

# CYBER SECURITY SHOW

9. Sicherheitsforum "Online-Banking"  
Im Forum der S-Academy in Dreieich

AWARE7 GmbH  
Bergmannstr. 5  
45886 Gelsenkirchen  
<https://aware7.de>

Chris Wojzechowski  
Geschäftsführer  
[chris@aware7.de](mailto:chris@aware7.de)  
[@wojzechowski](https://www.instagram.com/wojzechowski)

Matteo Große-Kampmann  
Geschäftsführer  
[matteo@aware7.de](mailto:matteo@aware7.de)  
[@pizzahax](https://www.instagram.com/pizzahax)



**#GELSENKIRCHEN**



# Technik begeistert!

Fotografieren, navigieren &  
kommunizieren  
von überall



# DIE DIGITALISIERUNG ERÖFFNET CHANCEN



## zur Kommunikation

71% der Menschen in Deutschland nutzen WhatsApp. Nur Youtube ist beliebter. Die Frage ist, wie lange noch?



## für den Weltwirtschaftsraum

Digitalisierung ist ein globaler Markt. Die Frage ist nur, welche Position Deutschland einnehmen wird - oder sogar inne hat?



## für die Gesundheit

Die EKG Funktion von Smartwatches haben Menschen warnen können, die einen Herzinfarkt erleiden werden.



FaceApp



Meinung?

Geschäftsmodell?

Chance oder Risiko?

KI wird uns beschäftigen

## Wo ist der Unterschied?







## Wie gehen Kriminelle vor?

Wir schauen uns die Betrugsmaschen der Kriminellen an, vollziehen sie nach, bauen sie nach um anschließend zu sensibilisieren.

## Welche Sicherheitslücken gibt es?

Wir schauen uns Medienphänome an, analysieren diese, schätzen sie ein und arbeiten bei verfügbaren Kapazitäten mit an der Lösung.

## Was ist das tagesaktuelle IT-Geschehen?

Wir sind stets auf dem neuesten Stand der IT-Sicherheit - im Privat, Geschäfts- & Forschungsbereich. Zum Nutzen aller.



## “One Hit Wonder”

Keine Ankündigung, Keine Drohung

ZDNet / Sicherheit / Cyberkriminalität

### Hacker zerstört nahezu jegliche Daten von US-E-Mail-Provider VFEmail

Betroffen sind Kunden, deren Daten in den USA gespeichert werden. Dort löscht ein unbekannter Hacker die Festplatten der primären und der Backup-Server. Nur ein Backup-Server in den Niederlanden übersteht den Angriff offenbar unbeschadet.

von Stefan Beiersmann am 13. Februar 2019, 12:33 Uhr

Digitaler Einbruch  
Festplatten überschrieben  
Backups gelöscht

Unternehmen passé

## “Kollateralschaden”

Keine gezielte Attacke

ENTERPRISE

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

### Shipping company Maersk says June cyberattack could cost it up to \$300 million

- Maersk has put in place "different and further protective measures" following the attack.
- Merck and WPP were among the companies that were also affected by NotPetya.

Jordan Novet | @jordannovet

Published 2:04 PM ET Wed, 16 Aug 2017 | Updated 3:00 PM ET Wed, 16 Aug 2017

CNBC

Unternehmen konnte nur gerettet werden, weil ein **Computer** in Nigeria **nicht in Betrieb** war (Stromausfall).

Das Fortbestehen des Unternehmens hing von der Verfügbarkeit einer einzigen Festplatte ab

# IT-Sicherheit bleibt auf der Strecke!



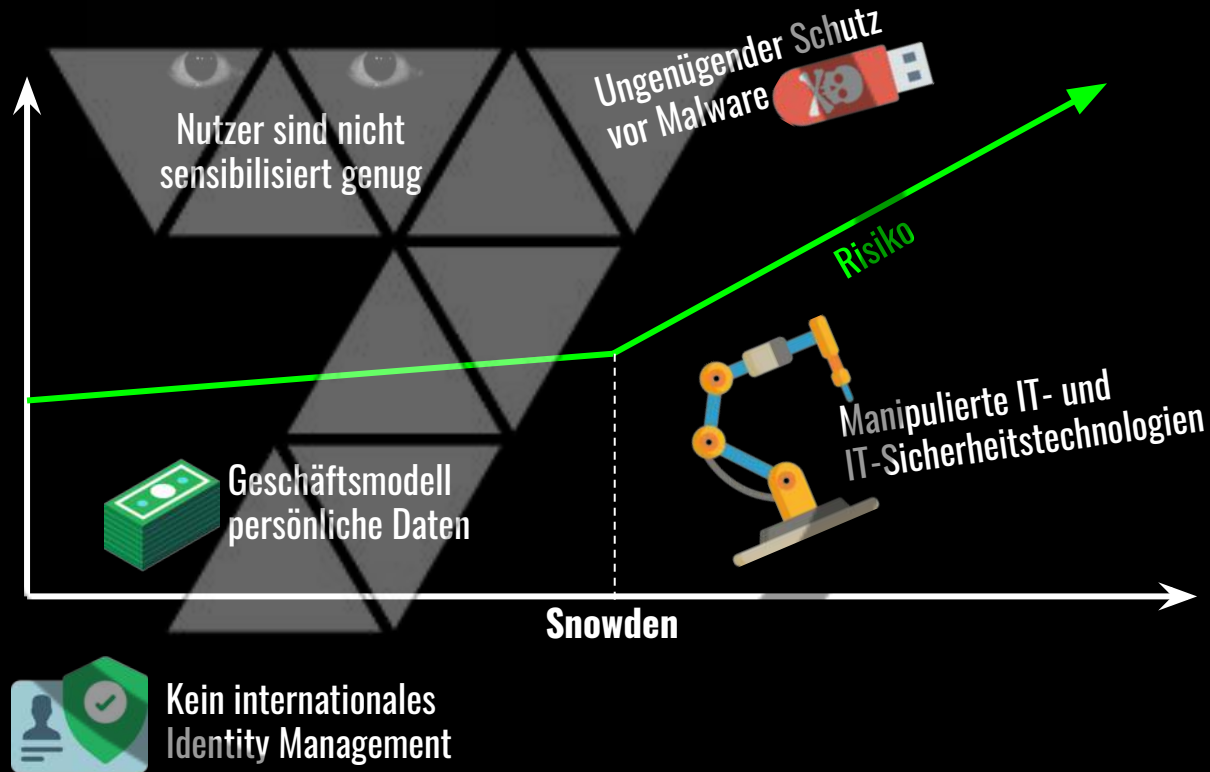
- 2009 erschienen
- 2014 Verschlüsselung etabliert
- 5 Jahre unsichere Kommunikation
- und wie sieht es jetzt mit personalisierter Werbung aus?
- .. und wird Ende 2019 mit Instagram & Facebook zusammengelegt



Cloud Computing ist eine Herausforderung



Ein hohes Risiko bei der E-Mail Nutzung





**Wir werden heute die Brechstange anlegen!**



**Wir wollen niemanden anstiften eine Straftat zu begehen!**



**Alle Informationen und Aktionen dienen ausschließlich dazu sein Risiko einzuschätzen und sich zu schützen!**

Datenmissbrauch durch Cambridge Analytica UPDATE 05.04.2018, 12:16 Uhr

**Facebook-Skandal betrifft bis zu 310.000 Nutzer aus Deutschland**

**Hacker-Jackpot: Credit Bureau Equifax gehackt**

08.09.2017 07:48 Uhr - Daniel AJ Sokolov

**Passwörter im Klartext: 20.000 Euro Bußgeld nach DSGVO gegen Knuddels.de**

380.000 Kreditkarten betroffen

**Datenpanne bei British Airways**

Stand: 07.09.2018 09:42 Uhr

**Yahoo verliert bei weiterem Hack Daten von eine Milliarde Nutzerkonten**

## TOP 5 Passwörter in Deutschland

1. hallo
2. passwort
3. hallo123
4. schalke04
5. passwort1

## TOP 5 Passwörter weltweit

1. 123456
2. 123456789
3. 1234
4. 12345
5. 12345678

## Setzt auf Eselsbrücken und Denkstützen!

(Persönlichen)  
Satz ausdenken

Ich kann mir mein Passwort nicht merken!

Die ersten  
Buchstaben markieren

Ich **k**ann mir mein **P**asswort nicht **m**erken!

Zeichen ersetzen

Ich-kann-mir-m**1**-Passwort-nicht-merken!

Restliche Zeichen  
verwerfen.

I-k-m-m**1**-P-n-m!

Passwort  
individualisieren

I-k-m-m**1**-P-n-m!**+ama**

.. und erheblich  
sicherer sein!

I-k-m-m**1**-P-n-m!**+fa**

## Speichert Zugänge und Daten

Benutzernamen, E-Mails, Passwörter

## Schlägt sichere Passwörter vor

Rezeptur gibt Stärke für jeden Zugang vor

## Tlw. Team- und Family Shares

Passwörter teilen, zentral sammeln und verwalten

## Es gibt on- und offline Varianten

Für jeden Geschmack und Bedarf ist etwas dabei

## Fügt Passwörter nur auf echten Websites ein

Indirekter Schutz vor Preisgabe von Creds auf Phishing Sites

## “Wo bin ich überall angemeldet?”

Konsequenter Einsatz sorgt für hohe Account Hygiene

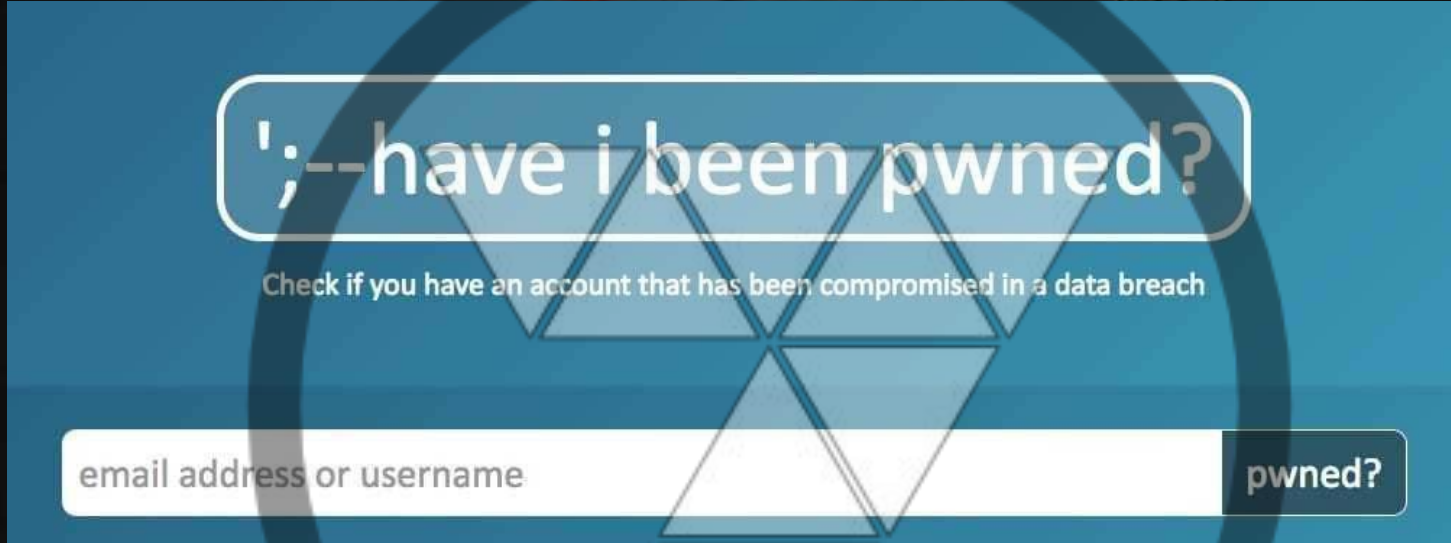






**zweiterfaktor.de** informiert umfangreich über mögliche Zwei-Faktor-Authentifizierungen:

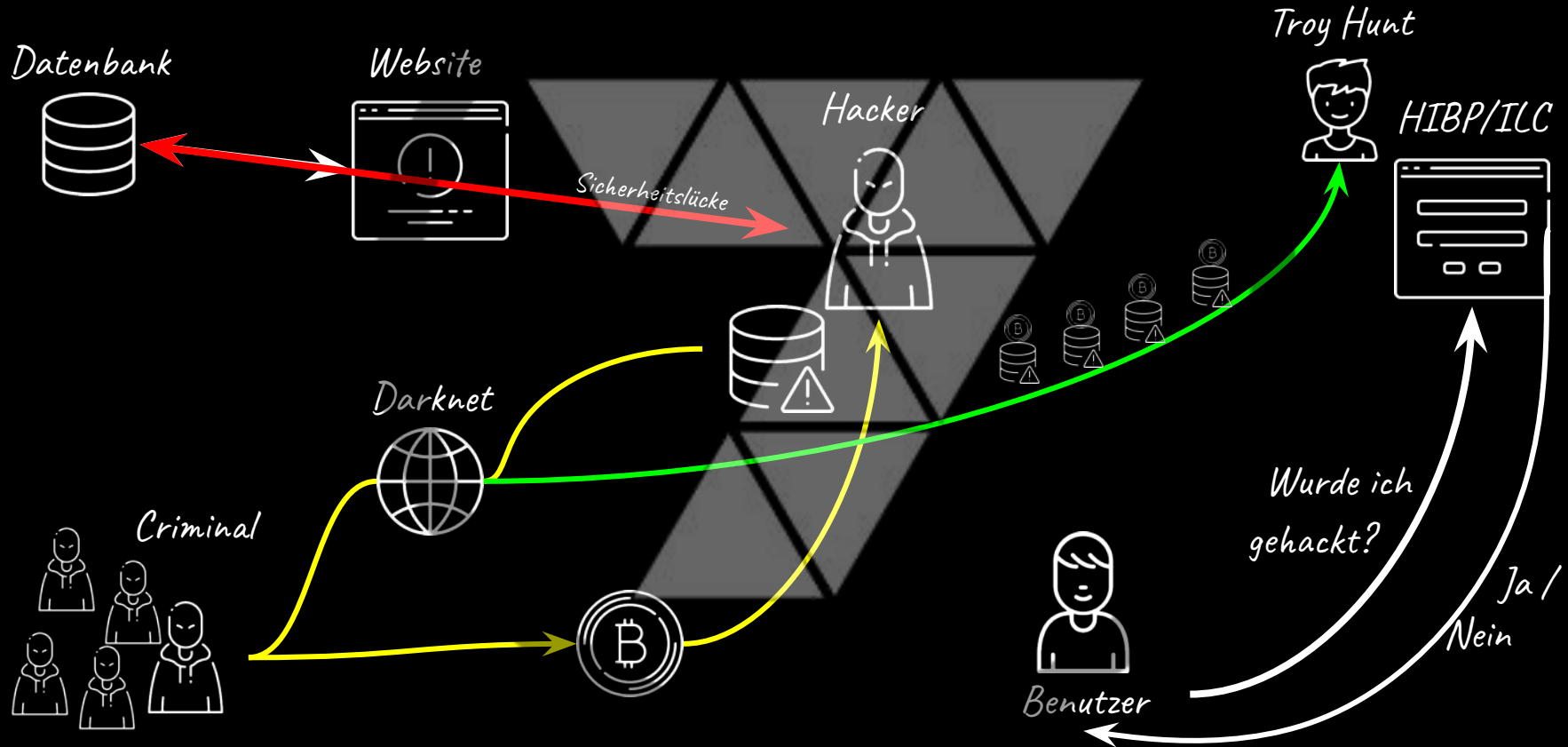
- Welcher Anbieter bietet überhaupt die 2FA an
- Welche Möglichkeiten der 2FA bieten die Plattformen an?
- Links zu den Anleitungen, wie die 2FA aktiviert/deaktiviert werden kann



[haveibeenpwned.com](https://haveibeenpwned.com) gibt Auskunft darüber ..

- ob die eigenen Daten in bekannten Datendiebstählen vorkommen
- und wenn ja in welchem Umfang
- nach Registrierung auch für sensible Datendiebstähle
- Alternative aus DE: identity leak Checker

## Woher stammen die Daten für Passwort Statistiken und HIBP?





Hallo Chris

Der Thermomix® TM5 von Vorwerk ist eine einzigartige Küchenmaschine, mit der Sie neue kulinarische Wege gehen, Ihr Potenzial als Koch entfalten können und gleichzeitig Zeit und Aufwand sparen können. Dabei ist er enorm leistungsstark, vielseitig innovativ und nimmt Ihnen beim Kochen viel Arbeit ab.

Nehmen Sie an unserer kurzen Umfrage teil und finden Sie heraus, ob Sie sich als Gewinner qualifizieren!

Jetzt teilnehmen

Der Thermomix® TM5

- Inklusive **Kochbuch + Rezept-Chip**
- **3 Ausgaben** des Kundenmagazine Finesse
- Zugang zum innovativen **Thermomix® Rezept-Portal**
- Einladung zum kostenlosen **Basis-Kochkurs**
- **Persönliche** Betreuung vor Ort



ANGEPASSTE CI

GUTE ANSPRACHE

STIL VON VORWERK

SCHWER ZU ERKENNEN...

## Können Sie es lesen?

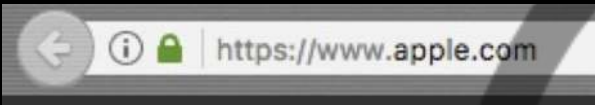
Ehct ksras! Gmäëß eneir Sutide eneir Uvinisterät, ist es nchit witihcg, in wlecehr Rneflogheie die Bstachuebñ in eneim Wort snid, das ezniige was wcthiig ist, das der estre und der leztte Bstabchue an der ritincegñ Pstoiin snid. Der Rset knan ein ttoaelr Bsinöldñ sein, tedztorm knan man ihn onhe Pemoblre lseen. Das ist so, weil wir nicht jeedñ Bstachuebñ enzelin leesñ, sñderon das Wort als gzeans enkreenn. Ehct ksras! Das ghet wicklirh! Und dfüar ghneen wir jrhlæng in die Slhcue!

**Und weil das funktioniert,  
funktioniert auch das ...**

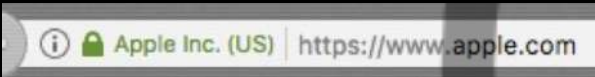
sls-direkty.de  
sls-direktz.de  
rls-direkt.de  
qls-direkt.de  
wls-direkt.de  
cls-direkt.de  
3ls-direkt.de  
sms-direkt.de  
sns-direkt.de  
shs-direkt.de  
sds-direkt.de  
slr-direkt.de  
slq-direkt.de  
slw-direkt.de  
slc-direkt.de  
sl3-direkt.de  
slsmdirekt.de  
sls-eirekt.de  
sls-firekt.de  
sls-lirekt.de  
sls-tirekt.de

sls-dhrekt.de  
sls-dkrekt.de  
sls-dmrekt.de  
sls-darekt.de  
sls-dyrekt.de  
sls-disekt.de  
sls-dipekt.de  
sls-divekt.de  
sls-dizekt.de  
sls-dibekt.de  
sls-di2ekt.de  
sls-dirdkt.de  
sls-dirgkt.de  
sls-dirakt.de  
sls-dirmkt.de  
sls-dirukt.de  
sls-direjt.de  
sls-direit.de  
sls-direot.de

**Das ist nur eine Inspiration..  
viele Adressen sind noch frei!**

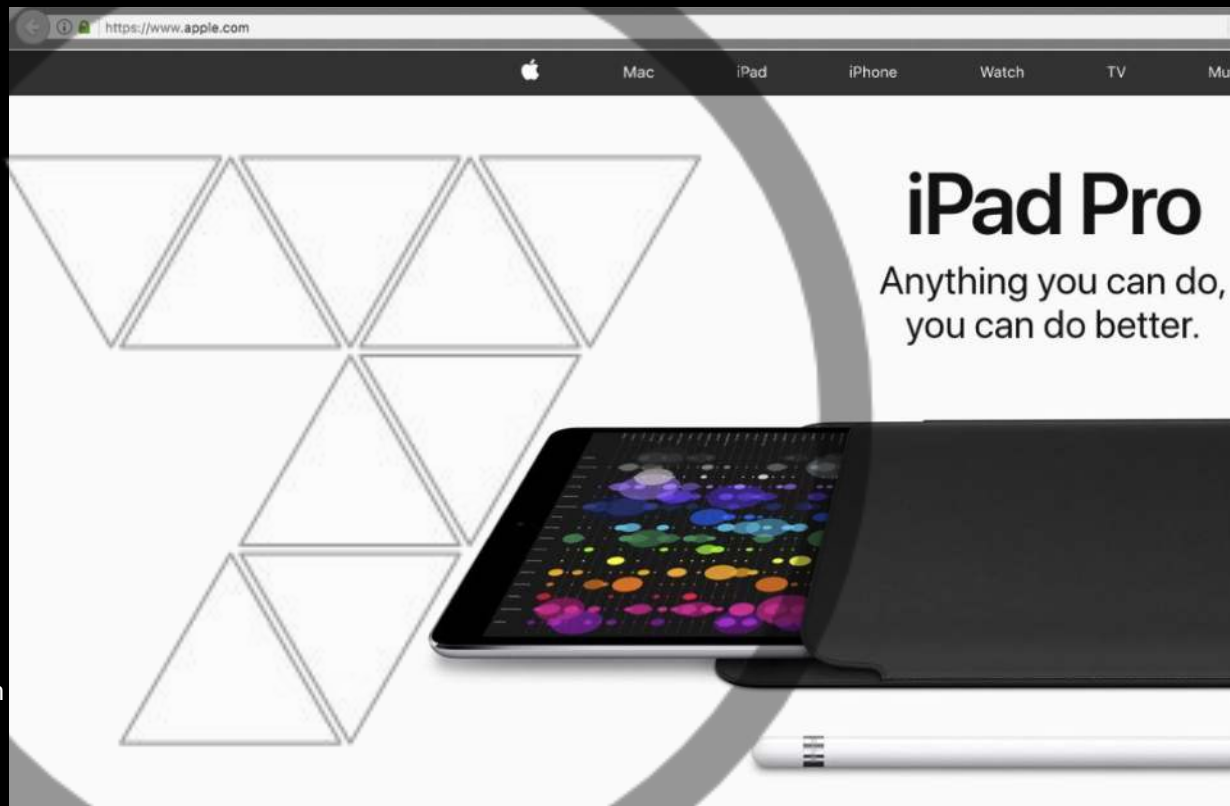


**SERIÖSE ADRESSE?**



**ORIGINAL**

- ca. **100 Millionen** solcher Domains gibt es
- unterschiedliche Sonderzeichen
- Adresse wenn möglich über **Tastatur** eingeben
- **Aktuellste Browser Version** nutzen
- **Verkürzte Links vermeiden**



## E-Mails : Welche Möglichkeiten zur Fälschung gibt es?

### Absendername (Leicht)

- Kann von jedem beliebig eingetragen werden.
- Technische Kenntnisse sind nicht nötig.
- Einstellung kann in jedem Programm vorgenommen werden

### Verweis (Leicht)

- Der Verweis ist nur der Name für den Link
- Hier kann alles eingetragen werden
- Was sich tatsächlich hinter dem Verweis versteckt, verrät nur der Link

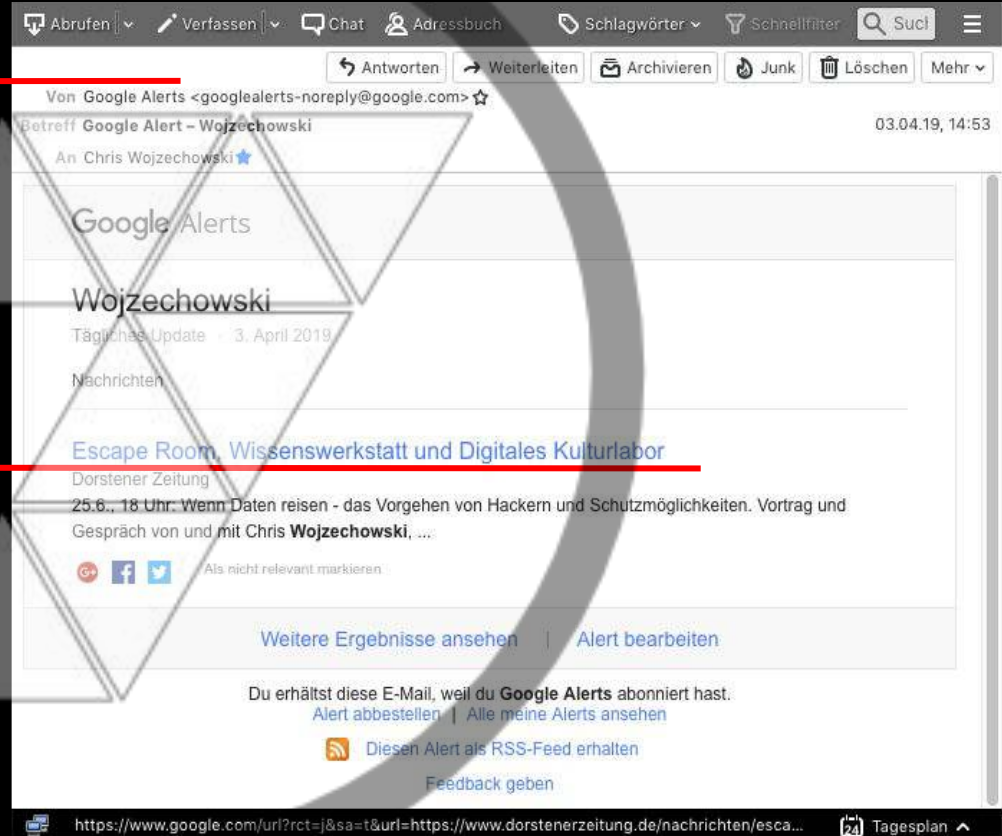
### Link (Mittel)

- Der Link ist das am Ende gefährliche
- Gut gefälschte Links sind schwierig zu erkennen

**Absendername**

**Verweis**

**Link**



## E-Mails : Welche Möglichkeiten zur Fälschung gibt es?

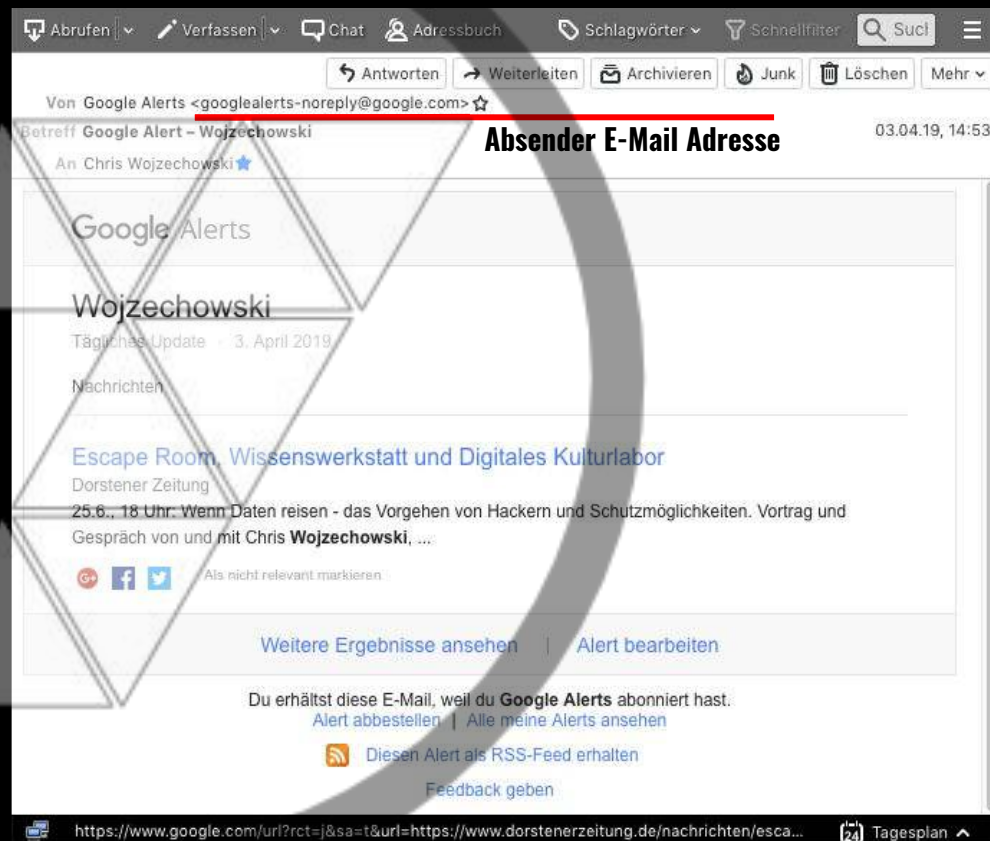
### Absender E-Mail Adresse

Zwei Varianten haben sich in der Vergangenheit etabliert:

1. **Die Adresse wird gefälscht.**  
 Jeder kann E-Mails im Namen von sls-direkt.de versenden.  
 Das hat jedoch diverse Nachteile für den Angreifer
2. **Die Adresse wird ähnlich registriert.**  
 Eine Adresse die ähnlich klingt ist "echt", kann bestätigt werden  
 und hat Vorteile für den Angreifer. Z.B.  
 sns-direkt.de  
 sls-firekt.de  
 sls-direkt.de  
 sls-direkt-de.com  
 www-sls-direkt.de

In allen Fällen gibt es offensichtlich falsche, semi-professionell gefälschte  
 und hochprofessionelle Phishingmails.

Letzteres erfordert zur Erkennung eine hohe Aufmerksamkeit.





INFORMATION  
ABFANG

if(is)  
internet-sicherheit.

ENKELTRICHTER  
POLIZEIMASKE

**Polizei NRW Bochum**  
23 Min · 🌐

Es hätte auch Ihre Mutter/Oma sein können ... Ein falscher Polizist und ein angeblicher Staatsanwalt haben eine Seniorin aus #Witten (76) um ihr Erspartes gebracht. Ihre Masche war perfide.

**Polizist falsch, Staatsanwalt auch**  
Betrüger bringen Wittener Seniorin um ihr Erspartes

Bitte teilen!

**ZURÜCKRUFEN!**

Chris Wojzechowski  
B.Sc.

Wissenschaftlicher  
Mitarbeiter

E-Mail: [wojzechowski\(at\)internet-sicherheit.de](mailto:wojzechowski(at)internet-sicherheit.de)

PGP-Key: [0x46D75D9C](https://keybase.io/wojzechowski)

Telefon: +49 (0) 209 95 96 766







Raum: A4.1.10.4

Webseite: <https://technique-blog.de/>

Angriffsmöglichkeiten - Hacking Hardware



## Angriffsmöglichkeiten - Hacking Hardware

<p>USB-Stick bestseller</p>  <p>2,94 €</p>	<p>USB Stick design</p>  <p>3,26 €</p>	<p>USB Stick loop</p>  <p>3,26 €</p>	<p>USB-C</p>  <p>MicroUSB</p> <p>Lightning</p>
<p><b>Sale!</b></p> <h3>USB KILL PRO KIT</h3> <p><b>64,95 €</b> Instead of 78,89-€</p> <p>Pro testing kit: USB Kill 3.0 Anonymous, Adaptor Pack and Testing Shield. Free International Shipping &amp; 20% Discount. Go Pro, order today!</p> <p>Chose your edition: 🔗 <b>Anonymous Edition:</b> No brand, no text, 100% discrete, or 🔗 <b>Standard Edition:</b> White Case, USB Kill Logo + Text</p>  			

Mehrfachverwendung möglich!

20.04.2019 17:37 Uhr

## Mutwillige Zerstörung an US-College: 58.000 Dollar Schaden durch USB-Killer

Ein College-Absolvent aus Albany, New York, hat zugegeben, an seiner alten Hochschule 66 Rechner mit einem USB-Killer zerstört zu haben.

Von Dorothee Wiegand

🔊 | 🖨️ | 👤 214

POLICY | US & WORLD | TECH

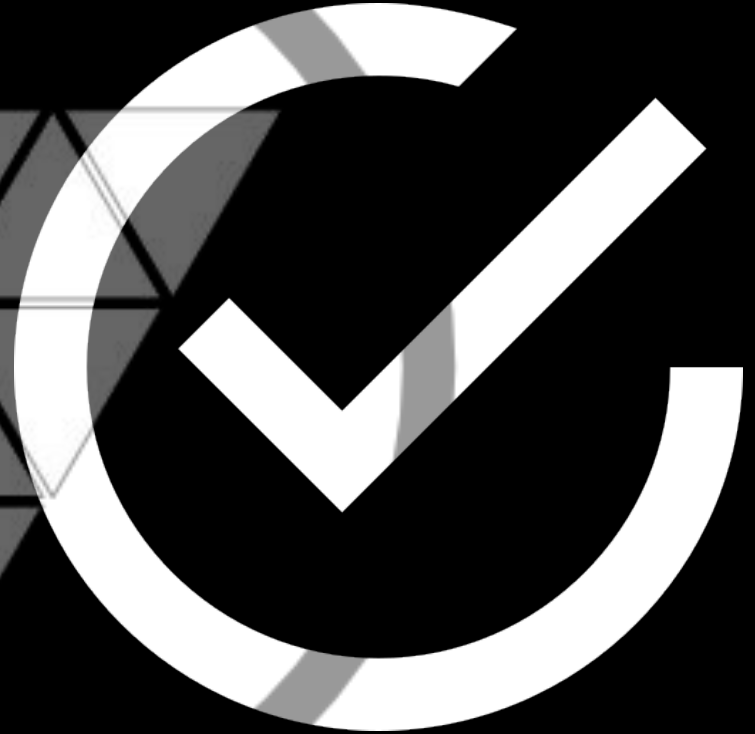
## Student used 'USB Killer' device to destroy \$58,000 worth of college computers

*The former College of Saint Rose student faces up to 10 years in prison*

By [Chris Welch](#) | [@chriswelch](#) | Apr 17, 2019, 3:07pm EDT

## DER 3 SEKUNDEN BSI-CHECK

1. Ist der Betreff sinnvoll?
2. Kenne ich den Absender?
3. Erwarte ich einen Anhang?



Wie kann man sich schützen?

## #Grundsätzliches



### Vorsicht bei E-Mail Anhängen!

Insbesondere bei ZIP-Dateien und Office Dokumenten (Vorsicht - Makros!)



### Software auf allen Geräten aktuell halten!

Schwachstellen werden geschlossen, neue Sicherheitsmechanismen ermöglicht und freigeschaltet

# WARNING



### Legen Sie Backups an!

Egal ob von Ihren virtuellen Maschinen und Daten.



### Schulen Sie sich regelmäßig!

Newsletter, Securitynews, Tagesschau, Websites, Blogs, Twitter, Facebook, RSS Reader ..

WannaCry/Emotet/Petya Vorfälle:  
"Kein Backup, kein Mitleid"

## Cyberpflege - Lösch meinen Account

Wir zeigen Dir, wie Du dich bei Diensten und in Apps abmeldest.

Suche mit den Anfangsbuchstaben des Dienstes den du suchst:

Einfach

Schwer

Reset

CYBERPFLEGE.de teilt die Möglichkeiten der Abmeldung, **vor** der Anmeldung, mit:

- besteht die Möglichkeit seinen Account zu löschen?
- mit welchem Aufwand habe ich zu rechnen?
- wo ist die Abmeldefunktion der Plattform versteckt?

# VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Sie interessieren sich für das Thema & wollen informiert bleiben?

<https://aware7.de>

Blog, Podcast, Termine, Events, Videos & weitere Informationen



## Security to go

<https://aware7.de/go/vortrag/>

- Neueste Blogbeiträge
- Exklusive Inhalte
- Warnmeldungen

**Verständlich. Praxisnah. Präventiv**



Facebook

<https://aware7.de/go/facebook/>



Instagram

aware.seven

<https://aware7.de/go/instagram/>