



openHPI: **Web-Technologien** Privatsphäre und Sicherheit im Social Web

Prof. Dr. Christoph Meinel

Hasso-Plattner-Institut

Universität Potsdam

Das „Privacy Paradoxon“ (1/2)

- Soziale Netzwerke ermutigen Nutzer, **private Informationen preiszugeben**
 - Profilinformationen: Voller Name, Wohnort, Telefonnummer, Geburtsdatum, Arbeitgeber, Schulabschlüsse, Foto, ...
 - Interessen: Facebook „Likes“
 - Freunde und Familienmitglieder
 - Persönliche Meinungen („Timeline“)
- **Privacy Paradoxon**
 - Nutzer sozialer Netzwerke geben **bereitwillig** ihre private Informationen preis („**Selbstoffenbarung**“)
 - Dennoch haben diese Nutzer **gleiches (hohes!) Bedürfnis nach Privatsphäre**, wie diejenigen, die soziale Netzwerke ablehnen

Das „Privacy Paradoxon“ (2/2)

Gründe für Privacy Paradoxon bei Nutzung sozialer Netzwerke

- Gefühlt viele Vorteile, Nachteile nicht offensichtlich
 - Nutzer sozialer Netzwerke machen überwiegend Erfahrung, dass Preisgabe privater Informationen fast immer ohne (direkte) negative Konsequenzen bleibt
 - Veröffentlichte Details aus Privatleben führen oft zu positivem Feedback („Likes“), Zuspruch oder Anteilnahme aus der Community
- Mangelndes Problembewusstsein
 - Nutzer wissen oft nicht, was mit ihren Daten geschieht
 - Bewusstsein, dass mit Daten für „kostenlose“ Leistung bezahlt wird, ist oft nicht vorhanden



Verletzung der Privatsphäre durch Dritte

Soziale Netzwerke erlauben oft Einschränkung der Sichtbarkeit preisgegebener Informationen auf bestimmte Empfängergruppen

- Aber: Durch Interaktion berechtigter Empfänger mit geteilten Inhalten können auch weitere Personen Zugriff erlangen
 - Beispiel:
 - Nutzer X teilt Information mit seinen Freunden
 - Nutzer Y aus Freundesliste kommentiert Information
 - Nutzer Z ist mit Y bekannt aber nicht mit X
 - Nutzer Z sieht: Y hat Information von X kommentiert
 - Z erlangt so Zugriff auf Information auch von X ($X \rightarrow Y \rightarrow Z$)
- **Vorsicht:** häufig nicht einfach zu durchschauen, wer auf welche preisgegeben Information Zugriff erhält

Mögliche Nachteile durch Selbstoffenbarung

Preisgabe privater Informationen kann **handfeste Nachteile** haben

- Zugang „unerwünschter“ Personen zu privaten Informationen
 - 60% der US-Arbeitgeber recherchieren Bewerber in sozialen Netzwerken
 - 49% dieser Arbeitgeber fanden Informationen, die dazu führten, Bewerber nicht einzustellen

(Quelle, www.careerbuilder.com, Apr. 2016)
- Informationsressource für Angriffe durch → **Social Engineering**
 - Erraten von Passwörtern (→ **Passwortsicherheit**)
 - Diebstahl digitaler Identitäten
- Überwachung durch Betreiber des sozialen Netzwerks
 - Betreiber kann Internet-Bewegungsprofil des Nutzers erstellen
 - eventuelle Weitergabe des Bewegungsprofils an Dritte

Social Engineering

Grundidee: Angreifer kontaktiert Opfer, gibt sich als Techniker oder Systemadministrator aus und versucht, Zugangsdaten (Passwörter) zu erlangen

Beispiel: Angreifer erlangten Zugang auf privaten Email-Account von ehemaligem CIA-Direktor John Brennan (Identitätsdiebstahl)

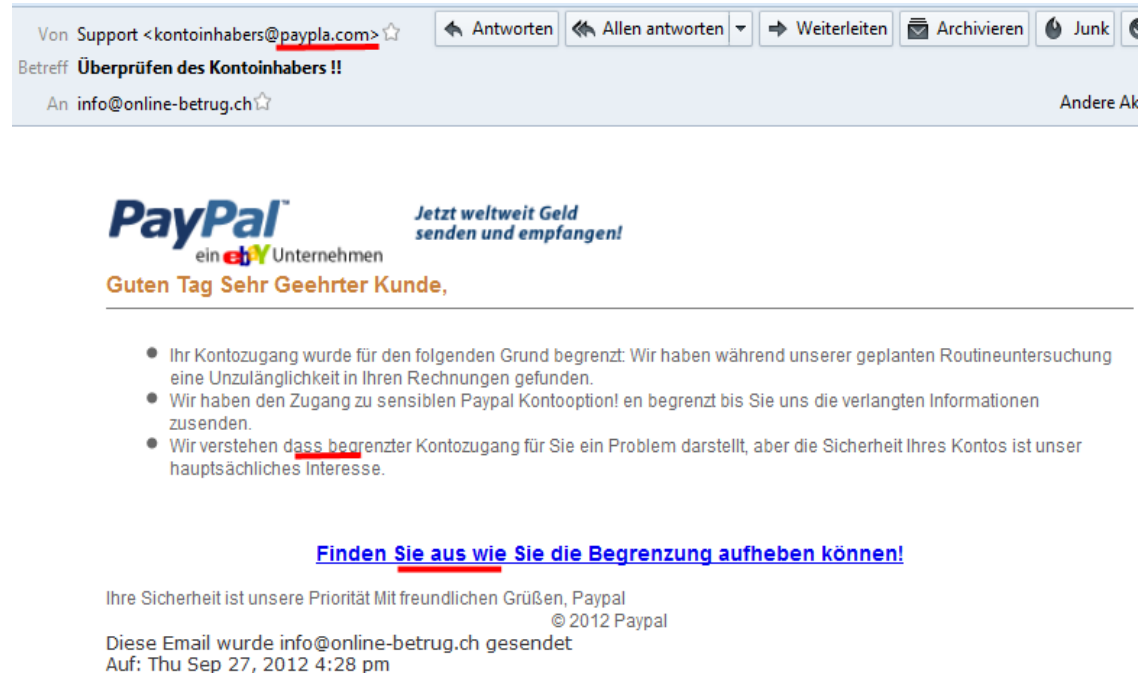
- Hacker kennt Handynummer des Opfers, stellt fest, zu welchem Provider (Verizon) dieser gehört (durch Reverse Lookup)
- Hacker gibt sich bei Verizon-Support erfolgreich als Verizon-Techniker aus, der Kundendaten benötigt – erhält z.B. letzte vier Stellen des Bankkontos
- Hacker gibt bei AOL-Support an, Passwort vergessen zu haben und kann mit Verizon-Daten die Sicherheitsfragen beantworten
- Passwort wird zurückgesetzt
- Angreifer hat 3 Tage lang Zugriff auf Email-Konto

Phishing = Password Fishing

- Technik zur betrügerischen Erlangung von sensiblen Informationen
- Typisches Vorgehen: Versand betrügerischer Emails
 - Versand mit vertrauenswürdig wirkender Absenderadresse, z.B. Bank, Unternehmen, Behörde, ...
 - Absenderadresse wird ausgewählt nach Information, die erschwindelt werden soll
 - Emailadressen können leicht gefälscht oder vorgetäuscht werden („Email Spoofing“)
 - Mit dem dadurch erlangten Vertrauen wird erwünschte Nutzerreaktion hervorgerufen
 - Herausgabe von Daten, z.B. Benutzernamen und Passwörter
 - Installation von Schadsoftware

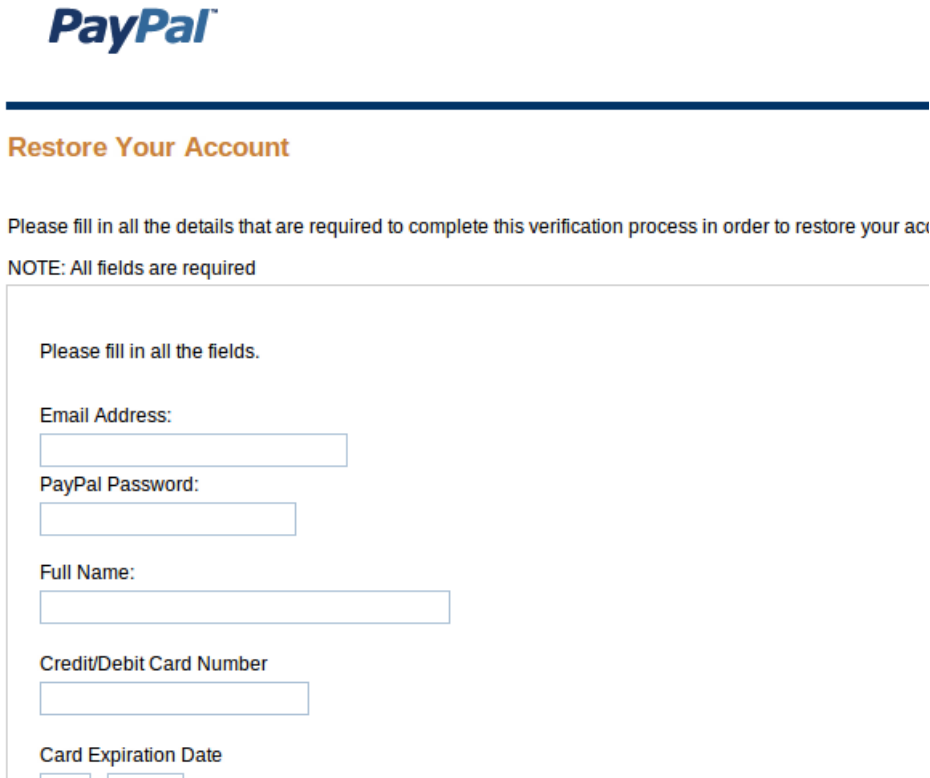
Beispiel:

- Versand einer Email mit vorgetäuschem Absender
- Nachricht stammt angeblich von Bankinstitut (Paypal) und hat entsprechend ähnliche Email-Adresse (paypla.com)
- Ziel: Empfänger soll veranlasst werden, seine Kontodetails preiszugeben, um Konto zurückzusetzen
- Phishing oft erkennbar an vielen sprachlichen Fehlern oder fehlender persönlicher Ansprache („Guten Tag Sehr Geehrter Kunde“)



- Email leitet weiter auf Webseite mit Eingabeaufforderung für Kontodaten
- Opfer wird aufgefordert, sämtliche Details über sein Konto preiszugeben
- Angreifer gelangt in Besitz der Daten

Gute Nachricht: Diese Art „herkömmlicher“ Phishing-Angriffe wird heute von vielen Internetnutzern als solcher erkannt und läuft dadurch ins Leere



The image shows a screenshot of a PayPal account restoration page. At the top is the PayPal logo. Below it is the heading "Restore Your Account". A message states: "Please fill in all the details that are required to complete this verification process in order to restore your account." Below this is a note: "NOTE: All fields are required". The form itself contains the instruction "Please fill in all the fields." followed by five input fields: "Email Address:", "PayPal Password:", "Full Name:", "Credit/Debit Card Number", and "Card Expiration Date". The "Card Expiration Date" field is split into two sub-fields for month and year.

Quelle: <http://labs.m86security.com/>

Schlechte Nachricht: Personalisierte Phishing-Angriffe, sogenanntes **Spear Phishing** ist auf dem Vormarsch

- Angreifer sammelt detaillierte Informationen über sein Opfer
- Hilfreich für vorgetäuschte Vertrauenswürdigkeit, z.B. Agieren unter Identität einer Person, die Opfer kennt und der es vertraut
- Opfer denkt, dass Email von vorgetäuschem Absender kommt, weil Nachricht Informationen enthält, die eigentlich nur dieser Absender kennen kann
- Erfolgsaussichten bei dieser Masche sind sehr hoch, aber auch für Angreifer ist Aufwand deutlich höher als beim herkömmlichen Phishing

Grundidee von Social Engineering-Attacken basiert auf Missbrauch von **Vertrauen**

- Opfer vertraut Angreifer, da dieser **vertrauliche Informationen** hat, die eigentlich nur Mitglieder eines **vertrauenswürdigen Kreises** haben
- Masche zieht genau so, wie beim Spear Phishing und Telefon-Betrug im Fall „John Brennan“

Wie erlangt Angreifer vertrauliche Informationen?

- Klassische Technik: **Dumpster Crawling** – Angreifer durchsucht Mülltonne des Opfers nach Briefen, Abrechnungen, Kontoauszügen, ...
- Informationstechnischer Ansatz: Hacken des Computers eines Opfers
- **Viel einfacher:** Einsammeln der freiwillig preisgegebenen Informationen aus den sozialen Netzwerken

Passwortsicherheit (1/2)

Auch **Angriffe auf Passwörter** können durch persönliche Informationen aus Social-Media-Profilen erleichtert werden

- Verbreitet: **Password Guessing** – Erraten von Passwörtern
 - Angreifer probiert wahrscheinliche Passwörter zu einem Account durch
 - Angriffstools arbeiten mit Wortlisten und Wörterbüchern
- **Problem:** Nutzer wählen gerne (immer gleiche/ähnliche) Passwörter, die sie sich leicht merken können, z.B.
 - Begriffe oder Daten aus persönlichem Umfeld
 - Geburtsdaten, Namen, Begriffe im Zusammenhang mit Interessen (Lieblings-Romanfigur, -Band, -Filmtitel, ...)
 - Persönlich Informationen der Opfer helfen Angreifer, kann z.B. **Wortlisten personalisieren** → Trefferwahrscheinlichkeit steigt

Passwortsicherheit (2/2)

Beispiel:

- Nutzer gibt auf Facebook an, Fan von „Star Trek“ zu sein
- Angreifer kann spezielle (fertig erhältliche) Wortliste mit allen Begriffen aus Star Trek-Universum verwenden
- Ähnliche Wortlisten auch verfügbar z.B. für „Herr der Ringe“, „Game of Thrones“, Monty Python-Filme und -Serien, ...

Informationen aus Social Networks nicht nur hilfreich beim Knacken (Raten) von Passwörtern, sondern insbesondere auch für sogenannte **Sicherheitsfragen** zum Zurücksetzen von Passwörtern, z.B.

- Mädchenname der Mutter
- Erstes Automodell
- Straße der ersten Wohnung
- Teile von Kreditkarten- oder Kontonummern (siehe John Brennan)