

# Social Engineering

**Marius Hamborgstrøm**

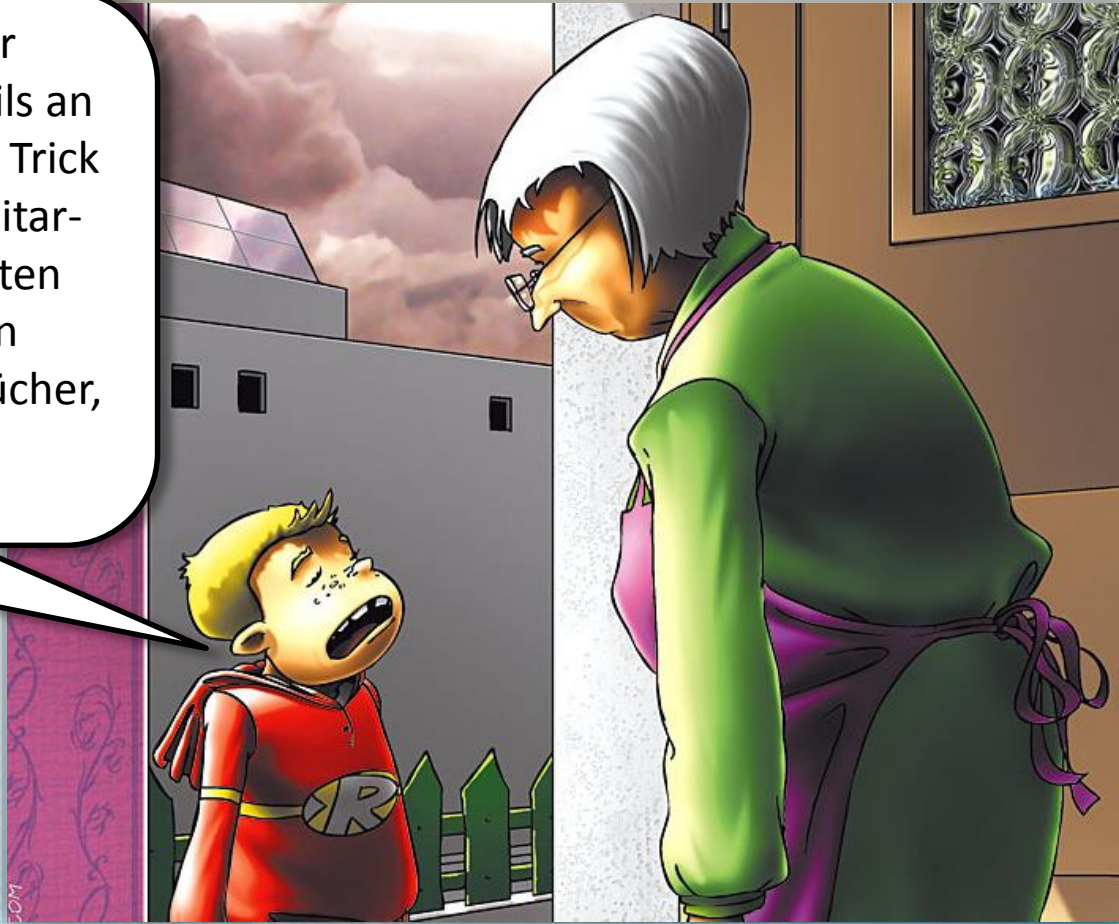
Security Consultant

Certified Ethical Hacker CEH, zert. IT-Sicherheitsmanager, ITIL Foundation

[hamborgstroem@goSecurity.ch](mailto:hamborgstroem@goSecurity.ch)

# Social Engineering

Grüss Gott. Ich komme von der UBS AG. Immer wieder versuchen Gauner über fingierte E-Mails an Kontoinformationen zu gelangen. Der neueste Trick ist, dass Leute, die offensichtlich keine Bankmitarbeiter sind, von Tür zu Tür gehen, um Kontodaten auszuspähen. Deshalb mussten wir ihre Konten umstellen. Geben Sie mir bitte alle Ihre Sparbücher, damit wir diese kostenlos für Sie aktualisieren können.



Quelle: <http://ritsch-renn.com/>

# Social Engineering

- Was ist Social Engineering?
  - Menschen manipulieren, um an Informationen zu kommen

# Social Engineering

- Was macht Social Engineering so erfolgreich?
  - Der Mensch
    - Gutgläubigkeit
    - Hilfsbereitschaft
    - Respekt vor Autoritäten
  - Software und Hardware ist als Schutz unbrauchbar

# Social Engineering

- Wie sieht der Betrüger aus?



# Informationsbeschaffung

- Welche Informationen benötigt ein Angreifer
  - Telefonlisten
  - Organigramme
  - Dienstleister
  - Gebäude- und Geländepläne
  - Netzpläne, Computernamen, Netzwerkadressen
  - Schriftverkehr
  - ...
- So viele Informationen wie möglich!

# Informationsbeschaffung

- Wie werden diese beschafft?

# Wie werden diese beschafft?

## Telefon



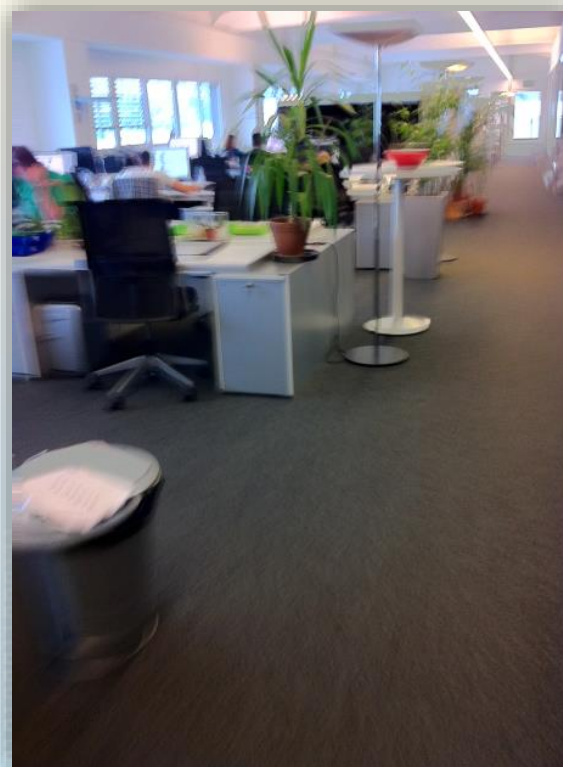
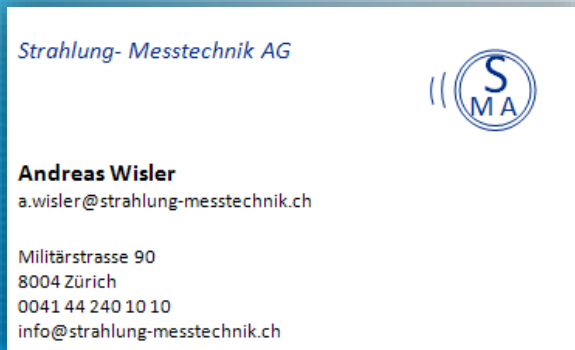


# Wie werden diese beschafft? Vor Ort



# Wie werden diese beschafft? Vor Ort

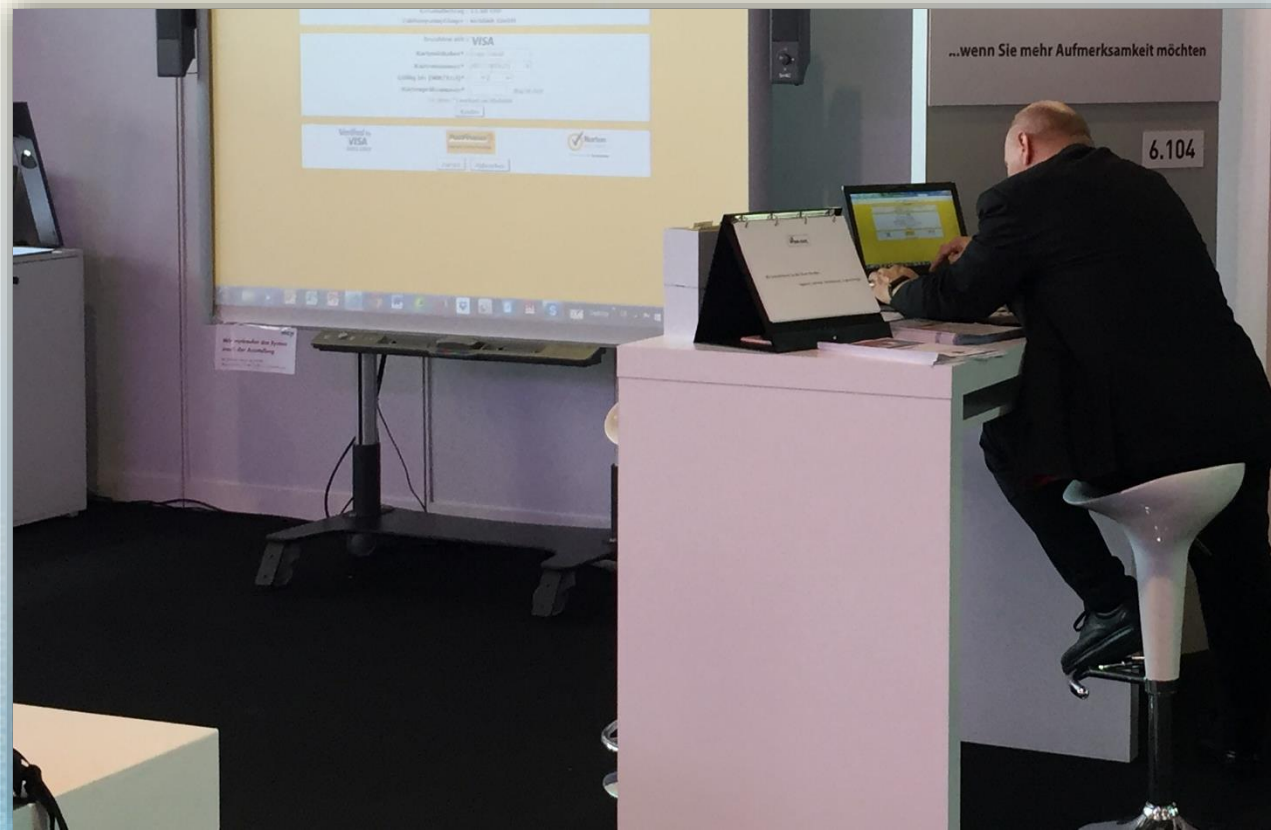
- Kontrolle des Arbeitsplatzes, «Dongle»



# Wie werden diese beschafft? Öffentlichkeit



# Wie werden diese beschafft? Öffentlichkeit



# Wie werden diese beschafft? Öffentlichkeit

Personen / Info zu Name - Personen-Suchmaschine yasni.de - Microsoft Internet Explorer bereitgestellt von GO OUT:  
http://www.yasni.de/

Favoriten | Vorgeschlagene Sites | Web Slice-Katalog | Links anpassen

Personen / Info zu Name - Personen-Suchmaschi...

**yasni.de** Person suchen | Person suchen

**Was weiss da**  
Vorname Nachname

Adam Courchaine Alida Kurras Andrea B  
Annina Ucatis Anja Müller Beyhan Günes  
Dieter Bohlen Fausta Giordano Jessica Ginkel  
Ninja Wagner Sa

**yasni VIPs** Neu > Ber

S. Kanig...  
seit 25.03.2009

P. We  
Unter

**facebook** Angemeldet bleiben | Passwort vergessen? | E-Mail | Passwort | Anmelden

Registrieren | Registriere dich für Facebook, um mit [redacted] in Verbindung zu treten.

Falscher [redacted]? Suche nach anderen Personen: [Suche]

It's not over until it's over.

[redacted] als Freundin hinzufügen | [redacted] eine Nachricht senden | [redacted] Freunde anzeigen

Hier sind einige von [redacted] Freunden:

[redacted] ist ein Fan von:

- Prominenter / Bekannte Person**  
Roger Federer  
Bud Spencer  
Jack Bauer  
Sylvester Stallone  
Pippa
- Gemeinnützige Organisationen**  
Jeder Fan bedeutet eine Kerze für die Opfer in Haiti. Mach mit!  
Für jeden Fan spende ich einen Rappen an die Aktion "JEDER RAPPEN ZÄHLT"
- Geschäfte**  
BASEL  
THE LANE -  
LANDLORDZLANE
- Musik**  
Kann dieses Brezel mehr Fans als TOKIO HOTEL haben?

**XING** Mitglieder | UBS

Start | Suche | Nachrichten | Kontakte | Gruppen | Events | Jobs | Unternehmen

**Suchergebnisse**

Stichwörter: UBS | Suchen | Erweiterte Suche

Ergebnisse 1-10 von 300  
<< Zurück | Weiter >> | 1 | 2 | 3 | 4 | 5 | ... | 30

- [redacted] Client Advisor, UBS AG, Zürich  
UBS AG  
Treffer in: Firmen (zuvor), Firma (jetzt), Positionen (zuvor), Position (jetzt), Sprache
- [redacted] Global Head Operations Product Capabilities Mgmt.  
UBS AG, UBS Global Asset Management  
Treffer in: Firma (jetzt), Firmen (zuvor), Firma (jetzt), Sprache
- [redacted] General Counsel UBS Investment Fund Services  
UBS AG  
Treffer in: Firmen (zuvor), Firma (jetzt), Position (jetzt), Sprache

# Wie werden diese beschafft? Dumpster Diving



# Arten von Social Engineering

- Computer Based
- Human Based
- Reverse Social Engineering

# Phishing

- Was ist Phishing?
- Arten von Phishing
  - Massen Phishing
  - Spear Phishing

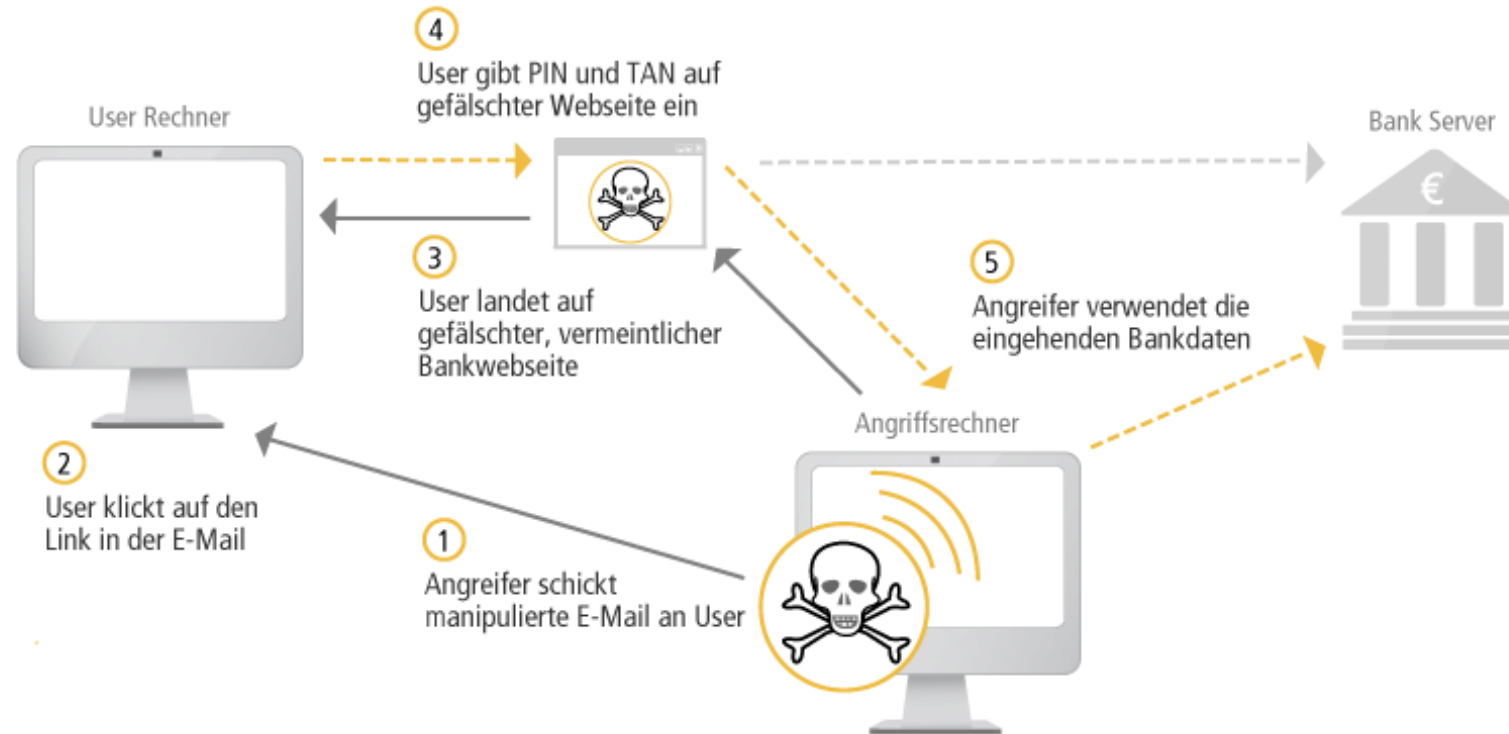


# Phishing – aktuelle Lage

- MELANI – Halbjahresbericht 2014/1
  - Im ersten Halbjahr 2014 gab es erneut auffallend viele Phishing-Versuche. Neben den eher international anmutenden E-Mails wurden auch einige auf die Schweiz zugeschnittene Phishing-E-Mails beobachtet. Die Kriminellen hatten es dabei vor allem auf die Kreditkartendaten der Opfer abgesehen.
  - Verwendete Firmen: Swisscom, Läderach, Bundesamt für Energie, PayPal

# Phishing - Funktionsweise

## PHISHING



Quelle: [www.wikibanking.net](http://www.wikibanking.net)

# DEMO Phishing

# Phishing – Ergebnisse aus Audits

Hallo Max

Die Geschäftsleitung der MUSTER AG ist überzeugt, alles für die optimale Sicherheit unserer Kunden zu unternehmen. Daher ist es enorm wichtig, dass auch unsere Mitarbeiter alles unternehmen, damit dieser Schutz hoch gehalten werden kann.

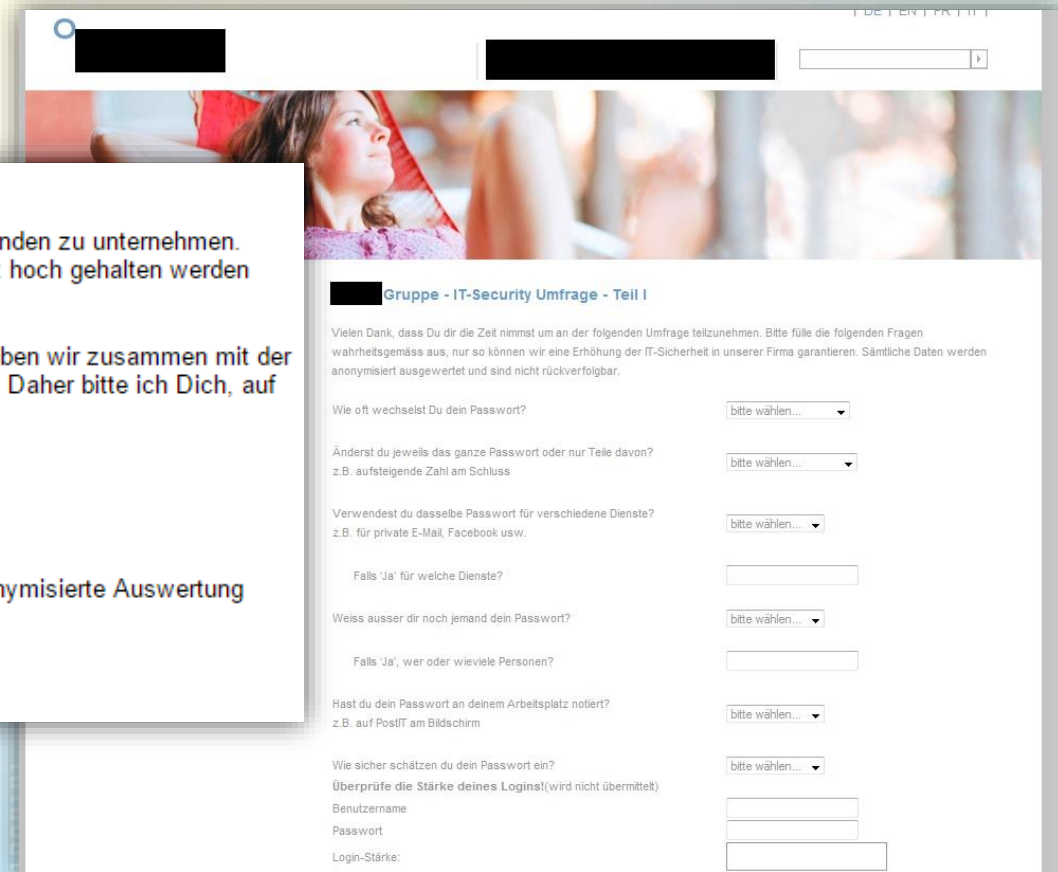
Hier sind wir auf Deine Mitarbeit angewiesen! Um die Sicherheit unserer Systeme zu erhöhen, haben wir zusammen mit der Firma TOPSECURE einen Fragebogen entworfen, um den Umgang mit Passwörtern zu erfahren. Daher bitte ich Dich, auf der folgenden Seite den kurzen Fragebogen auszufüllen:

[Link zur Umfrage](#)

Unter allen Teilnehmern werden 3 USB Sticks (64 GB) verlost.

**HINWEIS:** Wir garantieren, dass alle Angaben vertraulich behandelt werden und wir nur eine anonymisierte Auswertung erhalten werden!

Danke für Deine Hilfe.  
Gruss, Chris



TOPSECURE

Gruppe - IT-Security Umfrage - Teil I

Vielen Dank, dass Du dir die Zeit nimmst um an der folgenden Umfrage teilzunehmen. Bitte fülle die folgenden Fragen wahrheitsgemäss aus, nur so können wir eine Erhöhung der IT-Sicherheit in unserer Firma garantieren. Sämtliche Daten werden anonymisiert ausgewertet und sind nicht rückverfolgbar.

Wie oft wechselst Du dein Passwort?

Änderst du jeweils das ganze Passwort oder nur Teile davon?  
z.B. aufsteigende Zahl am Schluss

Verwendest du dasselbe Passwort für verschiedene Dienste?  
z.B. für private E-Mail, Facebook usw.

Falls 'Ja' für welche Dienste?

Weiss ausser dir noch jemand dein Passwort?

Falls 'Ja', wer oder wieviele Personen?

Hast du dein Passwort an deinem Arbeitsplatz notiert?  
z.B. auf PostIT am Bildschirm

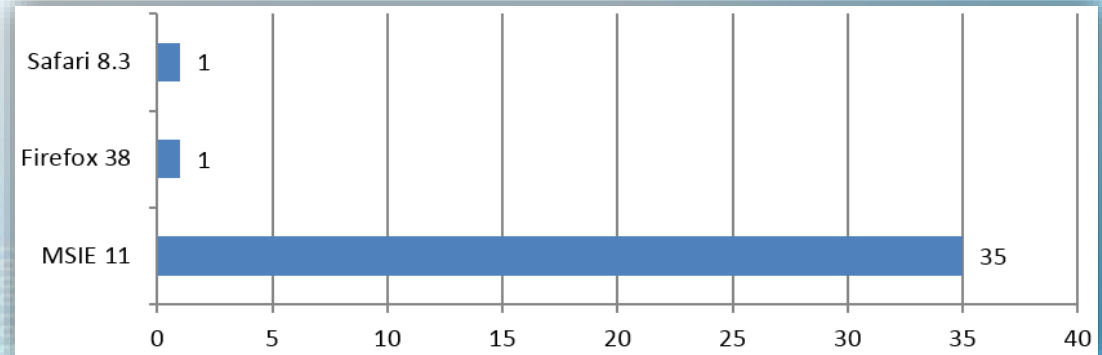
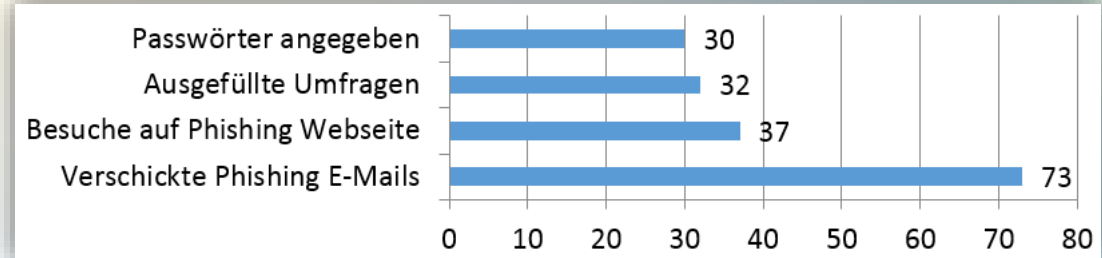
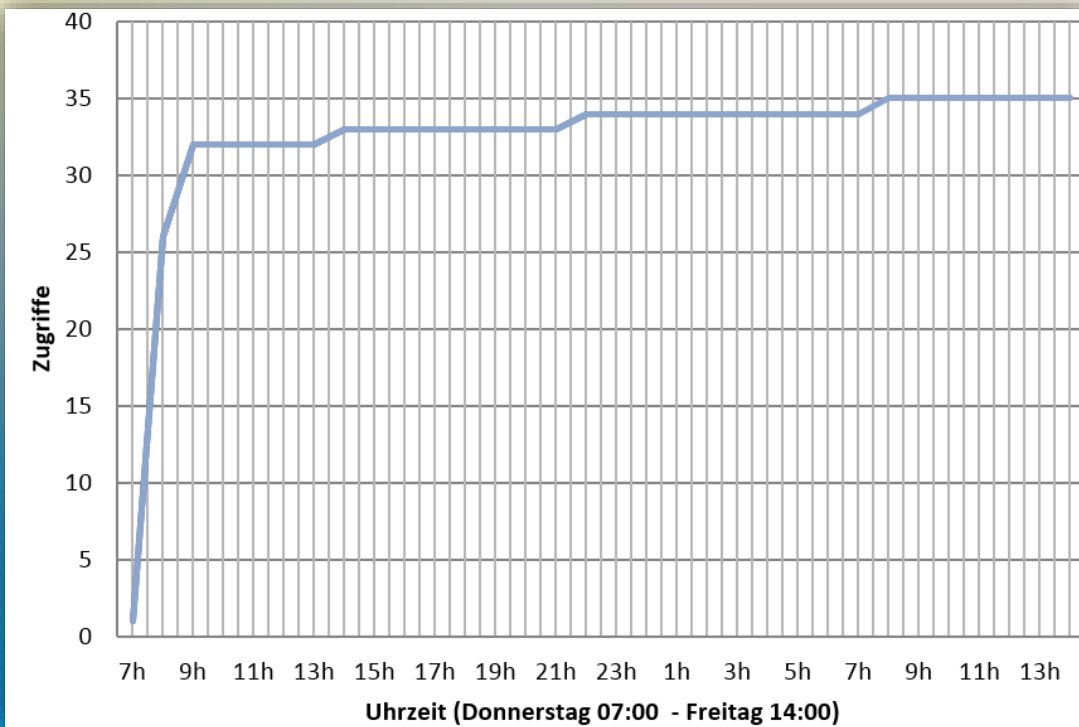
Wie sicher schätzen du dein Passwort ein?  
Überprüfe die Stärke deines Logins!(wird nicht übermittelt)

Benutzername

Passwort

Login-Stärke:

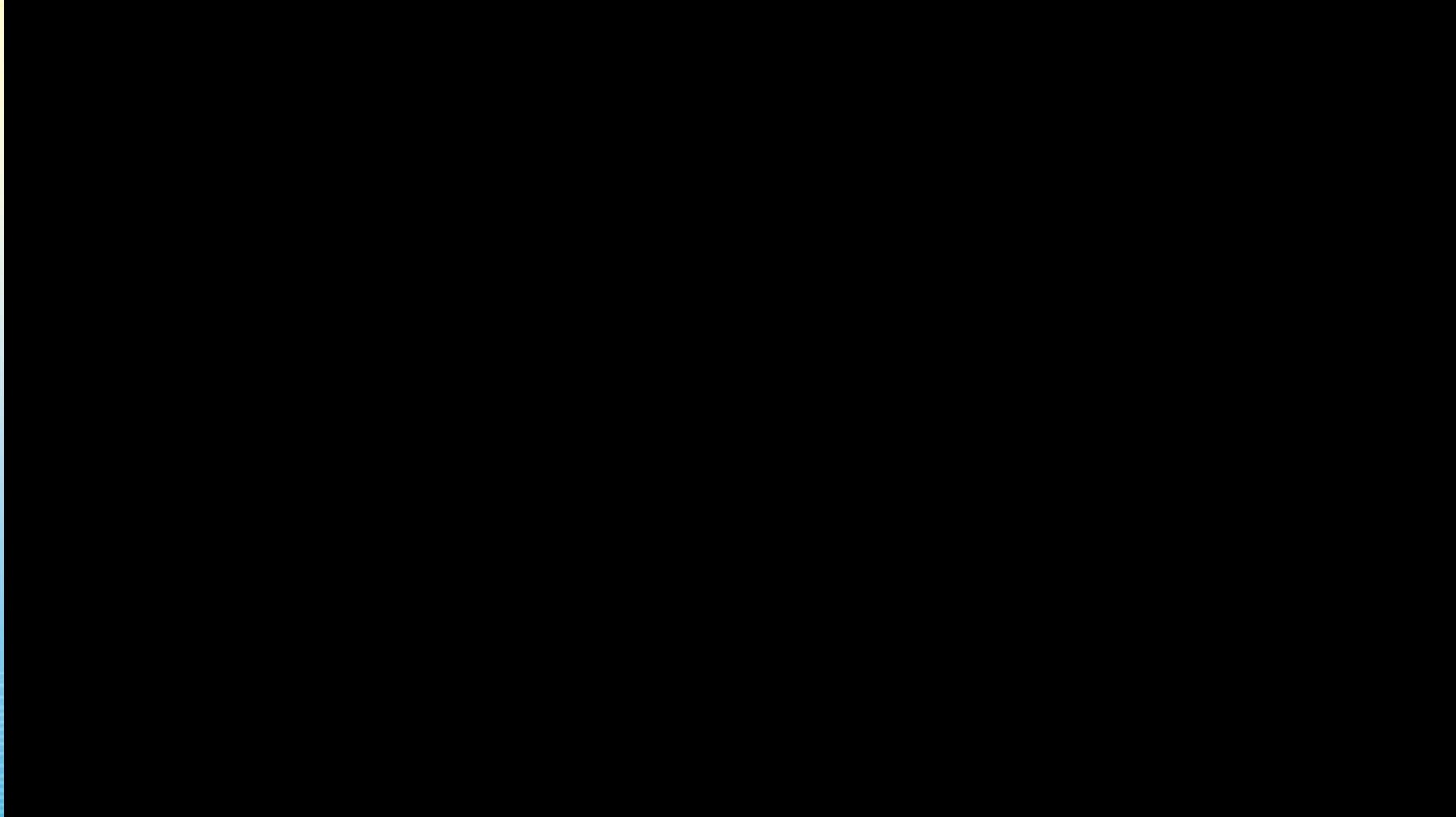
# Phishing – Ergebnisse aus Audits



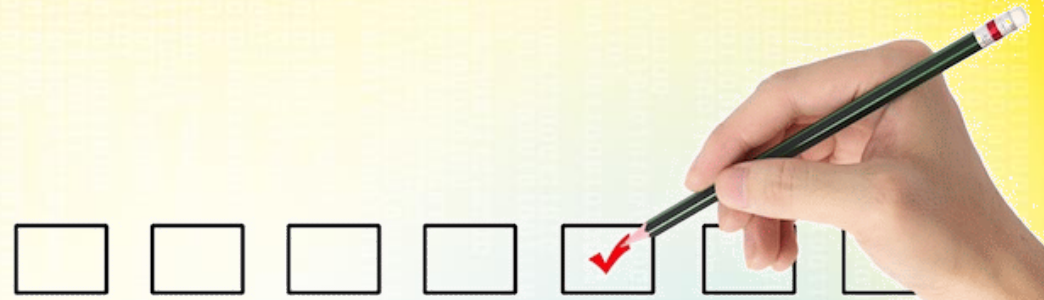
# Phishing – Ergebnisse aus Audits

- Auswertung
  - Formular wurde 32x ausgefüllt
  - Bewertung: 10x Mittel, 20x Sicher, 2x Sehr sicher
  - 12 Personen nutzen das Passwort auch ausserhalb
  - 1 Person hat das Passwort vor Versand wieder gelöscht
  - auch einfache Passworte vorhanden: Sommer14, Beckham13, Grauer123, Mario08, Batman123, NewOrleans15, Fribourg36, DreamBox01, Federer300, malediven16, Alex2002, Arna2012

# Social Engineering



# Fazit



- Es gibt keine 100%-ige Sicherheit, es gibt immer neue Techniken
- Sicherheit möglich durch:
  - Awareness erschaffen
  - Vertrauliche Informationen vernichten (Festplatten/Papier)
  - Vorbildfunktion der Geschäftsleitung
  - Passwörter und Identität schützen
  - Security Audit
  - Betriebsklima



# Informieren Sie sich!

- <http://www.melani.admin.ch>
  - Infoseite zu den Gefahren im Internet
- <http://www.ebankingabersicher.ch>
  - Infoseite für sicheres e-Banking
- <http://www.geschichtenausdeminternet.ch>
  - Infoseite zu den Gefahren im Internet
- <http://www.switch.ch/de/saferinternet/>
  - Sichere Websites für ein sicheres Internet

# Experten für Ihre IT-Sicherheit



A. Wisler



Th. Furrer



S. Müller



A. Kulhanek



M. Hamborgstrøm



M. Hennet



C. Wehrli



S. Walser

# Unsere Dienstleistungen

