# Betrugsschutz beim Online-Banking
## Nutzeraspekte und Mensch-Maschine-Interaktion

Christine Paulisch
Dr.-Ing. Ulrike Schmuntzsch
Prof. Dr.-Ing. Matthias Rötting

**Technische Universität Berlin**
**Institut für Psychologie und Arbeitswissenschaft**
**Fachgebiet Mensch-Maschine-Systeme**

**www.mms.tu-berlin.de**

# Agenda

- **Projektübersicht**
- **Vorstellung der Ergebnisse**
  - **Teil 1:** Nutzerseitige Ist-Analyse zu Betrugsfällen und Transaktionsverfahren
  - **Teil 2:** Schnittstellengestaltung zur nutzerseitigen Missbrauchsvermeidung
- **Fazit**

# Projektübersicht

## Teil 1: Analyse

- **Ist-Analyse zu Betrugsfällen**
  - Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern
- **Risikoanalyse bestehender Transaktionsverfahren**
  - Mensch-Maschine-Interaktion bei mTAN und sm@rtTAN-Verfahren

## Teil 2: Schnittstellengestaltung

- **Nutzung von sicheren digitalen Identitäten**
  - Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises
- **Nutzerseitige Missbrauchsvermeidung**
  - Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

# Agenda

- **Projektübersicht**
- **Vorstellung der Ergebnisse**
  - **Teil 1:** Nutzerseitige Ist-Analyse zu Betrugsfällen und Transaktionsverfahren
  - **Teil 2:** Schnittstellengestaltung zur nutzerseitigen Missbrauchsvermeidung
- **Fazit**

# Projektübersicht

## Teil 1: Analyse

- **Ist-Analyse zu Betrugsfällen**
  - Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern
- **Risikoanalyse bestehender Transaktionsverfahren**
  - Mensch-Maschine-Interaktion bei mTAN und sm@rtTAN-Verfahren

## Teil 2: Schnittstellengestaltung

- **Nutzung von sicheren digitalen Identitäten**
  - Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises
- **Nutzerseitige Missbrauchsvermeidung**
  - Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

# Ist-Analyse zu Betrugsfällen Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern

- **5 Fälle randomisiert mit Bildern dargeboten**:
  1. Phishing
  2. Falsches Zertifikat
  3. Manipulierte IBAN bei mTAN-Verfahren
  4. Manipulierte Login-Seite
  5. Normale Startseite

- **Instruktion**:
  - Bilder mit einem oder mehreren Merkmalen nach Sicherheits- und Angriffsmerkmalen bewerten und begründen

- **Fazit**:

<u>Positive Aspekte:</u>
- Mehrheit der Probanden misstraut Phishing-Angriff per E-Mail
- Mehrheit zeigt Skepsis gegenüber Mobilnummer-/TAN-Abfrage bei Login

<u>Negative Aspekte:</u>
- 28% verwenden TAN ohne Überprüfung von Betrag oder IBAN
- 40% achten auf https-Verschlüsselung
- 76% würden Sicherheitsausnahmeregel für Zertifikat bestätigen

# Projektübersicht

## Teil 1: Analyse

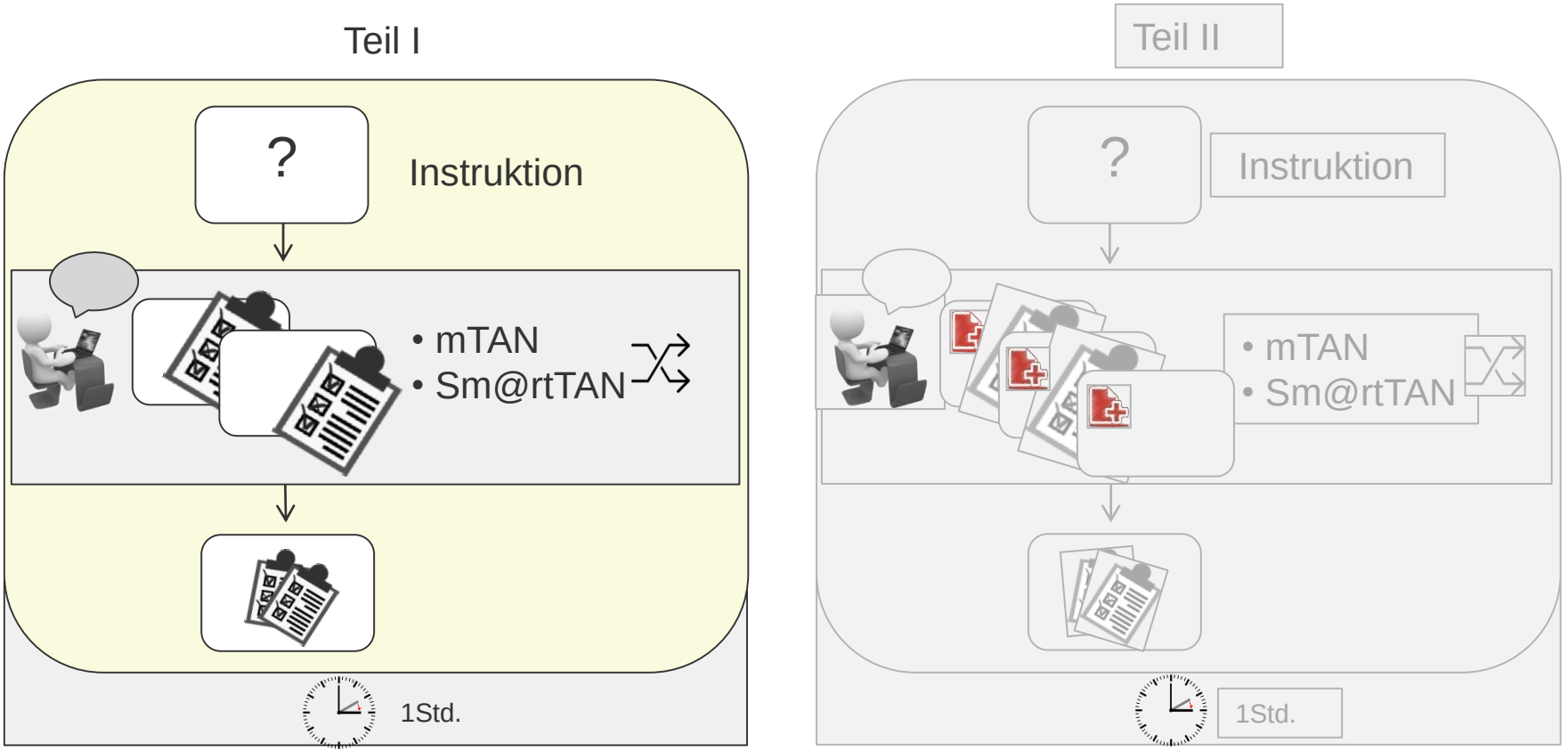
- **Ist-Analyse zu Betrugsfällen**
  - Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern
- **Risikoanalyse bestehender Transaktionsverfahren**
  - Mensch-Maschine-Interaktion bei mTAN und sm@rtTAN-Verfahren

## Teil 2: Schnittstellengestaltung

- **Nutzung von sicheren digitalen Identitäten**
  - Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises
- **Nutzerseitige Missbrauchsvermeidung**
  - Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

# Risikoanalyse bestehender Transaktionsverfahren Mensch-Maschine-Interaktion bei mTAN und Sm@rtTAN

**Nutzerstudie I:** Akzeptanz und Gebrauchstauglichkeit der Verfahren
**Nutzerstudie II**: Erhebung der Performanz und der Wahrnehmbarkeit sicherheitskritischer Situationen



# Kernergebnisse Nutzerstudie I

Usability der gewählten Transaktionsverfahren
auf Grundlage der Internationalen Norm DIN EN ISO 9241-110-S

| **Bewertungsskala** | **Mittelwerte** chipTAN / mTAN | **SD** chipTAN / mTAN | **Differenz** chipTAN - mTAN | **Sig.** |
|---|---|---|---|---|
| **Aufgabenangemessenheit** | **2,46 / 1,62** | **0,66 / 0,64** | **0,84** | **.000** |
| **Selbstbeschreibungsfähigkeit** | **2,81 / 2,25** | **0,82 / 0,69** | **0,56** | **.007** |
| Erwartungskonformität | 2,84 / 2,53 | 0,69 / 0,79 | 0,31 | .150 |
| **Lernförderlichkeit** | **2,20 / 1,53** | **0,73 / 0,71** | **0,67** | **.002** |
| **Steuerbarkeit** | **2,70 / 1,74** | **1,05 / 0,75** | **0,96** | **.000** |
| Fehlertoleranz | 2,44 / 2,16 | 1,08 / 1,03 | 0,28 | .258 |

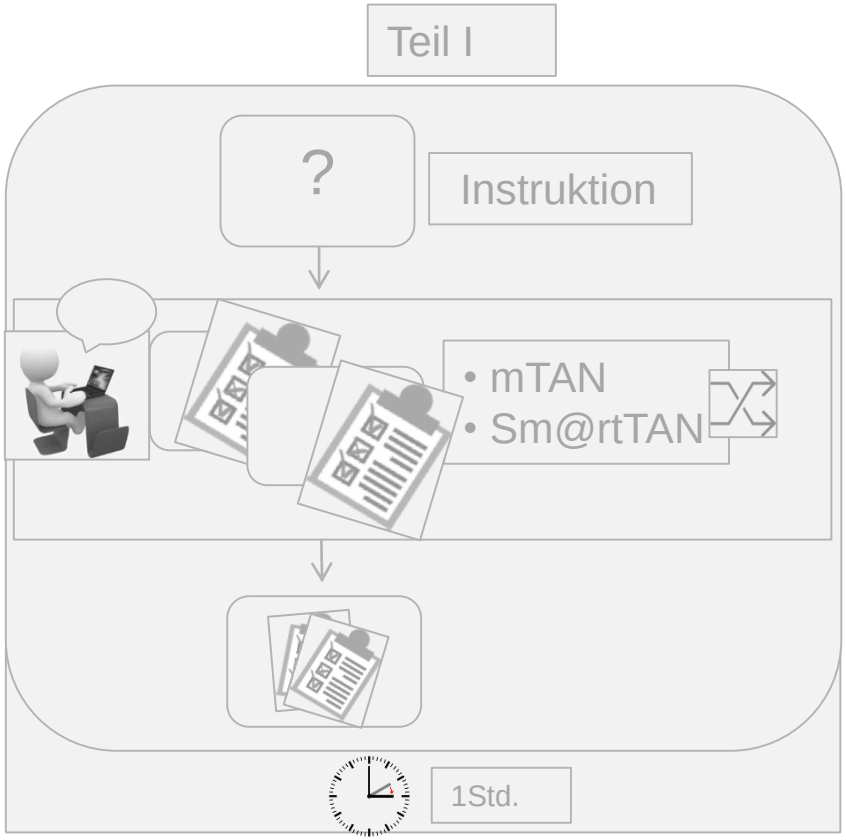
1 = „trifft voll zu" bis 5 = „trifft gar nicht zu"

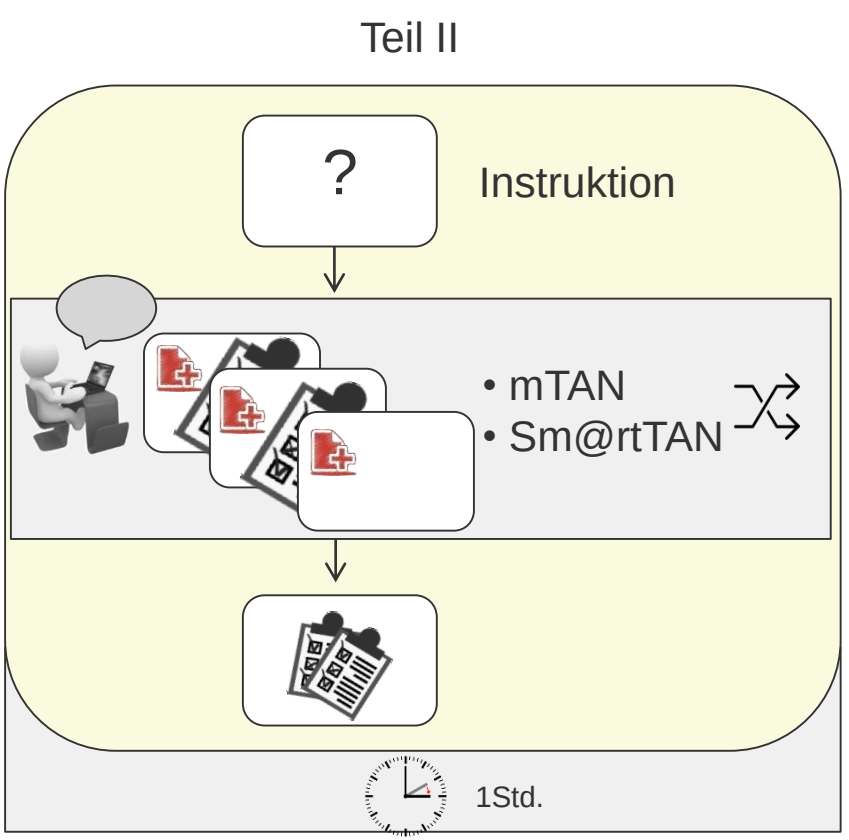
**Fazit:** Sign. positivere Bewertung des mTAN-Verfahrens hinsichtlich der Gebrauchstauglichkeit und Nutzerfreundlichkeit

**Grund:** Hohe Rate an **fehlgeschlagener Übermittlung** der Transaktionsdaten bei TAN-Generator → **Aufmerksamkeit vollkommen beansprucht → „Tunnelblick"** nach Gelingen und rasche Beendigung des Vorgangs angestrebt

# Risikoanalyse bestehender Transaktionsverfahren Mensch-Maschine-Interaktion bei mTAN und Sm@rtTAN

**Nutzerstudie I:** Akzeptanz und Gebrauchstauglichkeit der Verfahren
**Nutzerstudie II**: Erhebung der Performanz und der Wahrnehmbarkeit sicherheitskritischer Situationen



# Kernergebnisse Nutzerstudie II

**1. Betrugsszenario: Aufforderung zur Rücküberweisung**

- **44% erkennen** den Angriff **nicht**, aber nur **12% überweisen** den Betrag zurück.
- **Gründe:** Probanden erkennen die unterschiedlichen Empfänger oder empfinden die Sprache der Aufforderung als „bank-untypisch".
- **Social Engineering** hat jedoch Einfluss: Druck durch Kontosperrung bewegt zur Rücküberweisung.

**2. Betrugsszenario: Aufforderung zur Eingabe der Mobilfunknummer**

- **68%** geben Mobilfunknummer ein; **44%** äußern dabei keinen Zweifel an der Legitimität der Abfrage.
- **Gründe:** Generell kein Problem damit, die Mobilfunknummer preiszugeben; eher sicheres Gefühl - wer sollte sonst etwas mit der Nummer machen können? Nur TAN-Eingabe wird vorab als gefährlich eingestuft.

# Kernergebnisse Nutzerstudie II

**3. Betrugsszenario: Änderung der Transaktionsdaten im Hintergrund**

- **65%** gleichen nicht die **IBAN** in SMS / TAN-Generator mit den einzugebenden Daten ab und **70%** überprüfen auch nicht den zu überweisenden **Betrag**.
- **71%** erkennen den Betrug daher nicht oder erst nach der Transaktion.
- **Gefährliche Denkweise** bei Erkennen des Betrugs: Abbrechen => erneut einloggen => Daten eingeben. Sollte erneut ein Fehler auftreten, dann dem Gerät vertrauen.

**Generell über alle drei Szenarien: Überprüfen der Transaktionsdaten**

- **Durchschnittlich** gleichen **56%** der Probanden die **IBAN** in SMS / TAN-Generator nicht mit den einzugebenden Daten ab und weitere **44%** überprüfen nicht den **Betrag** in beiden Anzeigen.

# Agenda

- **Projektübersicht**
- **Vorstellung der Ergebnisse**
  - **Teil 1:** Nutzerseitige Ist-Analyse zu Betrugsfällen und Transaktionsverfahren
  - **Teil 2:** Schnittstellengestaltung zur nutzerseitigen Missbrauchsvermeidung
- **Fazit**

# Projektübersicht

## Teil 1: Analyse

- **Ist-Analyse zu Betrugsfällen**
  - Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern
- **Risikoanalyse bestehender Transaktionsverfahren**
  - Mensch-Maschine-Interaktion bei mTAN und sm@rtTAN-Verfahren

## Teil 2: Schnittstellengestaltung

- **Nutzung von sicheren digitalen Identitäten**
  - Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises
- **Nutzerseitige Missbrauchsvermeidung**
  - Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

# Nutzung von sicheren digitalen Identitäten Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises

- **Kernergebnisse der Nutzerstudie zum nPA**
  - Mittelmäßige Bewertung der Gebrauchstauglichkeit
  - Einwände wegen Sicherheitsbedenken, höherem Aufwand und unklarem Nutzen
  - Skepsis gegenüber zusätzlichem Gerät (Anschaffungskosten und Mobilitätseinschränkung)


- **Fazit**
  - Grundlegende Skepsis gegenüber dem Einsatz des nPA beim Online-Banking
  - Fokussierung auf Information zur Einstellungs- und Verhaltensänderung
  - Verbesserung der Gebrauchstauglichkeit

# Projektübersicht

## Teil 1: Analyse

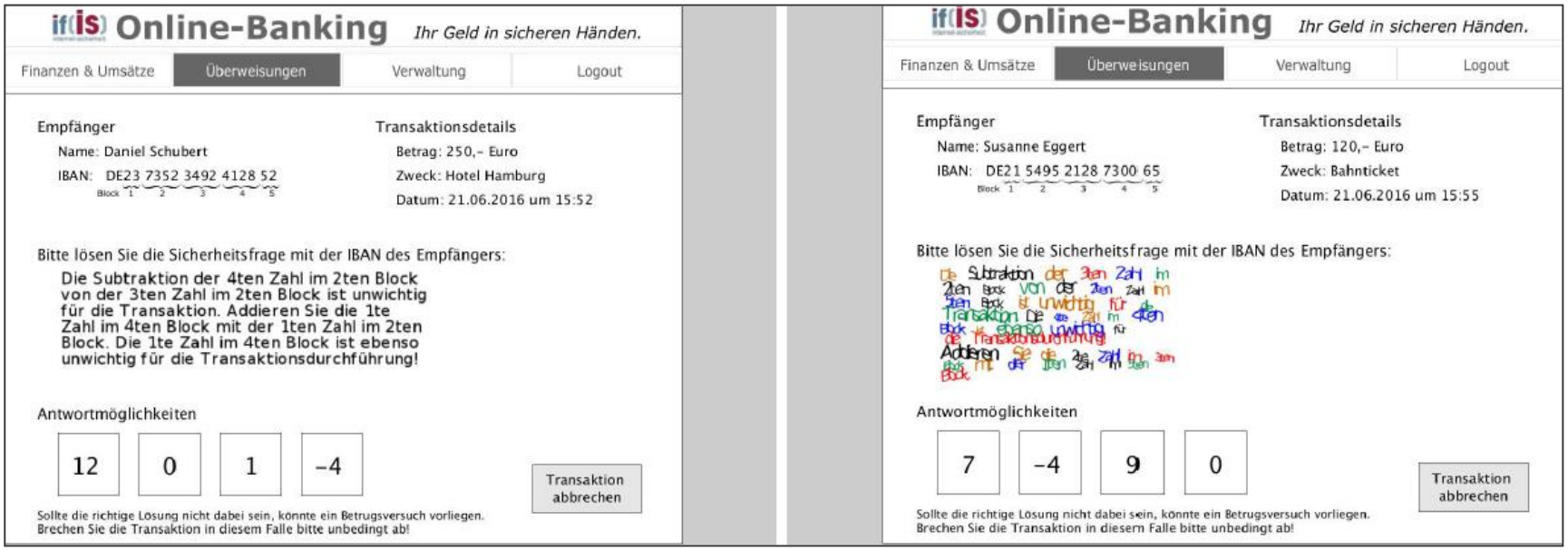
- **Ist-Analyse zu Betrugsfällen**
  - Mensch-Maschine-Interaktion bei Phishing-Angriffen und Trojanern
- **Risikoanalyse bestehender Transaktionsverfahren**
  - Mensch-Maschine-Interaktion bei mTAN und sm@rtTAN-Verfahren

## Teil 2: Schnittstellengestaltung

- **Nutzung von sicheren digitalen Identitäten**
  - Mensch-Maschine-Interaktion bei der Nutzung des elektronischen Personalausweises
- **Nutzerseitige Missbrauchsvermeidung**
  - Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

# Nutzerseitige Missbrauchsvermeidung
# Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

## Nutzerstudie 1 zu den CAPTCHAs

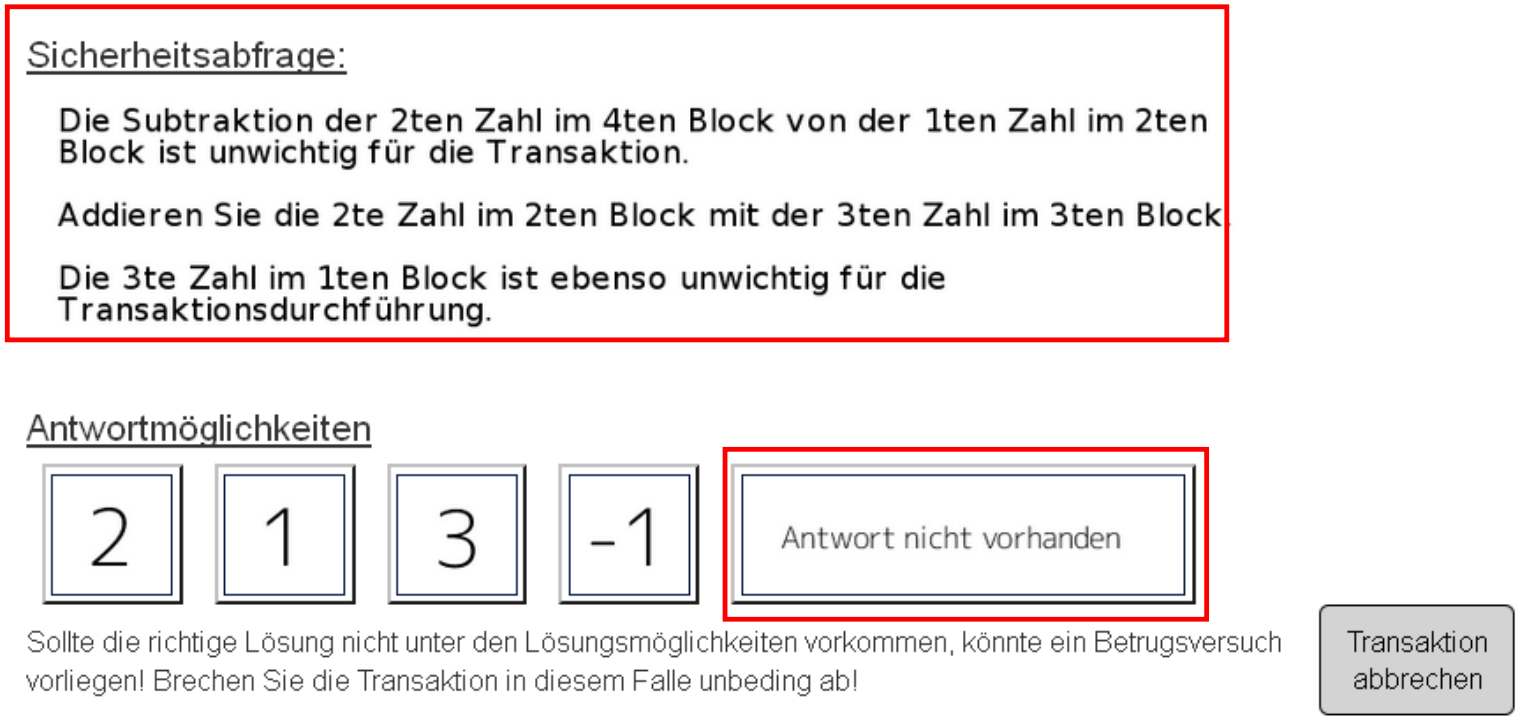



## Kernergebnisse von Nutzerstudie 1 zu den CAPTCHAs

- Klare Präferenz für die schwarzen CAPTCHAs
- 73% der Befragten würden CAPTCHAs nutzen
- Überarbeitung der Übersichtlichkeit der CAPTCHAs und Einfügen eines „Antwort-nicht-vorhanden"-Buttons

# Nutzerseitige Missbrauchsvermeidung
# Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

- **Nutzerstudie 2 zu den CAPTCHAs**
  - Vergleich der alten schwarzen CAPTCHA-Variante gegen eine überarbeitete Version



# Nutzerseitige Missbrauchsvermeidung
# Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

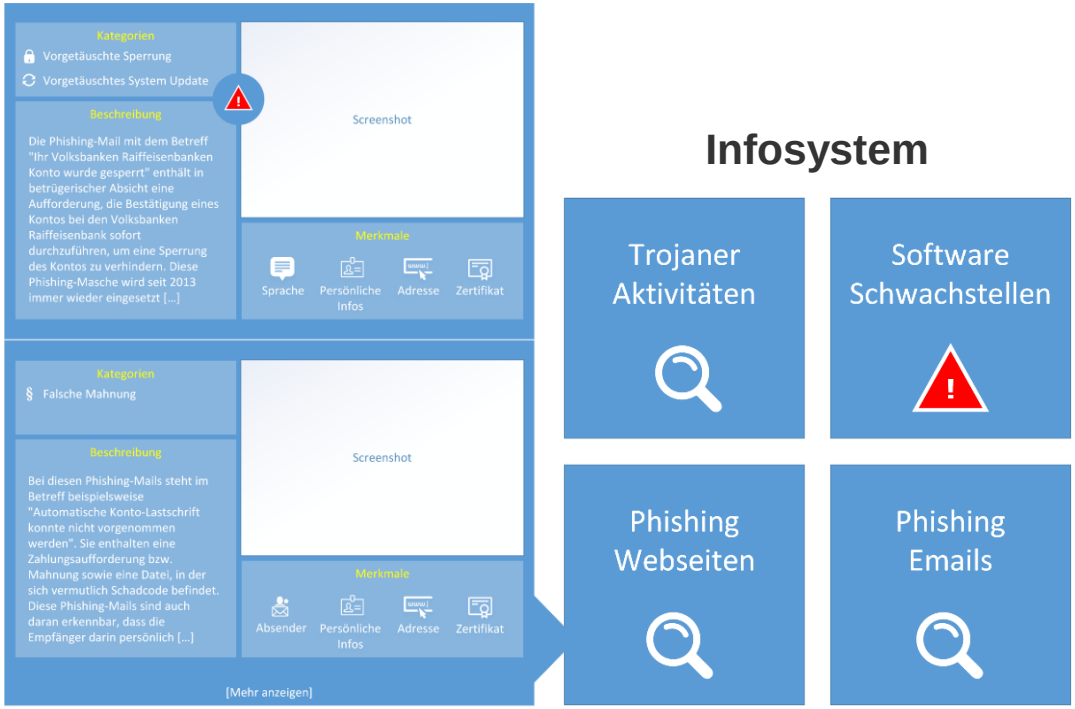
- **Kernergebnisse von Nutzerstudie 2 zu den CAPTCHAs**
  - Längere Bearbeitungsdauer und höhere mentale Beanspruchung bei der alten CAPTCHA-Variante
  - Klare Präferenz für die überarbeitete schwarze CAPTCHA-Variante wegen der leichteren Bearbeitung
  - 60% der Befragten würden CAPTCHAs nutzen, wenn diese die Sicherheit erhöhen

- **Wünsche**
  - Wunsch nach einfacheren CAPTCHAs ohne Heraussuchen und Zusammenrechnen von Zahlen
  - Als Alternativen wurden Bilder-CAPTCHAs genannt

# Nutzerseitige Missbrauchsvermeidung
# Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

## Fokusgruppendiskussionen zu Alertsystemen

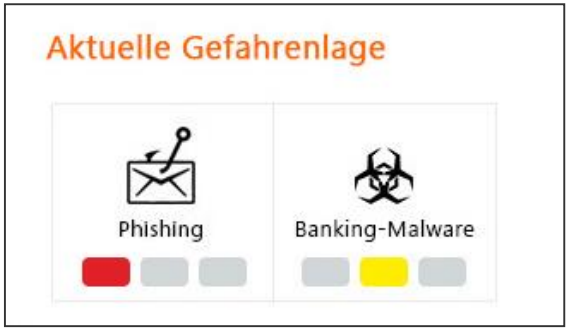
- 3 Fokusgruppendiskussionen mit insgesamt 15 Personen zum Vergleich von 3 Alertsystem-Varianten



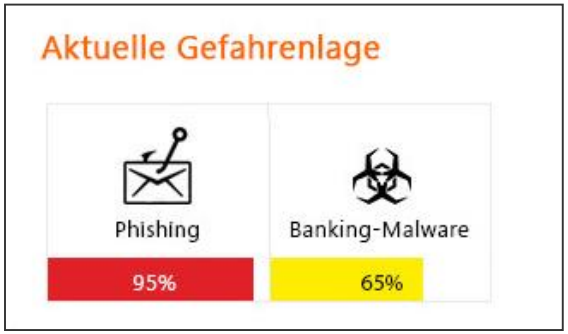

**Infosystem**




**Ampelsystem**




**Balkensystem**



# Nutzerseitige Missbrauchsvermeidung
# Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

- **Kernergebnisse der Fokusgruppendiskussionen zu Alertsystemen**
  - **Grundsätzlich positive Haltung** gegenüber Alertsystemen → Erzeugen von Risikobewusstsein und Information über Gefahren
  - Wunsch nach Alertsystem **direkt auf der Startseite** der Bank
  - **Ampel- und Balkensysteme**:
    - Erzeugen ggf. eine „falsche" Sicherheit beim „grün"-Status
    - Werfen Fragen auf bzgl. des geforderten sicheren Nutzerverhaltens („was soll ich als Nutzer jetzt bei „ROT" oder „GELB" machen bzw. kann ich überhaupt etwas machen?)
  - **Eindeutige Präferenz für das Infosystem:**
    - Hervorgehobener Informationscharakter, insbes. durch Screenshots
    - Detailbeschreibungen zu Gefahren
    - Wunsch nach genauen Handlungsanweisungen in der Detailbeschreibung

# Agenda

- **Projektübersicht**
- **Vorstellung der Ergebnisse**
  - **Teil 1:** Nutzerseitige Ist-Analyse zu Betrugsfällen und Transaktionsverfahren
  - **Teil 2:** Schnittstellengestaltung zur nutzerseitigen Missbrauchsvermeidung
- **Fazit**

# Fazit

**Welche Erwartungen und Wünsche zum Thema Sicherheit beim Online-Banking werden an die Bank gestellt?**

- Aktuelle Betrugsfälle und Schutzmaßnahmen publizieren
- Genaue Anleitung wie vorzugehen ist bei vermeintlichem Betrug

**Welche Aspekte beim Online-Banking werden als besonders kritisch betrachtet? Was ist der Grund dafür?**

- Länge der IBAN: Hervorhebung der Einzelkomponenten
- „Echtheit" der Aufforderungen oft unklar => Verhaltensanweisungen gewünscht
- Zeitdruck führt zu Vernachlässigung der Überprüfung

**Welche Hilfestellungen werden von den Probanden genannt, die bei der Identifizierung von Betrugsfällen unterstützen könnten?**

- Alertsysteme, welche über aktuelle Angriffe informieren
- Anschaulich gestaltete Lernplattform mit Betrugsbeispielen
- Pop-Up nach Übermittlung der Transaktionsdaten als Erinnerung zur Überprüfung der Bankdaten

Deutschland
Land der Ideen
Ausgewählter Ort 2010

# Vielen Dank für Ihre Aufmerksamkeit!

Technische Universität Berlin
Institut für Psychologie und Arbeitswissenschaft
Fachgebiet Mensch-Maschine-Systeme

www.mms.tu-berlin.de