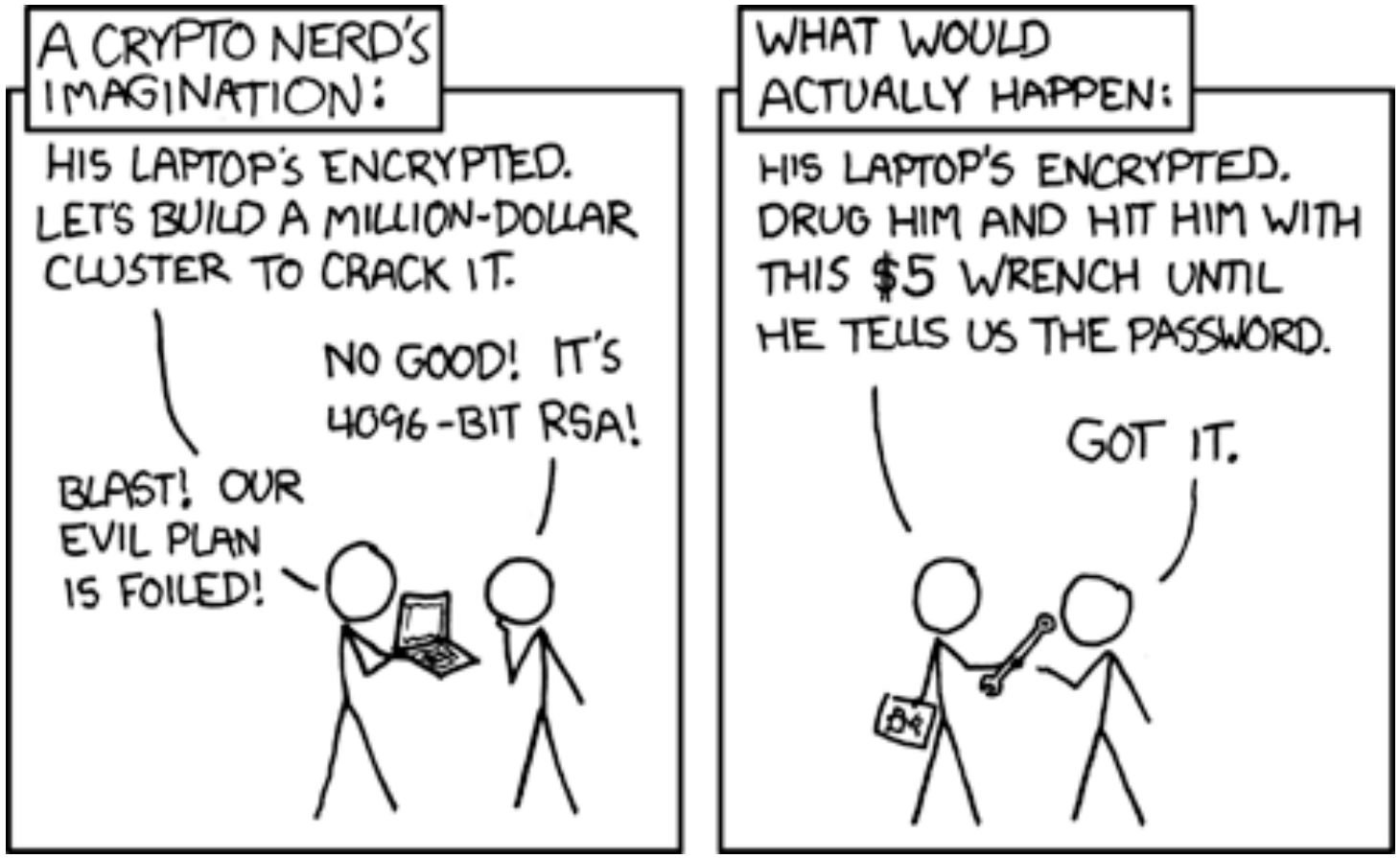
Usable Security: Die unendliche Geschichte

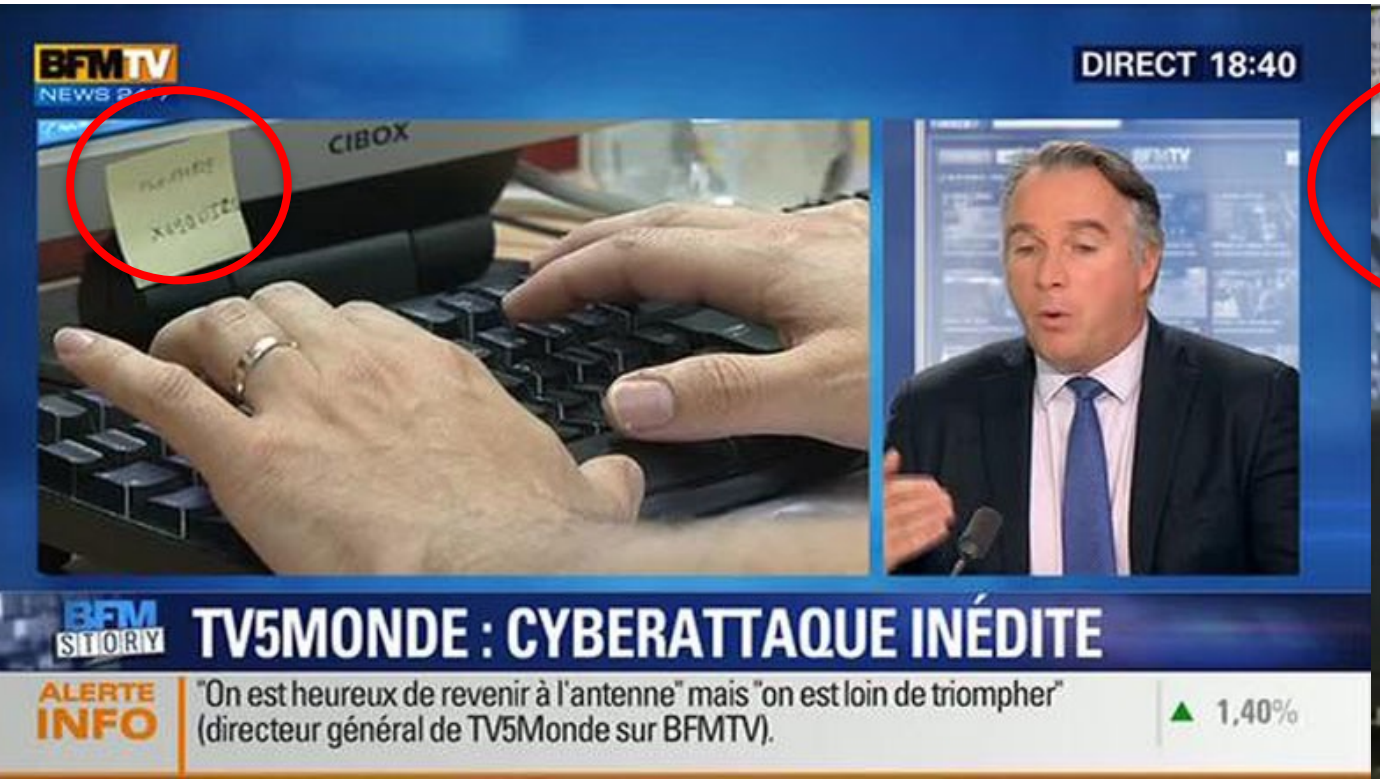
Matthias Fassl

Was ist Usable Security?

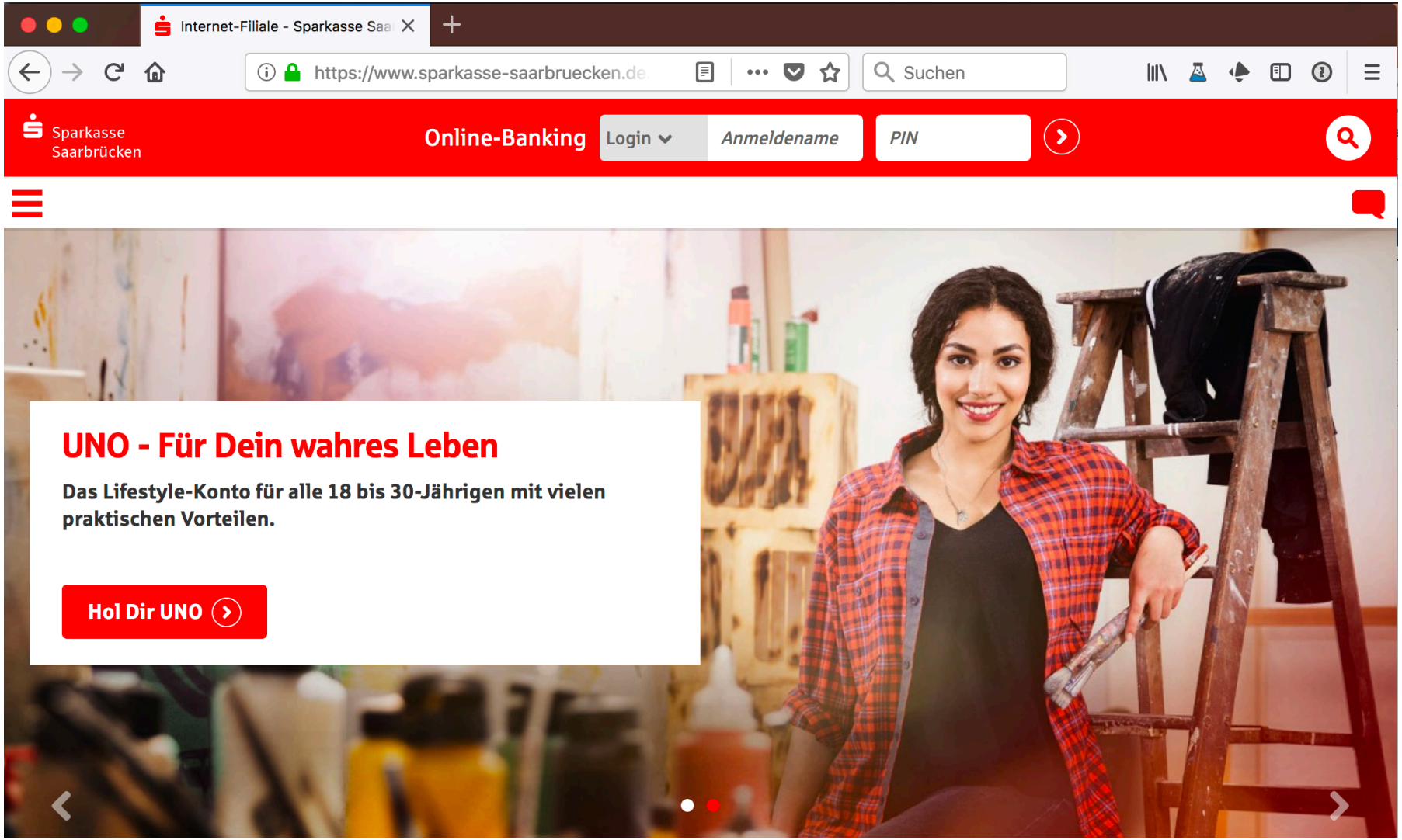


https://xkcd.com/538/

TV5 Monde Hack



HTTPS


Internet-Filiale - Sparkasse Saa
https://www.sparkasse-saarbruecken.de
Suchen
Sparkasse Saarbrücken
Online-Banking
Login
Anmeldename
PIN
UNO - Für Dein wahres Leben
Das Lifestyle-Konto für alle 18 bis 30-Jährigen mit vielen praktischen Vorteilen.
Hol Dir UNO

PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
Comment: GPGTools - https://gpgtools.org

mQINBFOYvycBEAC0nINy8Ziq1cySbuWQfvdmXW3kb3Pv6uQmfAifsHQhV/fAfSDp
ZjaKSnPDO9OB4RzXKgX3iFi8tBivoM+JhD/9C43K55kGYN+HRjIXUvne1IOIF4dZ
lUaWWWwGUNaPZ1jtT1RR+Dy54B42ehhnuJpeeEV4iUWl/Ur3MGZTyrSlE6qEgw7j
tVIX2R3k72K8TX3AH2HgN3X74dN42IeAYCYGzRX/ZuuliTnCmFUjVb9WoIS0TopE
PmdTwmXuaylcyExQmbkC9Oggz95p0Jyve7Dq4GYcgfgl92S/yFu6E8OK/LThDHp2
qBsEoo2bHd3eJR8db1fiQWAlyrd/VE9IbzHSRUkiuroz2zrIEvXsmYqExbevUVvW
lRur9rWZ/CYIgtY7MvBK+YiNRKTHIb5voMDzh1YHBu1vxlkHmTp9QhAIhYOk7eON
cfw1W7M/dnyW6/f1PbaGV90eziIaIcEmbVCNuSZzu3YZmBpFIsK1bXrn4XuCjpyR
z8mRMWo/cfAbXFRnlG/dACLVc5E7sW38wmdNivVpDdu6+WyR1ACcUGvIzHsBB1CC
R6UAlgCXkFzusjMpcep8RPBRCWcy1YQbjtZQBWHivhtlWI4QRAYHcHoqR8trwcUH
nkFaCpCPeIcqa2YHYn2r7JUkuoro0AuYZlWFmzdQqsrse3W6n6tUx3IxfQARAQAB
tDFLYXRoYXJpbmEgS3JvbWJob2x6IDxra3JvbWJob2x6QHNiYS1yZXNlYXJjaC5v
cmc+iQI9BBMBCgAnBQJTmL8nAhsDBQkHhh+ABQsJCAcDBRUKCQgLBRYCAwEAAh4B
AheAAAoJELGljvbARE1bW88QAJ4Am8s6kjiEpc7htgQIVUDWp4wrzvQyvYxTcOiv
O/CnPwPCrX4SX3wyhZxb0hWW7GPyn8x3tak3nGAhNNN9TsT3rsC7BRwdEdII1oni
Ve3INOX5mh830D9dT7xfeEa0nqC+OQKk/E4PpE8apb0vkTfRYHJ2+cDEqJ/ZXzaQ
1EmZAbjnok//u+tfbH3bQXOv873Qs2YGHIS8PT5y2+0LLdhaNj/rgw5S4TPMNF/K
DGetJPDhW6WQZVpQlrHcC01A4Yhm/UrqoUn5EKZrXevmZkLOUUroHMBXTe1ADSDA
pOdhz1d3ANw5IrLbtk+trK3cBkwg9k60wMdN2yco/VdYOavcSM8+gAPkVXZF4P26
IJZvsjIdNfJDSqIol5x7XI4KyTk77tewyQg7nItz7LDgcvZmyLpxGqyjEUTbaanB
rdZHLj39aFTbvDeDRXLa+H4hyw0vvWQakI9TQYb23K/5bhKeatIYdXI6RtcW1Sp8
CsbmCL1Mo8ojMn+KsFAVT21GgruJdb8Z4MUv3SWQHjjW9r/6+tygGuAyNrPm/Myg
xDoLaVGbbAzdYt4Zo5tmT7XDo3McwE7tvf8QrVaCjC+IesZNoSKUg7Ik52a7GEK7
sAvVb22LlDokmzQrGaTU5blNK5mUd+KuVKtUVZ57O0RFOhiTE2+kcKN+0nQtsjvF
6yR0uQINBFOYvycBEADJHG98Y8r0Ju/F5gx8gBmVBbkqTGLHnxUW9XmnbnF8pRJf
ksb7has48rhgNTz6O0Wn0JZlI3kKutaVdjR7kcERYKzU38VBco+MtvnBELpGWKs9
oYIU3Y4bC2DR0zHqSy8B4Vq/dMW2q6n9GTDr4wqdIIYbN8oUjXftBNBIp9X5dlRX
0119Guk/zk51YZu0zg084TLIFcOeia3W4OAt9TGfUVu3Ll41Ujv/4r1UO8Idj2P4
nGDFPFhbDzZVPR9EOQHFPaXMM15Rrc2VelVQ19qcsihZgaH3AK5zwdcx1EXUUeEB
PaIPfPlIxDoNjVZovDFGRDYJzNblDYM8a4poSkSpK5Xp4CyomlTpJgqFyM/YM0Rb
ob0dpoSZCtCxBGUCsds5EIBRTygZW2NV8lQf/yy75rWmbG0GugmZRK4kFXr6dFJn
vXtt2EXMuUIOa5bjD+HJrMAK73rsTtjMBnLcx5cEg81KKBS6PzPNQMtAFmcKdHQs
WXW4nyo82S/Z1Q6bbYYcg7wlWeDc262MV8OHE+OOdEE10I1DJlFoAgO+oqaQ1paN
I7uF/2Uvp3A3/OrUV5Vp2GXiOpiDIYQuf5733WzlQPfop2Pw+wkIuFVNsv3w5Uqs
LYAKJEE80tsYQKyHTovUwqRs9pqLKtRmpaEtdV7TSWfftkd6i3JfjCfTnj2GrQAR
AQABiQIlBBgBCgAPBQJTmL8nAhsMBQkHhh+AAAoJELGljvbARE1bl7IP/2c4P5rM
9+bG7to/IKbaOipzgAXi5DPmnuc1QgN99KCAyd++XUdso1DCW85IZl15Qrh+nsEv
e3vBnzgtd2PlU+31lwk5Fu2yQow1HYWa+yh+nk9oZBpi3OW9LiEEOhalJVAAZei1
ORK5GJQ5QN4Cb8OwrF9MIc4Lmb+UnzG2syVxNrElpbSGEy0FUisVs6K55x3gRP8Y
btYiIuxKpJ7wT7pC6O0Be8b1LvCJjUJMvqX1kEi9eE0BXiQ/d7/Vj2piOnVu07z6
qjn5o39jgQkpF9gOmO/SPIQq6c00AZZNijdoO7xGRhCf66icb3E66pdmjhJP4WGG
QTxSbnOUyLQhqi0pr3mVwput8+BGVVaY5egjjMgwCmC5WWoE3z85gUJf/OmT+4so
Uo/uv3Q3xGAvtX/aoOCGsc4496IaNOPNFXSHERb6DH4pZ9Im4HJw8PkZe8Af+8bl
pdxDi5LalIGMQ7jjgvReb047Rxgs4evUVZ/yIEtLd0UzCju92aL5Ac+EjamsIauI
S8h6Rfs/9sQyo0g9u6IFuk4qoLW5HVI0ETq7QuO7MfMtIU+K6NoJ1943lmzgQzR8
FWSO2F5MphJ5oEvG92Ymlwb6JmvehPISvWiBpLWo4SxwlRhh1LBP609Qg/t8hUq0
```

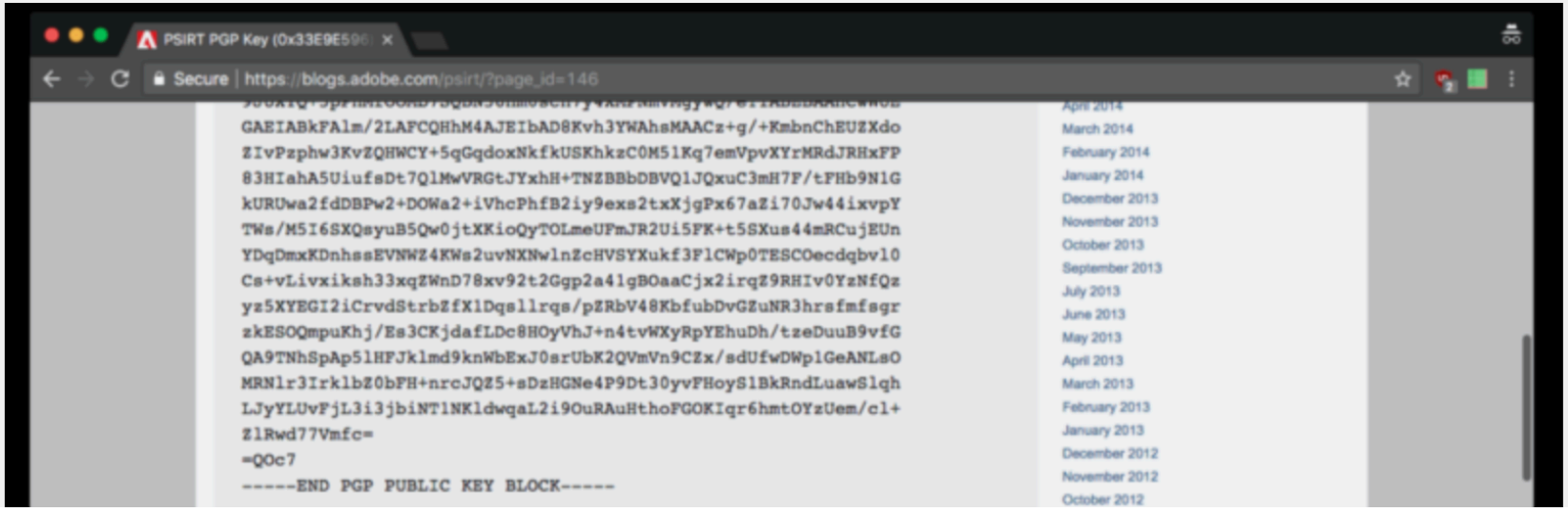
https://arstechnica.com/information-technology/2017/09/in-spectacular-fail-adobe-security-team-posts-private-pgp-key-on-blog/

YOU HAD ONE JOB —

In spectacular fail, Adobe security team posts private PGP key on blog

Since deleted, post gave public *and* private key for Adobe incident response team.

SEAN GALLAGHER - 9/22/2017, 10:37 PM



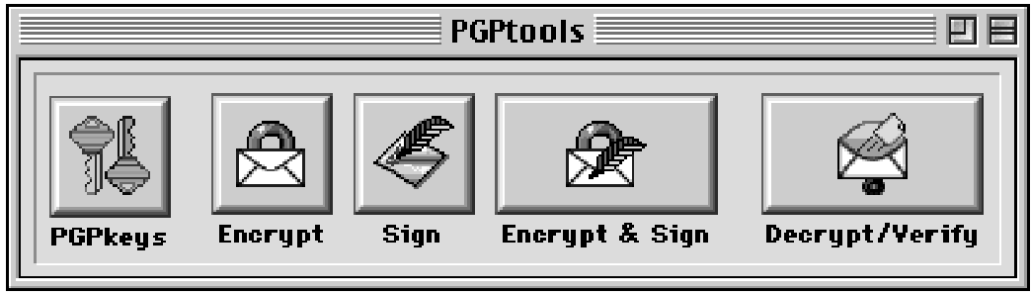
Psychological Acceptability (Saltzer & Schröder, 1975)**:**

It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.

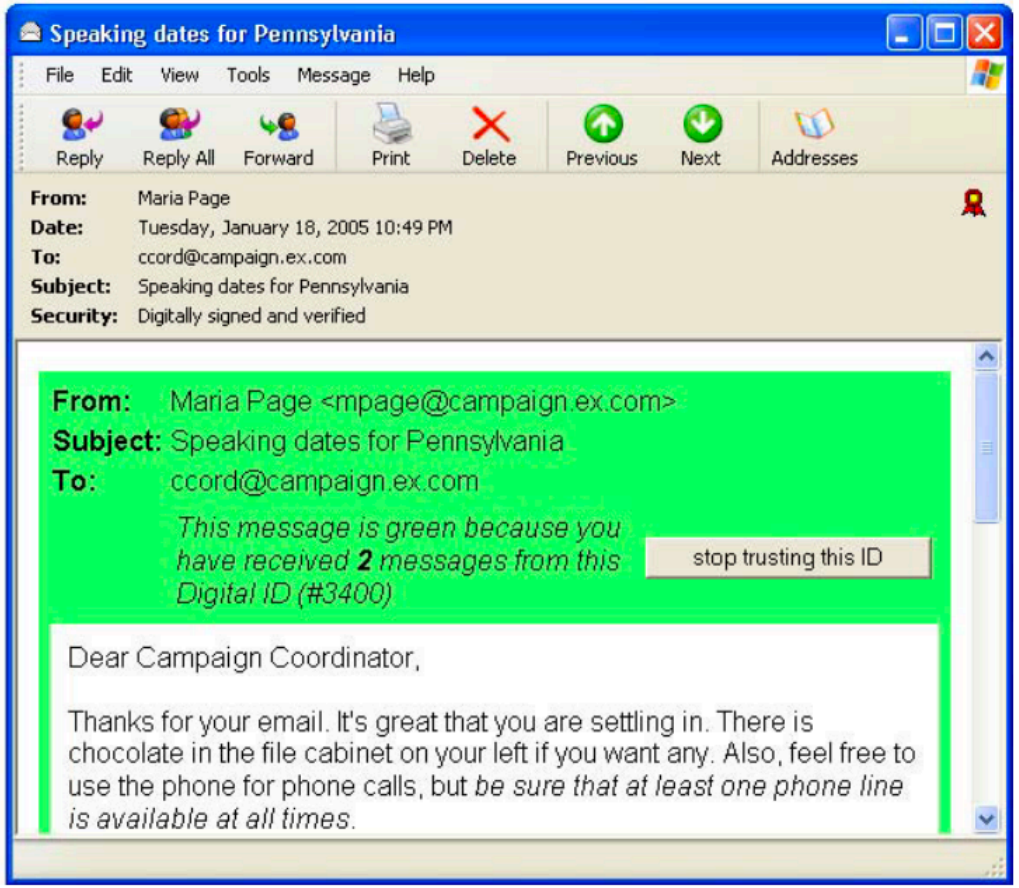
Sichere Kommunikation

Verschlüsselte E-Mail Kommunikation

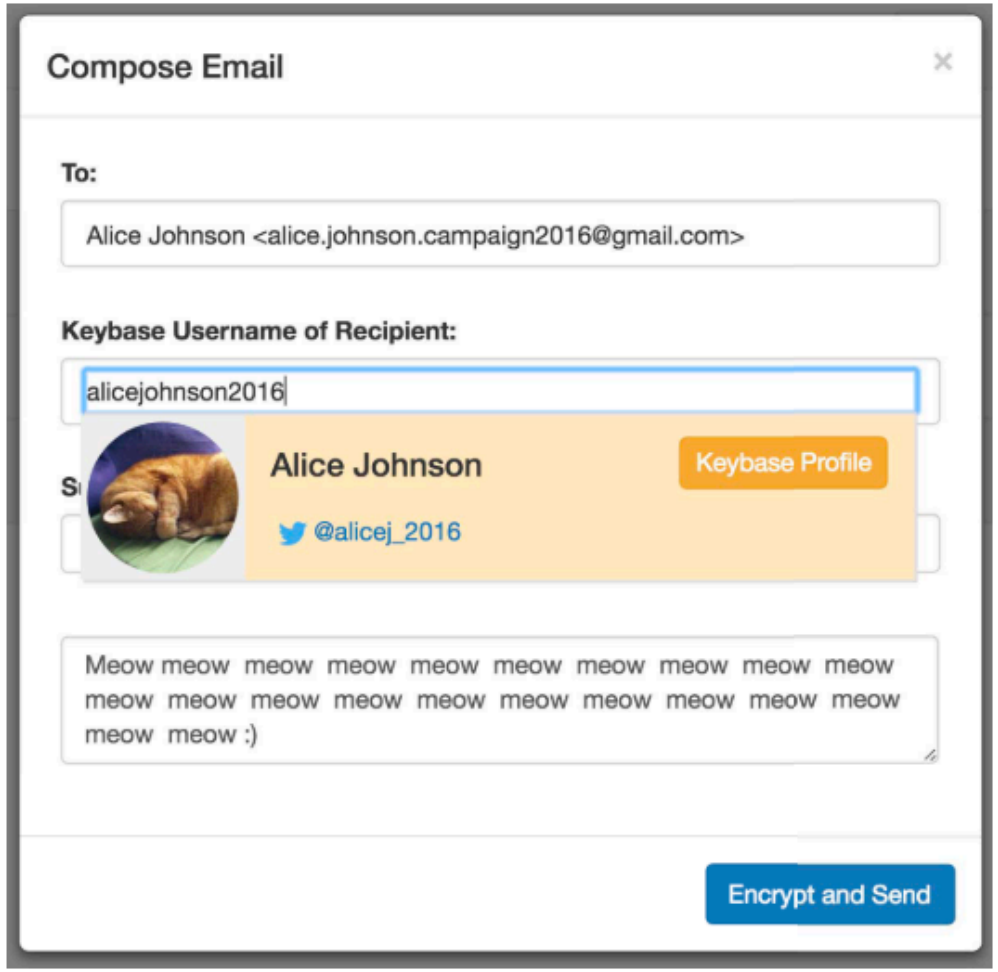
- **Evaluierung der Benutzbarkeit von PGP 5.0** (Whitten & Tygar, 1999)
  - Simulierte Test-Aufgabe: Eine geheime Nachricht an 5 verschiedene Teilnehmer_innen einer Wahlkampagne
  - Eine graphische Oberfläche macht Programme nicht automatisch verwendbar
  - Teilnehmer_innen fehlte ein konzeptionelles Modell von Asymmetrischer Verschlüsselung



Verschlüsselte E-Mail Kommunikation



Key Continuity Management (Garfinkel & Miller, 2005)



Confidante (Lerner, Zeng, und Roesner, 2017)

Verschlüsselte Sofort-Nachrichten

- Benutzerstudie zu OTR (Stedman, Yoshida, und Goldberg, 2008)
  - Automatische Schlüsselerzeugung
  - Automatischer Start der verschlüsselten Unterhaltung
  - Anleitung enthielt Negativ-Beispiele
  - Keine_r der Teilnehmer_innen fand heraus wie die Authentifizierung zu starten ist

Bild aus der damals aktuellen OTR Anleitung zeigt unsicheres Verhalten

Verschlüsselte Sofort-Nachrichten

- **Can Johnny finally encrypt?** (Herzberg & Leibowitz, 2016)
  - 65.2% öffnen keine Secret-Chats in Telegram
  - 56.25% waren sich nicht bewusst das eine Authentifizierungszeremonie notwendig ist
  - 70-90% ist nicht aufgefallen das sich Schlüsselmaterial geändert hat

- **When SIGNAL hits the Fan** (Schröder et al., 2016)
  - 28 Informatik Student_innen
  - MitM Angriff auch eine Konversation im Laborumfeld
  - 7 haben den Schlüssel korrekt verglichen
  - 3 davon wussten was zu tun ist
  - 1 Person erkannte das es ein MitM Angriff sein könnte

Verschlüsselte Sofort-Nachrichten

- **Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols** (Ermoshina, Halpin, und Musiani, 2017)
  - Developer-User Disconnect
  - High-Risk User haben andere Anforderungen und ein anderes Verhalten als Low-Risk User

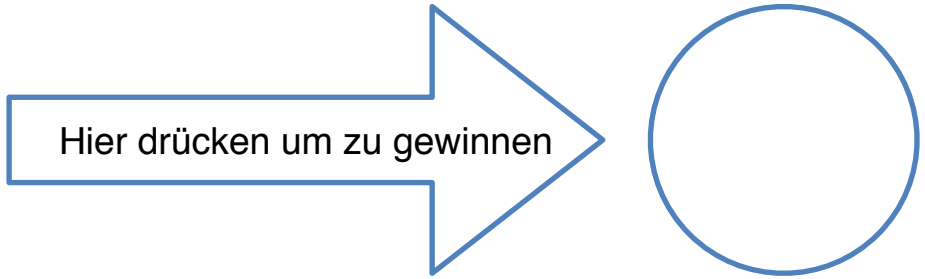
Interview	Developers	Low-risk Users	High-risk Users
Number	15	18	15
Repudiation (Security)	high	low	low
Group Support	high	high	high
Metadata Collection (Privacy)	high	low	high
Decentralization	high	low	low
Standard	high	low	low
Open Licensing	high	low	low

Wichtige und unwichtige Eigenschaften von sicheren Messungen

Usability vs. User Experience

Usability

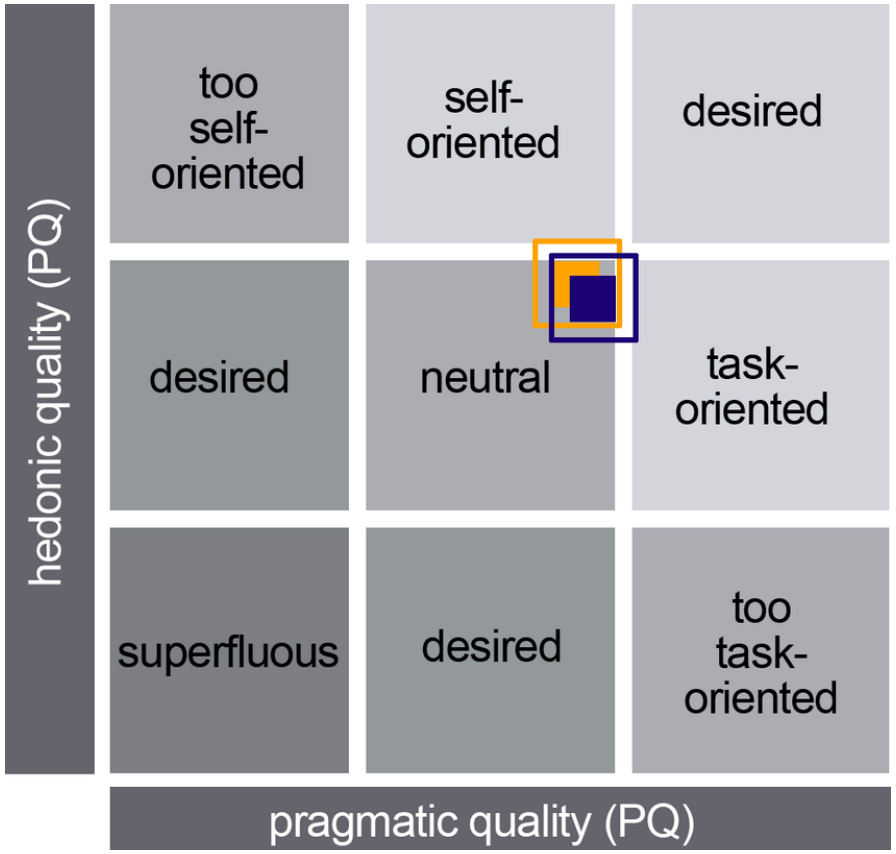
- Wenn Usability Engineers ein Spiel bauen würden:



- Einfach ist nicht immer gut
  - Automatische Schlüsselverwaltung und Verschlüsselung kann das Vertrauen in die Sicherheit senken (Ruoti et al. 2015, Lerner et al. 2017)
  - Sich sicher *fühlen* ist daher eine ebenso wichtige Eigenschaft wie tatsächliche Sicherheit
  - … und hängt nicht unbedingt mit dieser zusammen

User Experience

- Bankomat: Zeitpunkt der Kartenrückgabe vs. Anzeige des Kontostandes
- Hedonic vs. Pragmatic Qualitäten (Hassenzahl, 2010)



(Häusleschmid et al., 2015)

Secure Experiences: „SMS ist das sicherste Medium für Nachrichten“

(Abu-Salma et al., 2017)

1. Telefonprovider sind vom Staat reguliert
2. Banken senden TANs per SMS
3. SMS sind nur über die SMS Applikation am Handy lesbar, E-Mail und IM auch auf PCs
4. E-Mail und IM sind weniger sicher weil sie über das Internet gehen
5. Über E-Mail werden formalere Nachrichten geschickt, und die werden als sicherer wahrgenommen

Mental Models

Die Legende des DAUs

- **The Rational Rejection of Security Advice by Users** (Herley, 2009)

	Direct Costs	Indirect costs (*i.e.* externalities)
Attackers	Gain	Don't Care
Banks	Loss	Reputation
Victim Users	Possible Loss	Clean-up Effort
Non-victim Users	None	User Education

Die indirekten Kosten sind oft um ein vielfaches höher als die direkten Kosten

Die Legende des DAUs

- **Folk Models of Home Computer Security** (Wash, 2010)

	Graffiti	*Burglar*	*Big Fish*	*Contractor*
# Subjects	8	13	9	3
Identity of hacker(s)	Young technical geek	Some criminal	Professional criminal hackers	Young technical geek
Level of organization	Solo, or to impress friends	Unspecified	Part of a criminal organization	Solo, but a contractor for criminals
Reason for break-ins	Cause mischief	Look for financial and personal information	Look for financial and personal information	Look for financial and personal information
Effects of break-ins	Lots of computer problems; requires reinstall	Possible harm to computer; exposure of personal information	No harm to computer; exposure of personal information	Exposure of personal information
Target(s)	Anyone; doesn't matter	Opportunistic; could be me	Not me; only looking for rich or important people	Not me; looking for large databases of info
Am I a target?	Possibly	Possibly	No	No

Die mentalen Modelle von „Hacker“ und deren Auswirkungen auf das Security Verhalten

- Mentale Modelle sind allerdings schwierig zu ändern, im Idealfall sollte das vorhandene mentale Modell zur richtigen Sicherheitsaktion führen.

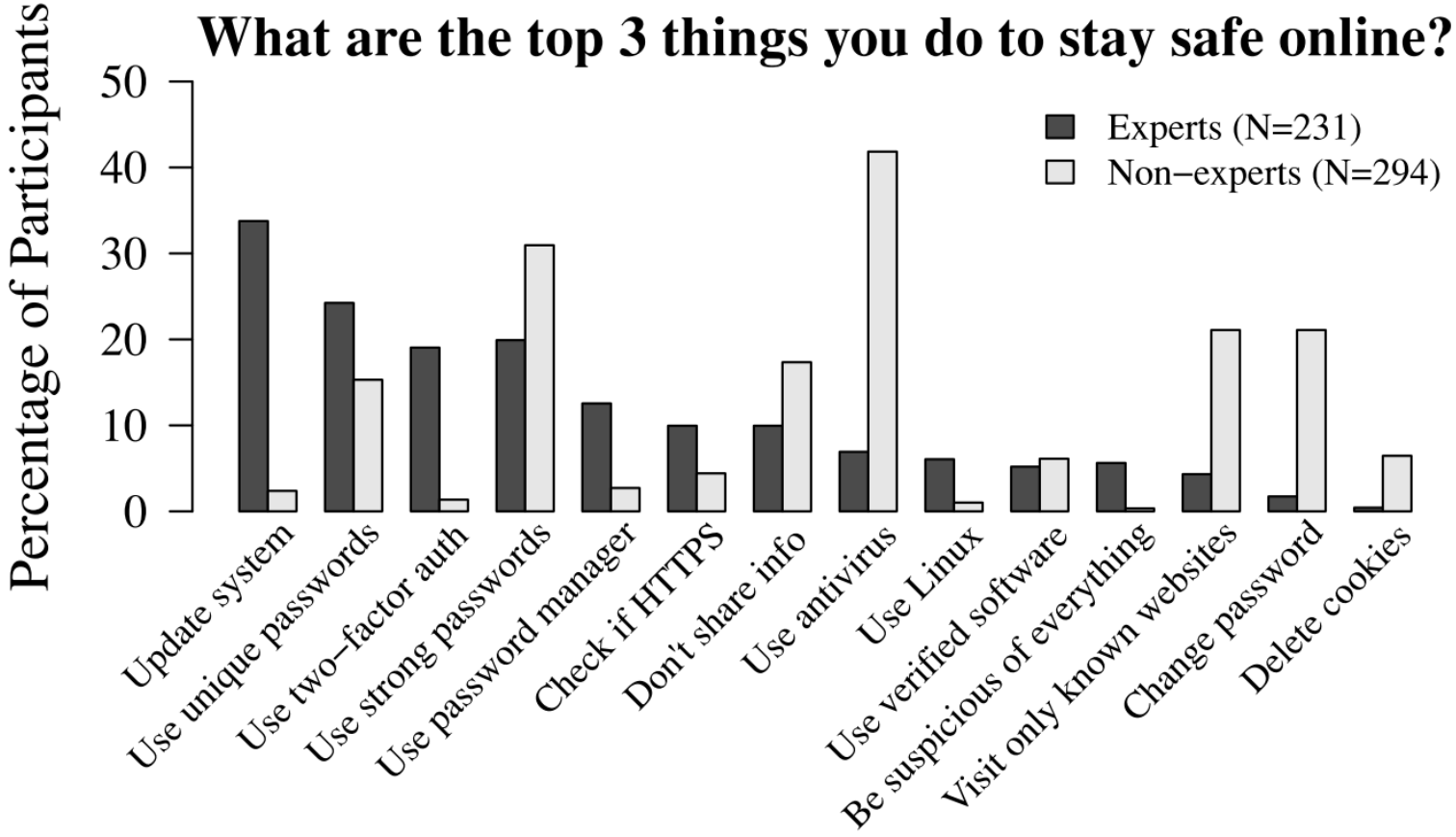
Die Legende des DAUs

- **Expert and Non-Expert Attitudes towards (Secure) Instant Messaging** (Luca et al., 2016)

> *„Despite experts showing a much higher level of understanding of technical details and possible threats, (voluntarily conducted) insecure behaviour exhibited by the participants in our study was roughly identical across both groups.“*

Was können User für ihre Sicherheit tun?

Security Tipps für End-User



"... no one can hack my mind": Comparing Expert and Non-Expert Security Practices (Ion, Reeder, und Consolvo, 2015)

Matthias Fassl

fassl@cispa.saarland

+49 681 302 70782