



Hochschule  
Albstadt-Sigmaringen  
Albstadt-Sigmaringen University

# Cyber Security und die hohe Kunst der Täuschung



# Cyber Security

und die hohe Kunst der Täuschung



# Tobias Scheible

- Studium Kommunikations- und Softwaretechnik, HS Albstadt-Sigmaringen
- Softwareingenieur im Bereich Web Development, Werbeagentur Gute Aussicht
- Seit 2012: Wissenschaftlicher Mitarbeiter, Hochschule Albstadt-Sigmaringen
  - Seit 2015 in der Fakultät Informatik als Praktikumsbetreuer tätig
  - Seit 2016 im Masterstudiengang Digitale Forensik als Autor und E-Tutor tätig

## **Praktikum IT Security 2**

Bachelor IT Security  
Prof. Holger Morgenstern

## **Projektstudium**

Bachelor IT Security  
Prof. Holger Morgenstern

## **Digitale Forensik**

Bachelor IT Security  
Prof. Holger Morgenstern

## **M103 Internet Grundlagen**

Master Digitale Forensik  
Prof. Dr. Martin Rieger

## **M104 IT-Sicherheit und Angriffe**

Master Digitale Forensik  
Prof. Dr. Martin Rieger

## **M107 Betriebssystemforensik**

Master Digitale Forensik  
Prof. Dr. Martin Rieger

## **M110 Datenträgerforensik**

Master Digitale Forensik  
Prof. Dr. Martin Rieger

## **M116 Unix-Forensik**

Master Digitale Forensik  
Prof. Dr. Martin Rieger

## **Aktivitäten**

Forschung im Bereich Sicherheit von  
IoT-Geräten und Zutrittskontrollen

## **Cyber Security Lab**

Blog, Workshops & Vorträge  
<http://cyber-security-lab.de>



# UMFRAGE IT-Sicherheit

- Wer war schon einmal von einem Hack betroffen?



<http://pingo.upb.de/742051>



# Cyber Security



00000000

?



00000000

# Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de



# Atom-Raketen: Steuerungstechnik aus den 70ern



Quelle: [zeit.de](http://zeit.de)

Quelle: [chip.de](http://chip.de)





# Angriff auf den Fernsehsender TV5

- Umfangreicher Angriff auf den französischen Sender TV5Monde
- Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
- Die Website verbreitete kurzfristig islamistische Drohungen
- Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
- Spekulationen über öffentlich einsehbare Passwörter

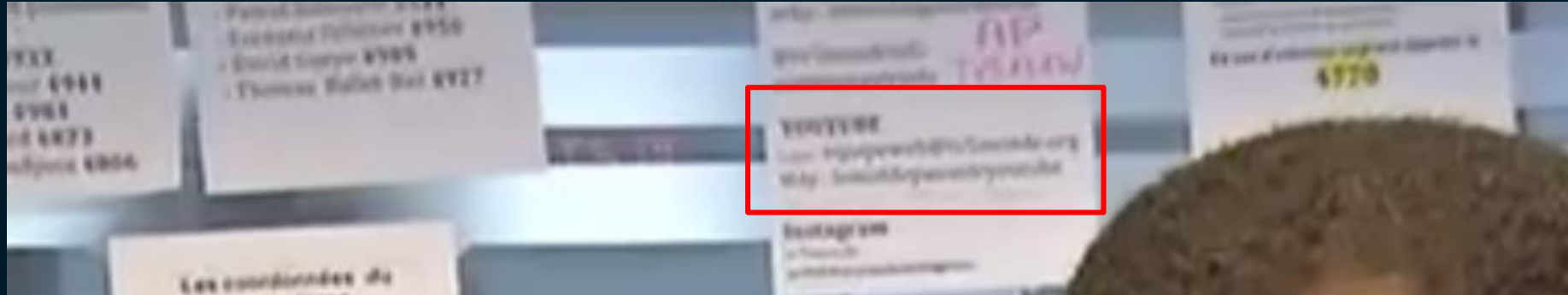
Quelle: [heise.de](http://heise.de)

# Angriff auf den Fernsehsender TV5



Quelle: heise.de

# Angriff auf den Fernsehsender TV5



YouTube Passwort: "lemotdepasseyoutube"  
(etwa "dasyoutubepasswort")



Quelle: heise.de



# Google als Hacking-Tool



Google-Suche

Auf gut Glück!



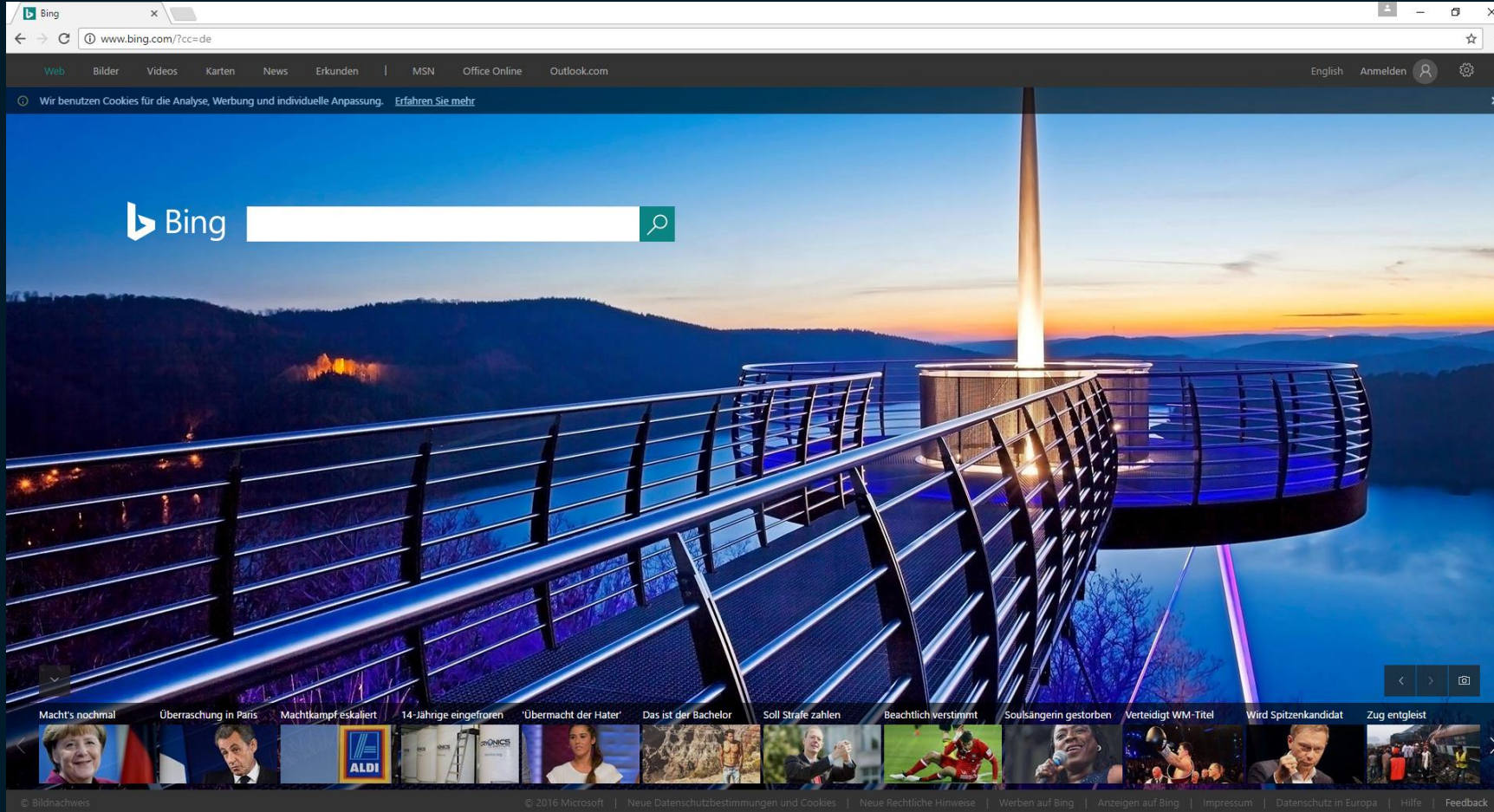
# PRAXIS Hacking mit Google

- GHDB – the Google Hacking DataBase
- Beispiel Suchanfragen nach Webcams:
  - `inurl:"viewerframe?mode=motion"`
  - `intitle:"snc-rz30 home"`
  - `intitle:"WJ-NT104 Main"`
  - `inurl:LvAppl intitle:liveapplet`
  - `intitle:"Live View / - AXIS"`
  - `inurl:indexFrame.shtml`





# PRAXIS Hacking mit Suchmaschinen



# Aktion der Groupe Mutuel



Zürich, Hauptbahnhof

Quelle: youtube.com

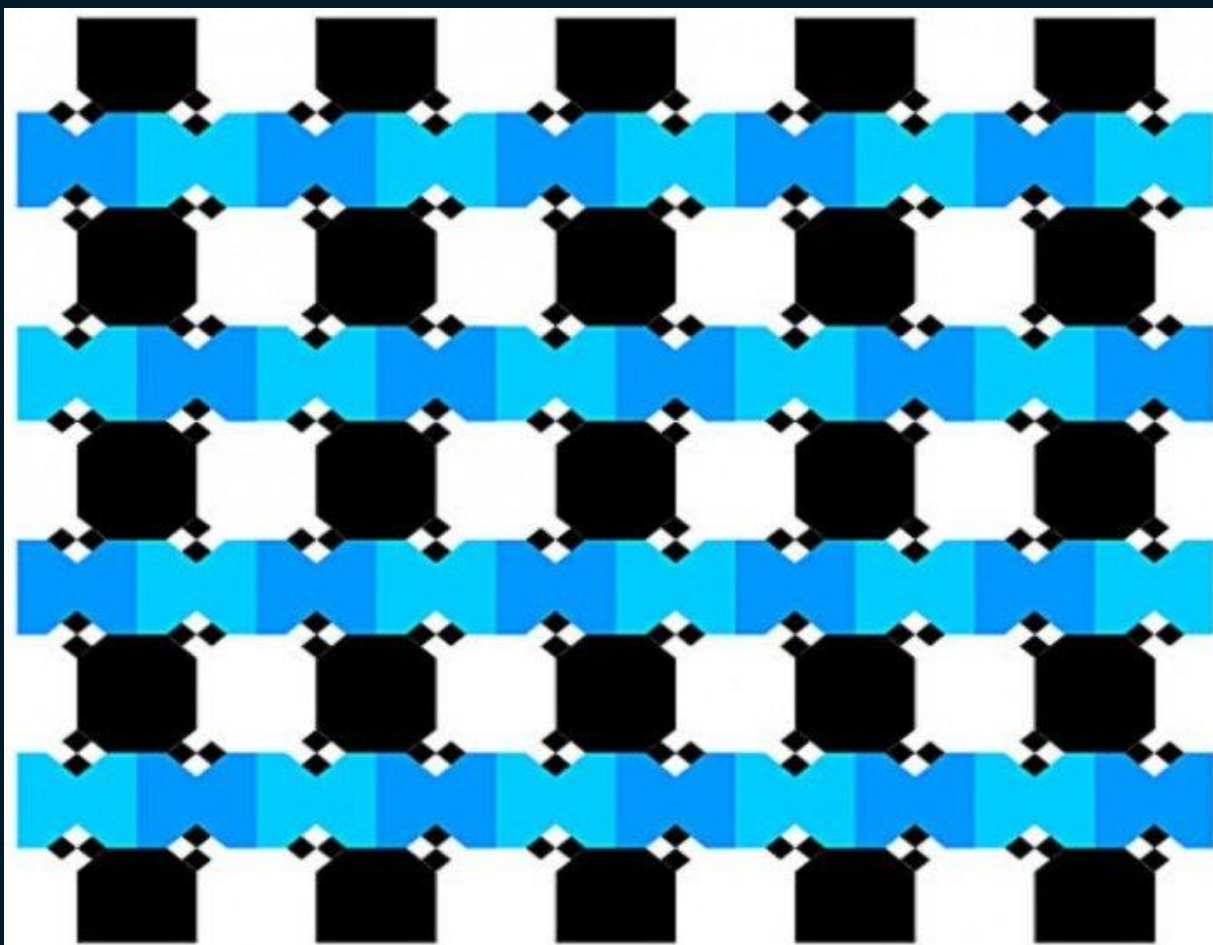




# Social Engineering



# UMFRAGE Menschliche Wahrnehmung



Welche Linien sind nicht gerade?

<http://pingo.upb.de/407781>



Quelle: [sowas-gibt-es.net](http://sowas-gibt-es.net)



# Mischtheatralismus

Alle Linien sind parallel zueinander

Quelle: [sowas-gibt-es.net](http://sowas-gibt-es.net)



# Social Engineering

- Der Mensch als größtes Sicherheitsrisiko
- Know-how der Mitarbeiter
- Social Engineering, um Menschen gezielt zu manipulieren
  - Hilfsbereitschaft
  - Autoritätsgläubigkeit
  - Eitelkeit
  - Neugierde
  - Legitimation





Quelle: [pics-for-fun.com](http://pics-for-fun.com)



Quelle: [de.pinterest.com](http://de.pinterest.com)

# Fingerabdruckscanner



Quelle: [imore.com](http://imore.com)



# Fingerabdruckscanner



Quelle: [rolf-fensterbau.de](http://rolf-fensterbau.de)

# Fingerabdruckscanner



Quelle: [telegraph.co.uk](http://telegraph.co.uk)



# Ursula von der Leyen



Quelle: [n24.de](http://n24.de)

# Fingerabdruck von Ursula von der Leyen

guten Tag, mein Name ist  
Dr. von der Leyen



Quelle: [heise.de](http://heise.de)



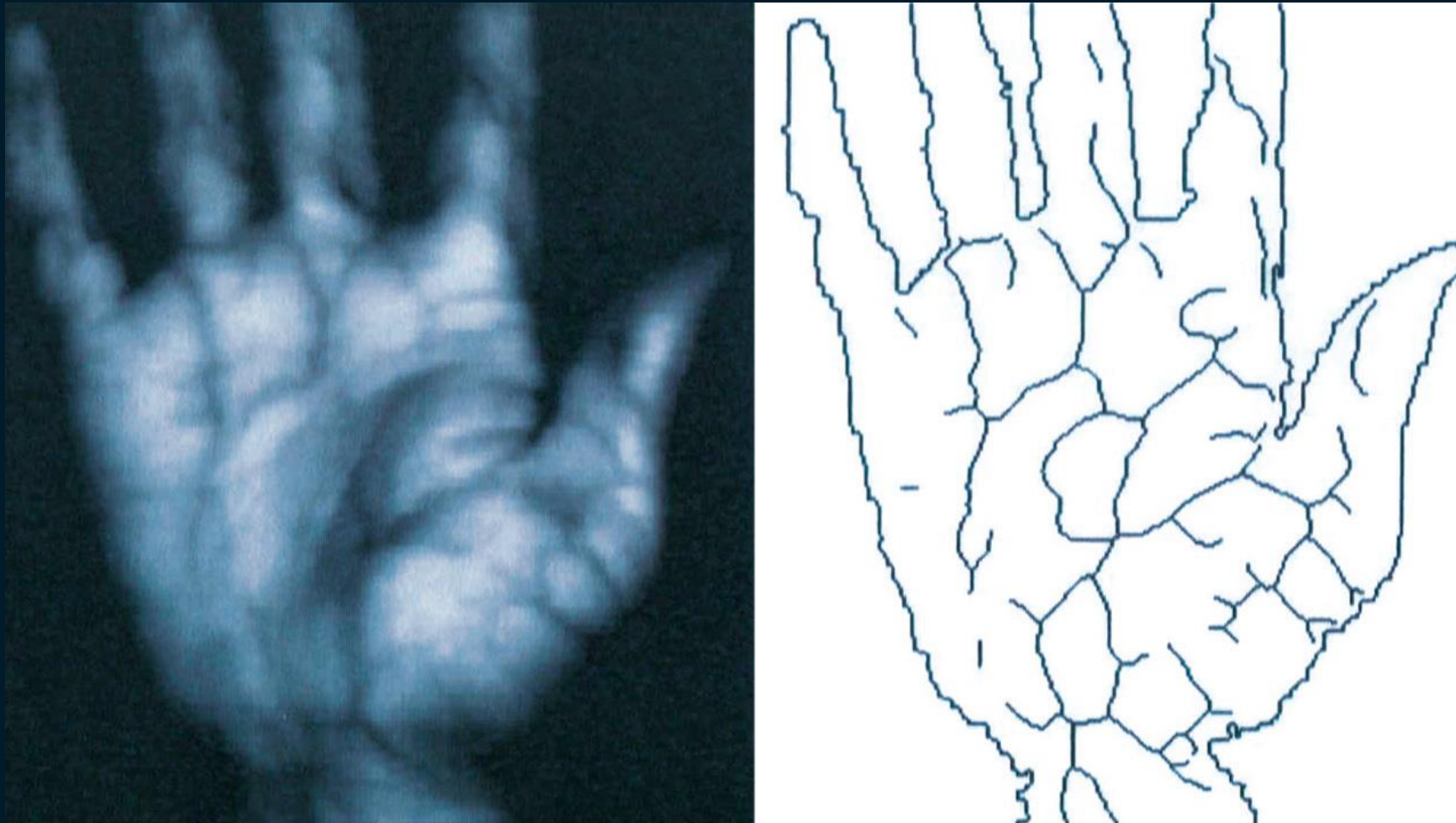
# Venen-Scanner



Quelle: [futerzone.at](http://futerzone.at)



# Venen-Scanner



Quelle: [futerzone.at](http://futerzone.at)

# Social Engineering - Gefälschte E-Mail

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop | Schlagzeilen | Wetter | TV-Programm | mehr ▼

**SPIEGEL ONLINE SCHULSPIEGEL** Login | Registrierung

Abi - und dann? | Querweltein | Leben U21 | Wissen

Nachrichten > SchulSPIEGEL > Wetter > Schulfrei in Niedersachsen wegen gefälschter E-Mail

## Gefälschte E-Mail: Schulfrei ermöglicht



Winterwetter in Niedersachsen: Freier Tag im Schnee wegen gefälschter E-Mail

Eine gefälschte E-Mail hat Schülern in Niedersachsen einen freien Tag beschert. Der Unterricht falle wegen des Winterwetters aus, hieß es darin. Hunderte Schüler glaubten der Meldung - und blieben zu Hause.

Quelle: [spiegel.de](http://spiegel.de)





# Phishing

München, den 09.10.2014

**Wichtige Kundenwarnung!**

**Sehr geehrte Damen und Herren,**

wir, das Amazon Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst.

Aus diesem Grund ist es nötig in regelmäßigen Zeitabständen Ihre persönlichen Daten zu bestätigen.

Diese Bestätigung dient dazu, dass Ihre persönlichen Daten stets aktuell sind. So können wir Sie unter anderem auch vor Missbrauch durch Dritte schützen, da unser System Abweichungen erkennen kann.

Sollte eine Abweichung vom System erkannt werden, werden Sie anschließend von einem unserer Mitarbeiter telefonisch kontaktiert.

Bitte tragen Sie alle erforderlichen Daten wahrheitsgemäß und vollständig ein.

**Zur Bestätigung** (anklicken)

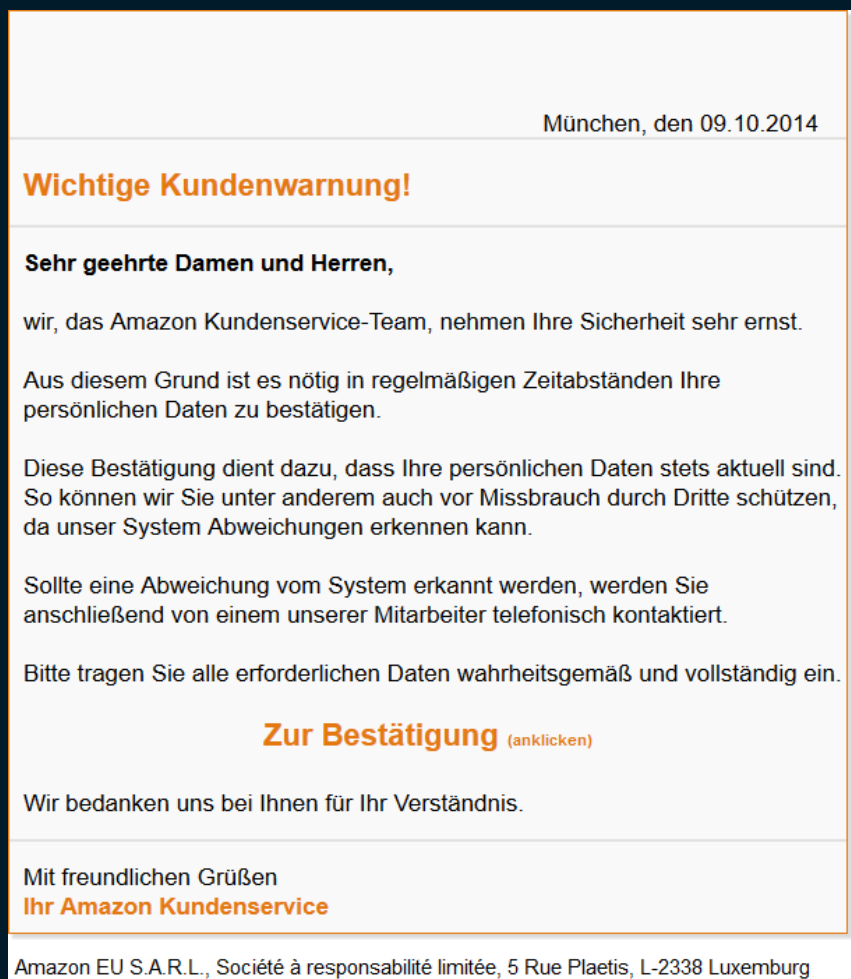
Wir bedanken uns bei Ihnen für Ihr Verständnis.

Mit freundlichen Grüßen  
**Ihr Amazon Kundenservice**

Amazon EU S.A.R.L., Société à responsabilité limitée, 5 Rue Plaetis, L-2338 Luxembourg



# Phishing



- 1. Falsche E-Mail-Adresse
  - Nicht bei Amazon registriert
- 2. Keine Anrede
  - Amazon hat meine Daten
- 3. Kein Amazon Link
  - <http://link-share.cc/10>

PHISHING



# Moderner Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- Social Engineering Angriff auf das Gefängnis
  - Smartphone eingeschmuggelt
  - Domain reserviert, die dem zuständigen Gericht ähnelt
  - E-Mail-Adresse mit dieser Domain eingerichtet
  - Hat sich als leitender Beamter ausgegeben
  - Anweisungen zu seiner Entlassung gegeben
- Gefangener kam frei

Quelle: [heise.de](http://heise.de)



# Passwortsicherheit



Quelle: youtube.com

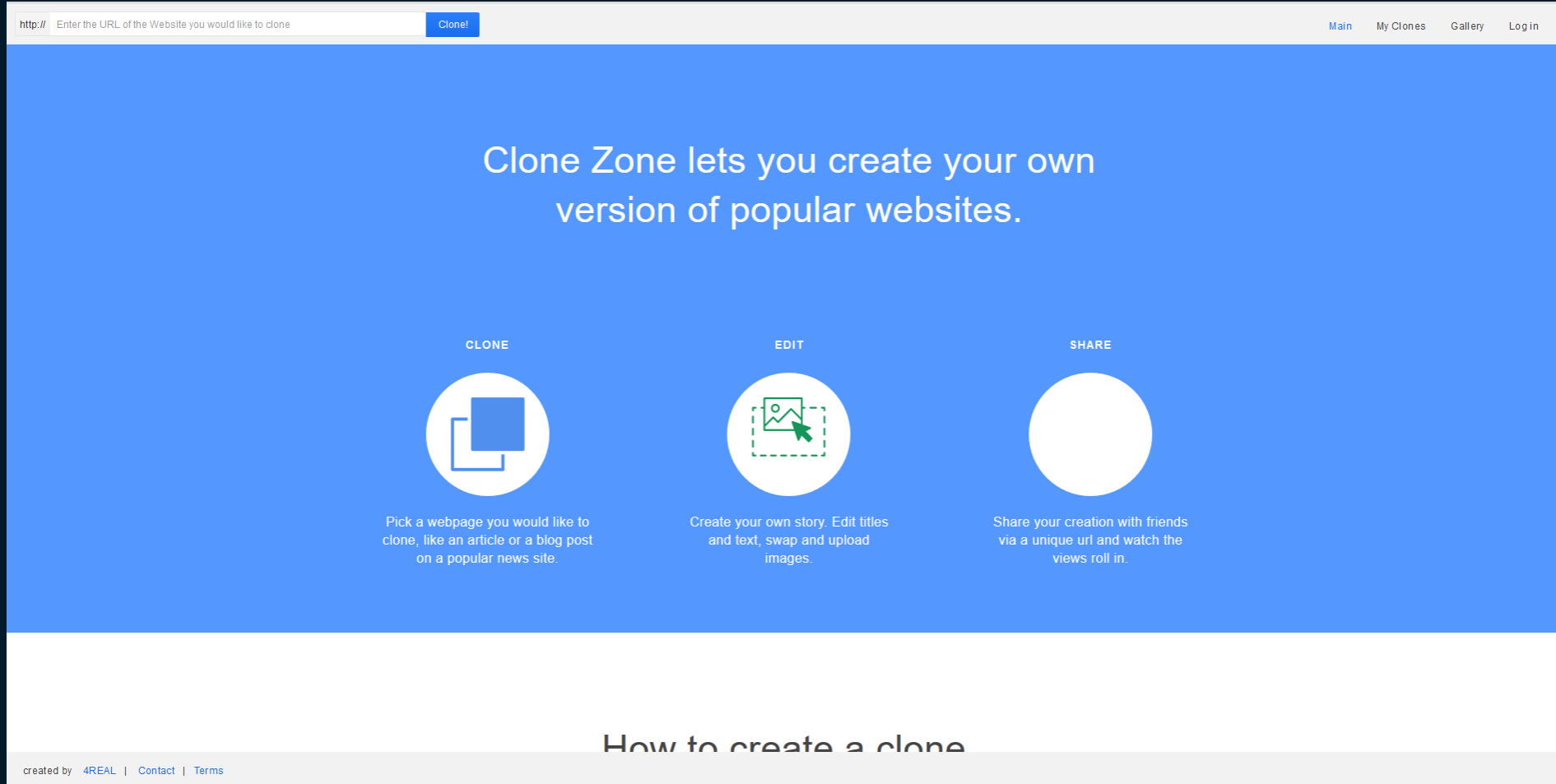




# Social Hacking



# PRAXIS Website manipulieren




Quelle: [clonezone.link](http://clonezone.link)



# PRAXIS E-Mail-Versand manipulieren

Cyber Security Vortrag · x

← → ↻ <https://cyber-security-lab.de/vortrag/mail.php> ☆ ⋮



Hochschule  
Albstadt-Sigmaringen  
University of Applied Sciences

Fakultät Informatik

Kompetenzzentrum  
Cyber Security Lab

Cyber Security Vortrag  
**E-Mail Versand manipulieren**

Der Versand von E-Mails kann sehr einfach manipuliert werden.

**Versand**

Absender Name	Absender Mail	Empfänger	Betreff
<input type="text" value="Nachname, Vorname"/>	<input type="text" value="mail@example.com"/>	<input type="text" value="mail@example.com"/>	<input type="text" value="Text"/>

Text

E-Mail senden






# PRAXIS SMS-Versand manipulieren

Cyber Security Vortrag · x

← → ↻ <https://cyber-security-lab.de/vortrag/sms.php> ☆ ⋮



Hochschule  
Albstadt-Sigmaringen  
University of Applied Sciences

Fakultät Informatik

Kompetenzzentrum  
Cyber Security Lab

Cyber Security Vortrag  
**SMS-Versand manipulieren**

Der Versand von SMS kann sehr einfach manipuliert werden.

**Versand**

Absender  Empfänger

Text

**SMS senden**

# UMFRAGE Authentizität

- Ist die Immatrikulationsbescheinigung echt?



<http://pingo.upb.de/169348>



# PRAXIS Website manipulieren

The screenshot shows a web browser window with the URL [qis.hs-albsig.eu/verify.html](http://qis.hs-albsig.eu/verify.html). The page header includes the university logo and navigation links: [Startseite](#), [Verifikation](#), and [Chipkarte Info](#). Below the header, there is a section titled "Studentisches Leben" with a sub-link "Verifikation von Studienbescheinigungen". The main content area is titled "Verifikation von Studienbescheinigungen" and contains the following text: "Bitte geben Sie in das folgende Eingabefeld den Verifikationsschlüssel ein. Anschließend bestätigen Sie Ihre Eingabe mit einem Klick auf Verifizieren." Below this text is a form with a label "Verifikationsschlüssel / Verify-Id" and three input fields. A "Verifizieren" button is located below the input fields. The footer of the page displays the number of active users (84) and provides contact information for the webmaster and lost card service.

Hochschule Albstadt-Sigmaringen - QIS - Online Funktionen

[Startseite](#) [Verifikation](#) [Chipkarte Info](#)

[Startseite](#) | [Anmelden](#)

[Studentisches Leben](#)

Sie sind hier: [Startseite](#) > [Verifikation von Studienbescheinigungen](#)

■ [Verifikation von Studienbescheinigungen](#)

**Verifikation von Studienbescheinigungen**

Bitte geben Sie in das folgende Eingabefeld den Verifikationsschlüssel ein.  
Anschließend bestätigen Sie Ihre Eingabe mit einem Klick auf Verifizieren.

Verifikationsschlüssel / Verify-Id

[Verifizieren](#)

Anzahl aktueller Nutzer: 84 [Startseite](#) [Zurück](#) [Chipkarten Infos](#) [Webmaster-qis@hs-albsig.de](mailto:Webmaster-qis@hs-albsig.de) [Tarifliste verloren? tarifliste@hs-albsig.de](mailto:Tarifliste-verloren?tarifliste@hs-albsig.de)



# Wissenschaftliche Weiterbildung



# Weiterbildungsangebot

## Vorkurse

### Studium Initiale

Berufsbegleitend zum Hochschulzugang

## Zertifikate

### Hochschulzertifikate

Auf hohem akademischen Niveau mit ECTS-Punkten

## Masterstudiengänge

### Data Science

Riesige Datenmengen und moderne Technologien nutzen

### Digitale Forensik

Online Studium für Ermittler im Bereich Cybercrime

### IT GRC Management

Intensiver, praxisorientierter Kompetenzaufbau

Weitere Informationen:

<http://hs-albsig.de/weiterbildung>





# Vielen Dank

Präsentation online unter <http://cyber-security-lab.de>