnenen Informationen
- Post-Attack clean-up

Planung I

- Auswahl der zu phishenden Firma/Zielperson
- Auswahl der Art des „Angriffs“
 - Kompromittierte Datei
 - .zip- im .zip-File zur Umgehung des AV
 - Office-Dokument mit Makro
 - Etc.
 - Link zur kompromittierten Webseite
 - Subdomains (<http://signin.ebay.com.example.de/>)
 - Anmeldedaten (<http://ebay.de:ebay@example.de/>)
 - Gross-/Klein-Schreibung (<http://www.paypal.de/>) -> großes i statt kleinem L
 - IP-Adresse als Hex: <http://oxcoa80101/> - <http://192.168.1.1/>
 - Etc.
 - Formular in der E-Mail selbst

Planung II

- Auswahl des psychologischen Triggers
 - Gier
 - Neugier
 - Freundlichkeit / „Soziale Verpflichtung“
 - Autorität
 - Dringlichkeit / Zeitdruck
 - Mögliche Kompromittierung
 - Angst
 - Mitgefühl
 - Etc.
- Auswahl des Absenders der E-Mail
 - Mit Subdomains arbeiten
 - Mail-Spoofing

Reconnaissance

- Passive Reconnaissance (Ohne direkten Kontakt zur Zielfirma/-Person)
 - Veranstaltungsseiten
 - Social Media
 - Webarchiv (<https://archive.org/web/>)
- Aktive Reconnaissance
 - Direkter Kontakt mit der Zielperson / dem Unternehmen
 - Kontakt zum Umfeld der Zielperson / des Unternehmens

					00:00:00	999
					02:00:00	999
Mixed	1	Volkswagen VO-Runners 2	01:19:14	86	00:18:17	5
					00:18:53	8
					00:20:38	28
					00:21:26	45
					00:21:43	55
					02:00:00	999
Mixed	2	Uni Kassel Versität	01:19:31	116	00:17:32	3
					00:19:23	16
					00:20:40	30
					00:21:56	67
					00:22:06	70
					00:32:40	602
Mixed	3	Laufbande Retterode	01:24:01	196	00:18:41	6
					00:20:24	24
					00:22:22	78
					00:22:34	88
					00:24:18	161
					00:22:31	888
Mixed	4	Auf Achse	01:27:45	284	00:19:58	20
					00:21:37	52
					00:22:29	83
					00:23:41	129
					00:22:33	888
					02:00:00	999
Mixed	5	Partyservice Giese - Blumenhaus Wennmacher	01:31:26	568	00:17:06	1
					00:23:05	112
					00:24:05	150
					00:27:10	305
					02:00:00	999
					02:00:00	999
Mixed	6	Landkreis Kassel/Volkshochschule 1	01:31:40	415	00:22:09	71
					00:22:23	79
					00:22:48	100
					00:24:20	165
					00:24:47	190
					00:24:59	201
Mixed	7	Kasseler Sparkasse	01:34:24	610	00:19:34	18
					00:23:03	109
					00:24:38	180
					00:27:00	300

← → ↻ 🔒 [DE] | view-source:https://www. .de/fileadmin/downloads/broschueren/_imagebroschuere_1605.pdf

```
15364 </rdf:Seq>
15365 </crs:GradientBasedCorrections>
15366 <Iptc4xmpCore:CreatorContactInfo
15367   Iptc4xmpCore:CiAdrPcode="34119"
15368   Iptc4xmpCore:CiTelWork="0172/ "
15369   Iptc4xmpCore:CiAdrRegion="Hessen"
15370   Iptc4xmpCore:CiAdrCity="Kassel"
15371   Iptc4xmpCore:CiAdrCtry="Deutschland"
15372   Iptc4xmpCore:CiEmailWork="info@ .com"
15373   Iptc4xmpCore:CiAdrExtadr=" "
15374   Iptc4xmpCore:CiUrlWork="www. .com"/>
15375 </rdf:Description>
```

Finden Sie Personen auf XING

starbucks kassel

Suchen

Suchergebnisse für: starbucks kassel



[Redacted]
Store Manager
Kassel, Deutschland



[Redacted]
Kuratorin
Frankfurt, Deutschland



[Redacted]
Service Teamleiter Region Niedersachsen, Kassel, Herford
Hannover, Deutschland

Kostenlos Mitglied werden:

Vorname

Nachname

E-Mail

Passwort

☐ Ich akzeptiere die
[Datenschutzbestimmungen](#) und [AGB](#).

Jetzt registrieren



Starbucks Deutschland



Home 20+



Deutschland

Starbucks
Deutschland
(Kassel,
Germany) ✓

Home

About

Photos

Reviews

Likes

Posts

Create a Page



Like

Share

Save

More

Call Now



Status



Photo / Video



Write something on this Page...



Starbucks Deutschland

November 14 at 2:00pm · 🌐

Hello my dear friend, welcome back. #NewYorkCheesecake



Coffee Shop
in Kassel, Germany

4.4 ★★★★★ Open Now

Search for posts on this Page



2,563 people like this



3,173 people have been here



Open Now · 8:00AM - 8:30PM

Get additional info

Chat (Off)



Deutschland

Starbucks
Deutschland
(Kassel,
Germany) ✓

Home

About

Photos

Reviews

Likes

Posts

Create a Page



👍 Like ➦ Share 📌 Save ⋮ More ▾

Call Now

People

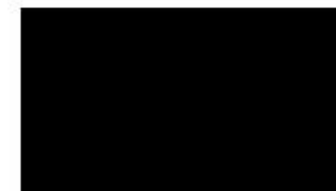
16 People Talking About This

3,173 People Checked In Here

2,563 Total Page Likes
▲ 0.2% from last week

6 New Page Likes
▲ 500%

Invite your friends to like Starbucks De...



Invite

Invite

See All Friends

— This week
— Last week

Chat (Off)

Reconnaissance

Facebook Graph Search


- „versteckte“ Funktion
 - Facebook-Spracheinstellung: Englisch
- Nützliche Befehle: <https://wollmilchsau.de/human-resources/facebook-suche-go-befehle/>




EXPLORE


 Groups

 Pages

 Events 3

 On This Day 4

 Photos

 Pages Feed 20+

▼ See More...

CREATE

[Ad](#) · [Page](#) · [Group](#) · [Event](#)



 Add Friend ... ▼

Works at Starbucks Deutschland
Studied at Universität zu Köln
Lives in Essen



 Add Friend ... ▼

Works at Starbucks Deutschland
Studied at FH Bonn-Rhein-Sieg
Lives in Bonn, Germany



 Add Friend ... ▼

Store Shift Supervisor at Starbucks Deutschland
Went to Albrecht-Dürer-Schule, Berufskolleg der Stadt Düsseldorf
Lives in Dinslaken
1 mutual friend:



 Add Friend ... ▼


Barista at Starbucks Deutschland
Lives in Duisburg
Read Jean Paillett - Legenden sterben nie



 Add Friend ... ▼

Works at Starbucks Deutschland
Went to Bernhard Overberg Realschule
Lives in Recklinghausen, Germany




 Add Friend ... ▼

Barista at Starbucks Deutschland
Read Hogwart wychował mnie na świetnego czarodzieja
Married to Krystian Mikulski since October 2, 2015

English (US) · Deutsch · Türkçe ·
Español · Português (Brasil)



[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  ·
[Cookies](#) · [More](#) ▼

Facebook © 2016

Chat (Off)



People who worked at Starbucks Deutschland



Home 20+



EXPLORE

Groups

Pages

16 Events 3

On This Day 4

Photos

Pages Feed 20+

▼ See More...

CREATE

Ad · Page · Group · Event



Add Friend



Works at Abercrombie & Fitch
Former Barista at Starbucks Deutschland
Studies Kulturwirt at Universität Duisburg-Essen '18
1 mutual friend:



Add Friend



Mönchengladbach, Germany
Worked at Starbucks Deutschland
Lives in Mönchengladbach, Germany



Add Friend



Konrad-Adenauer-Schule
Worked at Starbucks Deutschland
Went to Konrad-Adenauer-Schule
1 mutual friend:



Add Friend



Works at Starbucks Deutschland
Studied at Universität zu Köln
Lives in Essen



Add Friend



Works at Starbucks Deutschland
Studied at FH Bonn-Rhein-Sieg
Lives in Bonn, Germany



Add Friend



Store Shift Supervisor at Starbucks Deutschland
Went to Albrecht-Dürer-Schule, Berufskolleg der Stadt Düsseldorf
Lives in Dinslaken

English (US) · Deutsch · Türkçe ·
Español · Português (Brasil)



Privacy · Terms · Advertising · Ad Choices ·
Cookies · More

Facebook © 2016

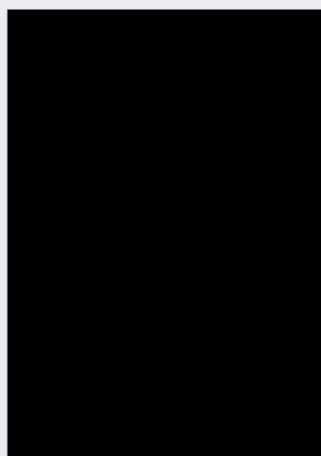
Chat (Off)



Single women who live nearby



Home 20+



EXPLORE

Groups

Pages

16 Events 3

On This Day 4

Photos

Pages Feed 20+

▼ See More...

CREATE

[Ad](#) · [Page](#) · [Group](#) · [Event](#)

Kassel, Germany
Single · Female · Interested in males
Lives in Kassel, Germany

Add Friend ... ▼

Elisabeth-Knipping-Schule
Single · Female · Interested in males
Lives in Kassel, Germany

Add Friend ... ▼

Elisabeth-Knipping-Schule
Single · Female · 25 years old
Lives in Kassel, Germany

Add Friend ... ▼

Dancer at Justin Bieber - The Bieberhood Fan Site
Single · Female
Lives in Kassel-Wilhelmshöhe, Hessen, Germany

Add Friend ... ▼

Haupt-und Realschule Kirchditmold
Single · Female · 47 years old · Interested in males
Lives in Kassel, Germany

Add Friend ... ▼

Works at Cineplex Baunatal
Single · Female · Interested in males

Add Friend ... ▼

English (US) · Deutsch · Türkçe ·
Español · Português (Brasil)



[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#) ·
[Cookies](#) · [More](#) ▼

Facebook © 2016

Chat (Off)



Apps used by people who worked at Starbucks Canada



Home 20+



EXPLORE

Groups

Pages

Events

4

On This Day

4

Photos

Pages Feed

20+

▼ See More...

CREATE

Ad · Page · Group · Event



Monster Legends

★★★★★ Games · Action

Breed new species! Battle through treacherous lands in Adventur...
Amber Lee Lane plays this · Amber is a Barista at Starbucks

Play Now



Avataria

★★★★★ Games · Simulation

Live, love, laugh, chat! Life is what you make it in Avataria on Face...
Louise Gabrielle Funcion plays this · Louise was a Manager at St...

Play Now



Diggy's Adventure

★★★★★ Games · Puzzle

THE #1 RATED ADVENTURE GAME ON FACEBOOK
Louise Gabrielle Funcion plays this · Louise was a Manager at St...

Play Now



Monster Busters

★★★★★ Games · Match 3

The most advanced match 3 puzzle game ever! Defeat the monst...
Donna Madrigal plays this · Donna worked at Starbucks

Play Now



Township

★★★★★ Games · Builders

Township is a unique blend of city-building and farming experienc...
Mai Nguyen plays this · Mai was a Barrista at Starbucks
Alexandra Spargo and 1 other friend play this

Play Now



Mobile

★★★★★ Photo

The Facebook Mobile application allows you to view a stream of the...
Ersan Ameti uses this · Ersan worked at Starbucks

Use Now

English (US) · Deutsch · Türkçe ·
Español · Português (Brasil)



Privacy · Terms · Advertising · Ad Choices ·
Cookies · More

Facebook © 2016

Chat (Off)

Reconnaissance

Facebook Identify

- Konto-Findung: <https://www.facebook.com/login/identify>

Finde dein Konto

E-Mail-Adresse, Telefonnummer, Benutzername oder
vollständiger Name



Ich kann mein Konto nicht identifizieren

Suchen

Abbrechen

Setze dein Passwort zurück

Wie möchtest du dein Passwort zurücksetzen?

- ☒  Einen Link zum Zurücksetzen meines Passworts per E-Mail senden
m*****r@t*****.de
- ☐  Einen Code zum Zurücksetzen meines Passworts per SMS senden
+*****14



Facebook-Nutzer

Hast du auf diese keinen Zugriff mehr?

Weiter

Das bist du nicht?

Du kannst deinen Namen und dein Profilbild sehen, da es deine Privatsphäre-Einstellungen zulassen.

1	m*****r@t*****.de
2	m. r@t-online.de

Setup

Social Engineering Toolkit (SET) (live)

- Site-Cloner

Python-Script zum E-Mail-Versand (live)

- E-Mail-Versand

Informationssammlung

- Automatische E-Mail-Antworten
- Gewonnene (Zugangs-)Daten
- Ausgeführte/Geöffnete Anhänge/Exploits

Ausnutzung der gewonnenen Informationen

Automatische E-Mail-Antworten

- Ist das „Ziel“ im Urlaub/Krank?
- Wird ein alternativer Ansprechpartner genannt?
- Eventuell wieder von Vorne beginnen

Gewonnene (Zugangs-)Daten

- Unterschiedlich, je nach Ziel des Angriffs
 - Weiterleitung / Kopie der E-Mails einrichten
 - Passwort-Rücksetz-Adresse ändern
 - Eigene Telefonnummer hinterlegen

Ausgeführte/Geöffnete Anhänge/Exploits

- Unterschiedlich, je nach Ziel des Angriffs
 - Verschlüsseln
 - Hintertür einrichten
 - Sabotage

Post-Attack clean-up

Je nach Ziel/Art des Angriffs

- Benachrichtigungsmails über „unüblichen Login“ löschen
- Phishing-Mail an sich löschen (falls Zugang zum E-Mail Account)
- Spuren verwischen / Falsche Spuren legen

Fazit

Treibt bitte keinen Unsinn!

„It's all fun and games until the FBI shows up!“

- The Basics of Web Hacking