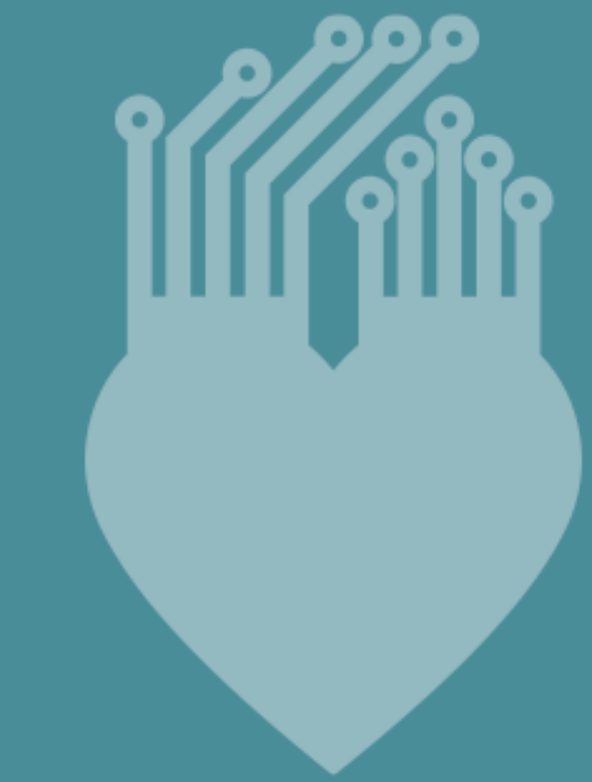
Dr. med. Christina Czeschik
Serapion | Technisches Marketing
www.serapion.de



Usable Security & der Wissensfluch

Forschungstag IT-Sicherheit NRW
26.06.2017, Hagen

Quelle: http://glenngreenwald.net/

In Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 169-183

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of Californi
Berkeley, CA 94720
tygar@cs.berkeley.edu

Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software

Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
shengx@cmu.edu

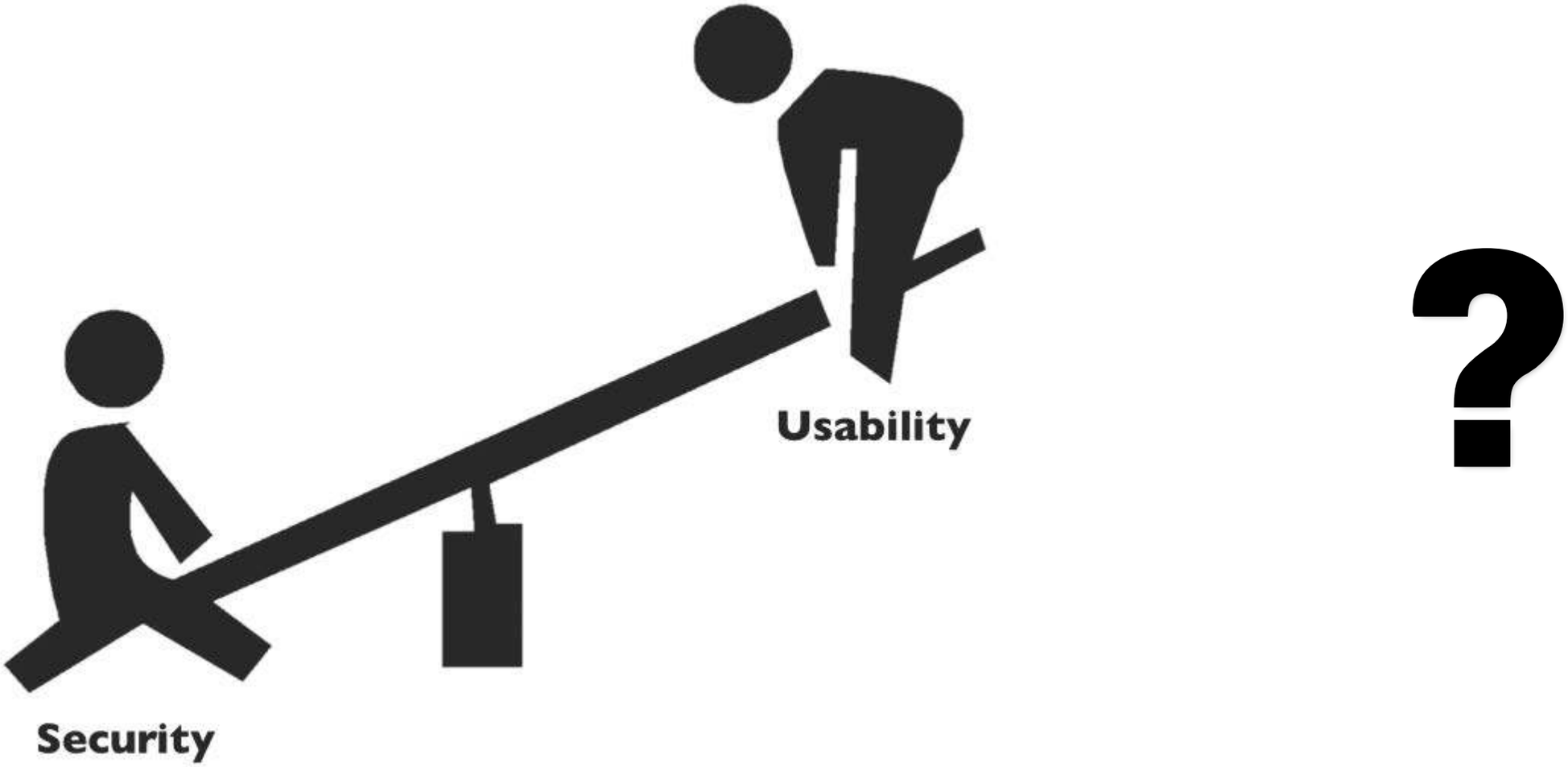
Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
lpb@ece.cmu.edu

Colleen Alison Koranda
HCI Institute
Carnegie Mellon University
ckoranda@andrew.cmu.edu

Jeremy J. Hyland
Heinz School of Public Policy and Management
Carnegie Mellon University

Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu



Quelle: https://blog.surf.nl/surfconext-rich-clients/

Quelle: http://www.failfunnies.com/31/pages/keep-closed-fail.html

The more secure you make something, the less secure it becomes.

Why?

Because when security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security.

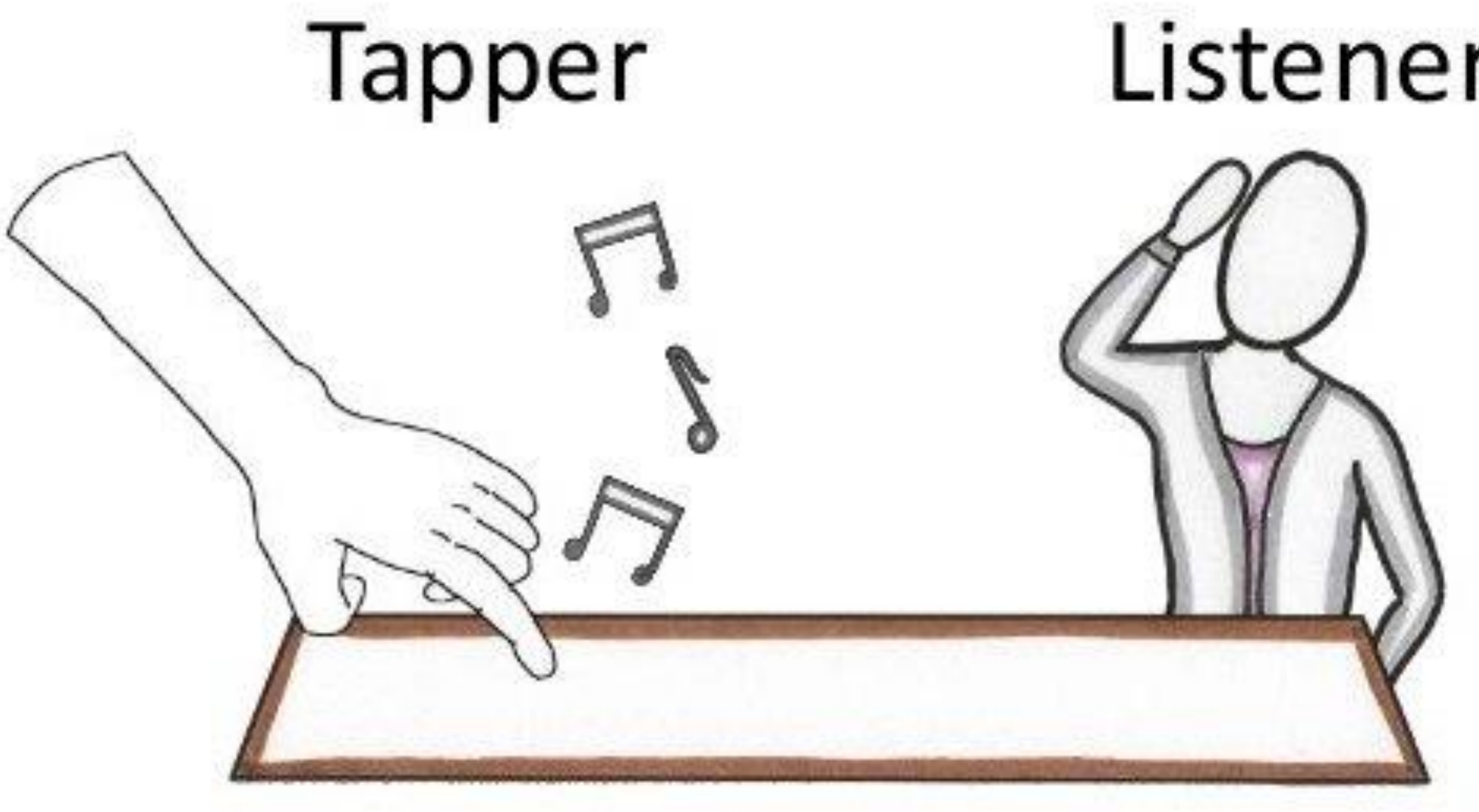
(Don Norman)

Quelle: http://www.jnd.org/dn.mss/when_security_gets_in_the_way.html

The more usable you make something, the more secure it becomes.

Der Wissensfluch

Der Wissensfluch: "Klopfer" vs. "Zuhörer"



Quelle: https://www.linkedin.com/pulse/tappers-listeners-syndrome-kesavan-m

Der Wissensfluch: "Klopfer" vs. "Zuhörer"

Quelle: https://www.linkedin.com/pulse/story-communication-tappers-listeners-dr-biz

Der Wissensfluch: "Klopfer" vs. "Zuhörer"

Fazit:

Es ist für jemanden mit einem bestimmten Vorwissen **extrem schwierig**, willentlich eine naive Haltung einzunehmen.

Oder auch: Sich in den Kopf von jemandem zu versetzen, der dieses Vorwissen nicht hat.

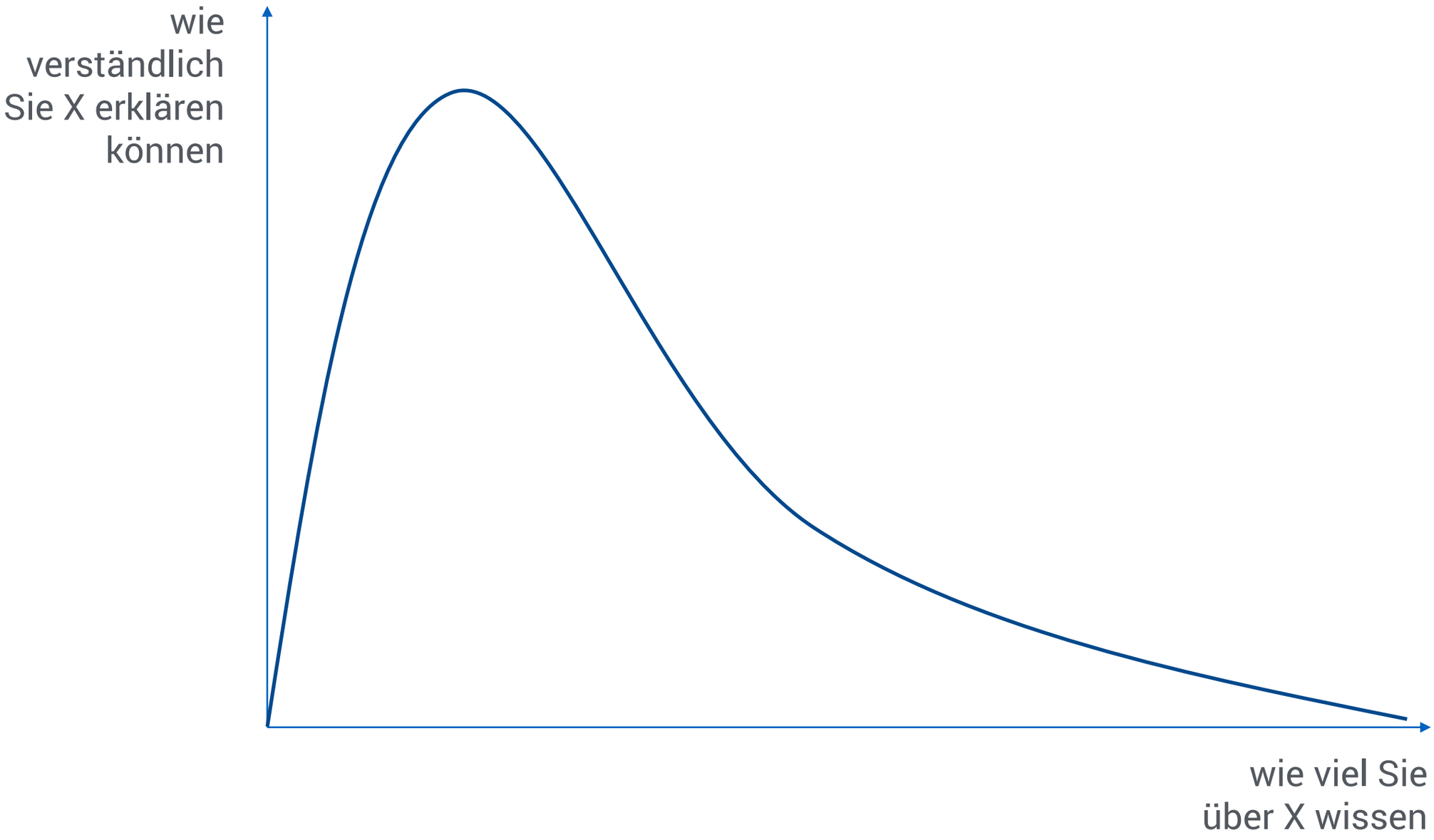
Der Wissensfluch: "Klopfer" vs. "Zuhörer"

"In the **beginner's mind**, there are many possibilities,

in the expert's mind, there are few."

Quelle: Shunryu Suzuki

Der Wissensfluch



Der Wissensfluch: Ursachen

Der Wissensfluch: Kognitive Ursachen

Bündelung & Abstraktion
("Chunking")

Bündelung & Abstraktion

Ein mathematisches Verschlüsselungsverfahren
+
eine Nachricht
+
ein öffentlicher Schlüssel, mit dem man Text unleserlich macht
+
ein privater Schlüssel, mit dem man diesen Text wieder leserlich macht
(oder umgekehrt bei Signaturen)

= **Public-Key-Kryptographie**

Der Wissensfluch: Kognitive Ursachen

Funktionale Fixierung
("Functional Fixity")

Funktionale Fixierung

Es wird nicht erklärt, wie eine Sache aussieht oder woraus sie besteht, sondern nur, wofür man sie verwendet.

Funktionale Fixierung

"Verwenden Sie **Prüfsummen-Programm**, um festzulegen, welches der eingestellten Prüfsummen-Programme für das Erstellen von Prüfsummendateien verwendet werden soll."

(Erläuterung des Menüpunktes "Prüfsummen-Programm" in einem Programm zur Verwaltung von X.509- und OpenPGP-Zertifikaten)

Der Wissensfluch: Kognitive Ursachen

Wissensfluch im engeren Sinne
("Curse of Knowledge")

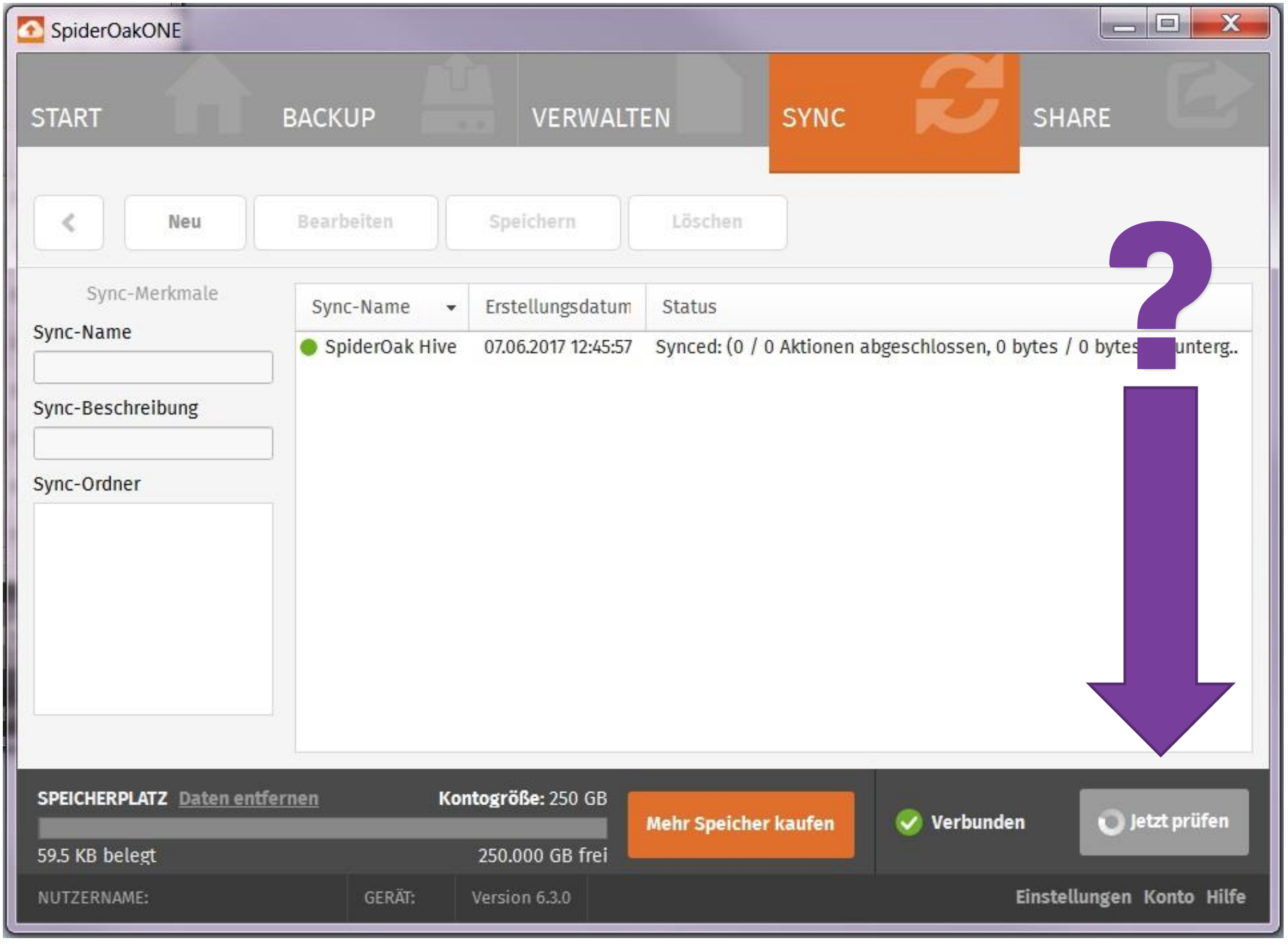
Wissensfluch im engeren Sinne

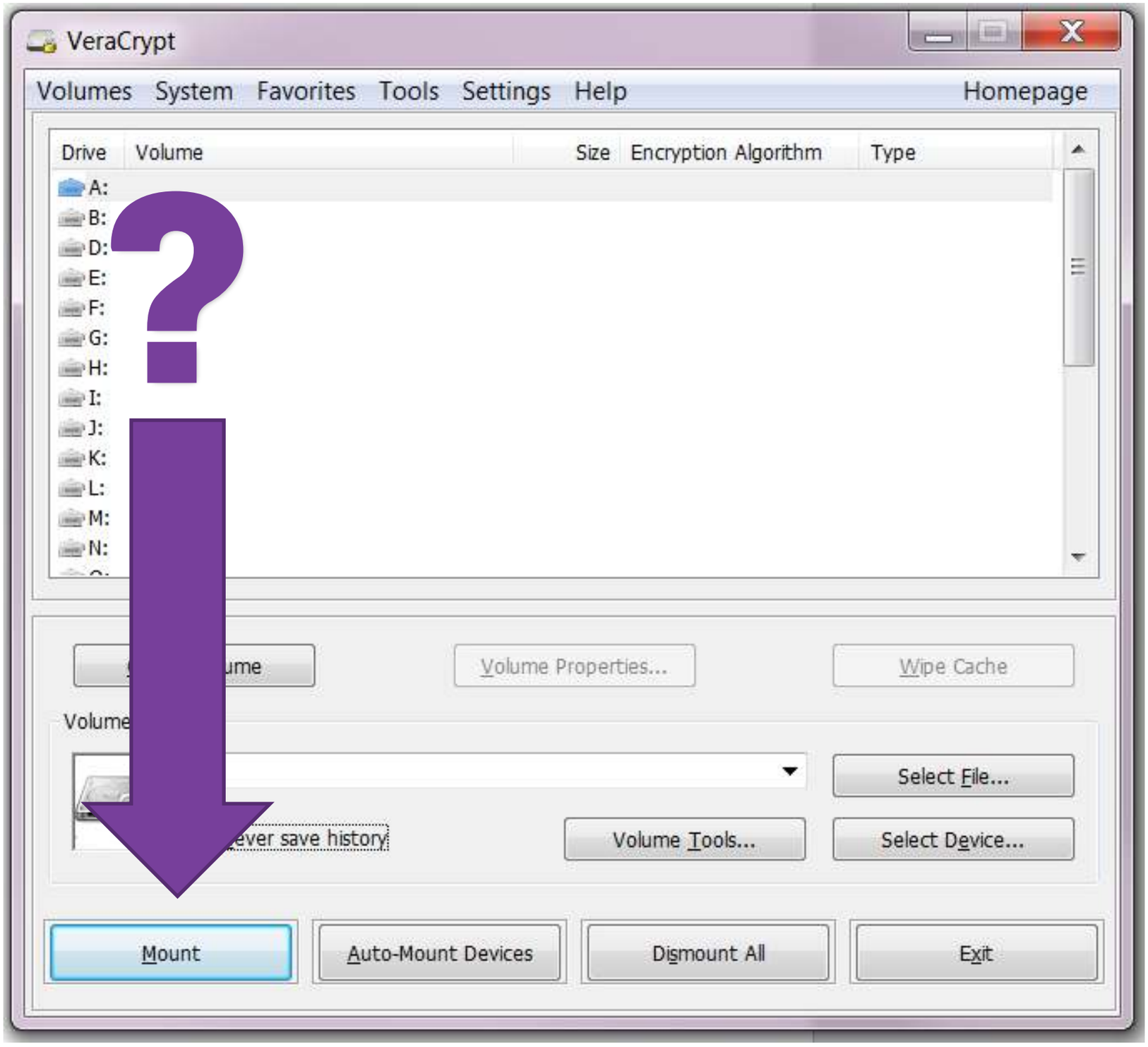
Ein Konzept, ein Wort oder eine Abkürzung werden als bekannt vorausgesetzt.

Zum Beispiel:

"Kleopatra ist das KDE-Programm zum Verwalten von X.509- und OpenPGP-Zertifikaten in GpgSM- und GPG-Schlüsselspeichern, und zum Abfragen von Zertfikaten von LDAP- und anderen Zertifikatsservern."

Der Wissensfluch und Usability


SpiderOakONE
START
BACKUP
VERWALTEN
SYNC
SHARE
Neu
Bearbeiten
Speichern
Löschen
Sync-Merkmale
Sync-Name
Sync-Beschreibung
Sync-Ordner
Sync-Name
Erstellungsdatum
Status
SpiderOak Hive
07.06.2017 12:45:57
Synced: (0 / 0 Aktionen abgeschlossen, 0 bytes / 0 bytes
unterg..
SPEICHERPLATZ
Daten entfernen
Kontogröße: 250 GB
59.5 KB belegt
250.000 GB frei
Mehr Speicher kaufen
Verbunden
Jetzt prüfen
NUTZERNAME:
GERÄT:
Version 6.3.0
Einstellungen
Konto
Hilfe

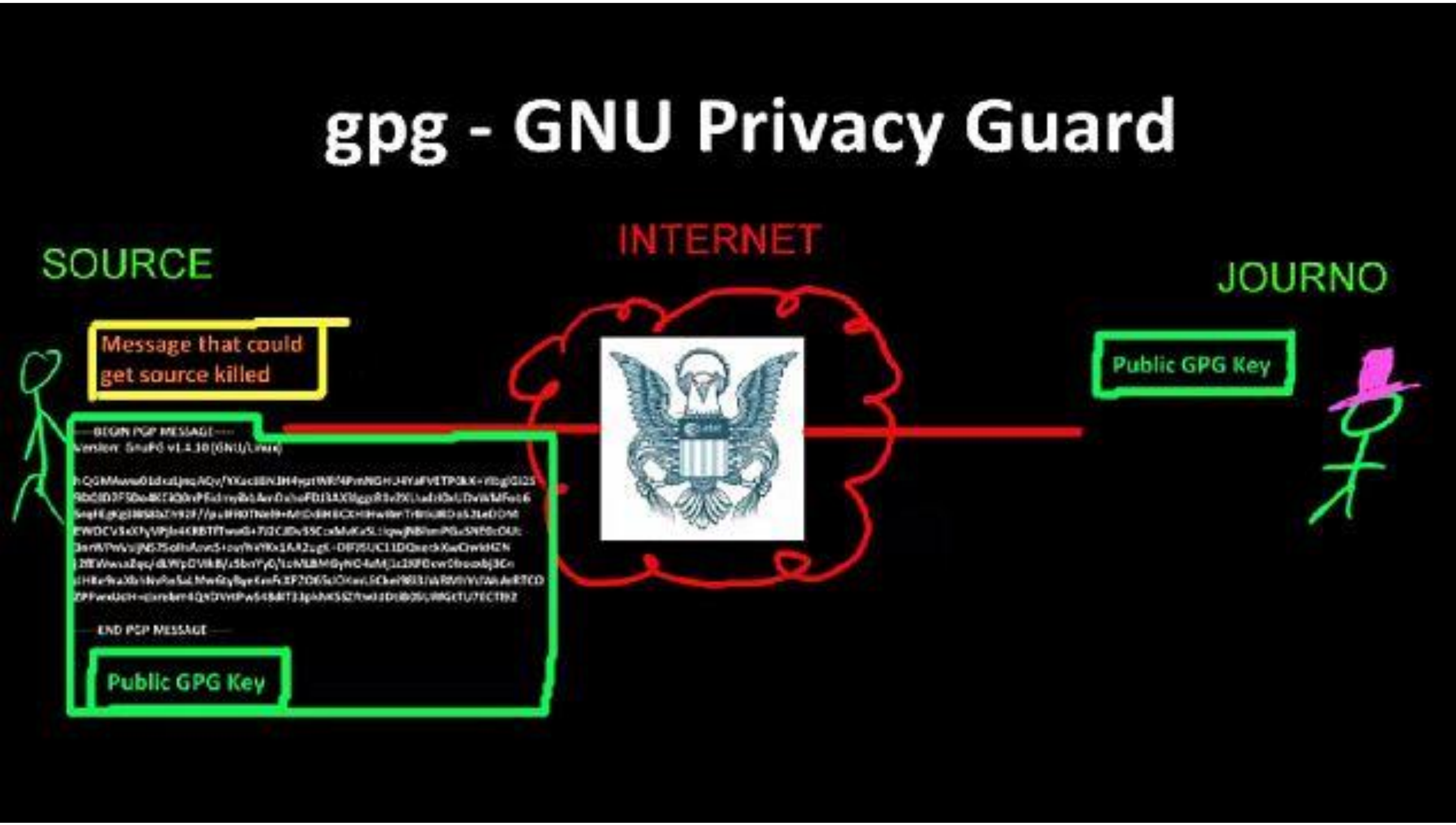

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
D:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Volume Properties...
Wipe Cache
Volume
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit


Gpg4win Installation
Willkommen bei der Installation von Gpg4win
Gpg4win ist ein Installationspaket für Windows zur Nutzung von E-Mail- und Datei-Verschlüsselung unter Verwendung der Kernkomponente GnuPG für Windows. Die beiden relevanten kryptographischen Standards OpenPGP und S/MIME werden unterstützt. Gpg4win und die in Gpg4win enthaltene Software sind Freie Software.
Klicken Sie auf Weiter, um fortzufahren.
Dies ist Gpg4win Version 2.3.3
Dateiversion 2.3.3.59409
Releasedatum 2016-08-18
Weiter >

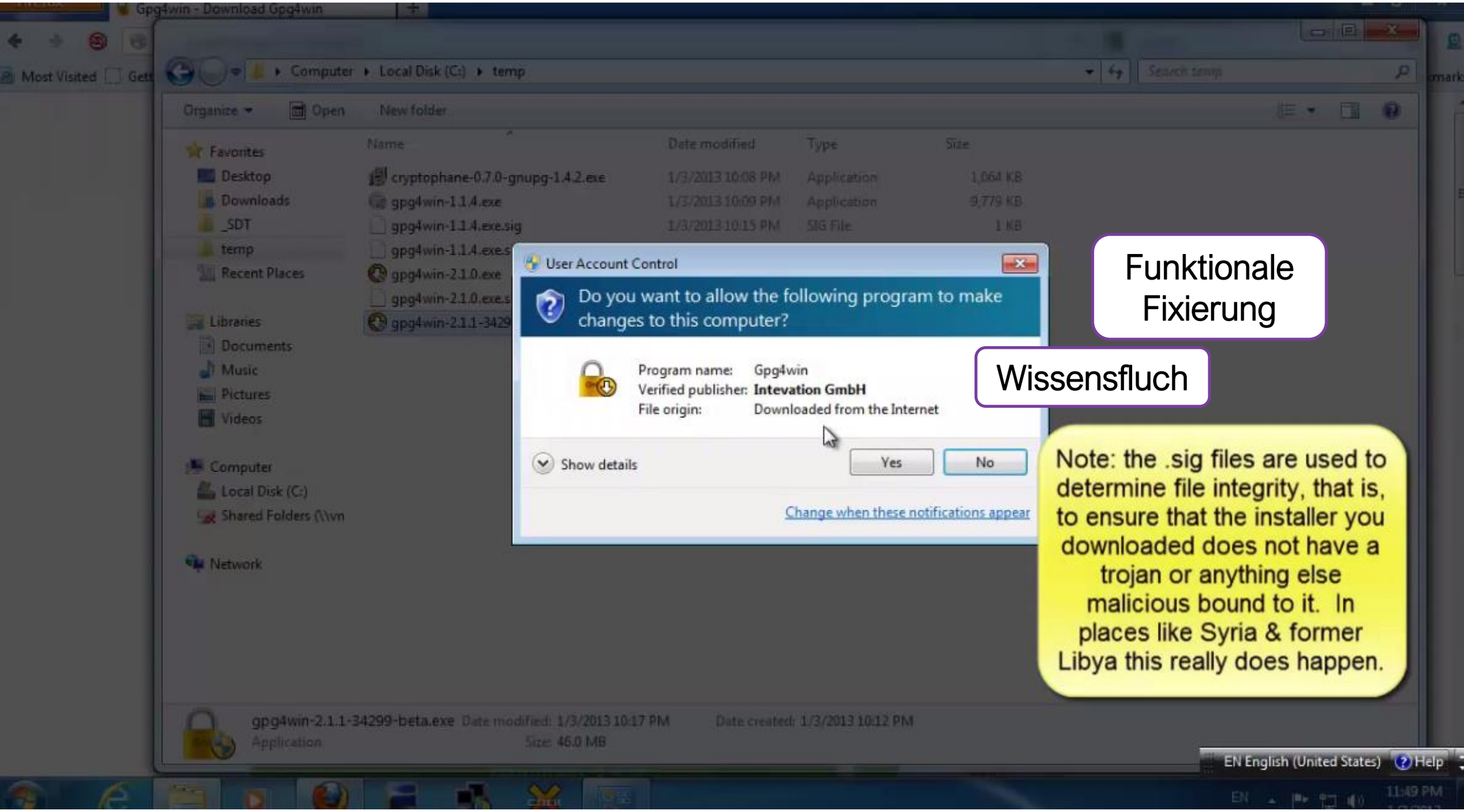

Gpg4win Installation
Komponenten auswählen
Wählen Sie die Komponenten aus, die Sie installieren möchten.
Wählen Sie die Komponenten aus, die Sie installieren möchten und wählen Sie diejenigen ab, die Sie nicht installieren wollen. Klicken Sie auf Weiter, um fortzufahren.
Wählen Sie die Komponenten aus, die Sie installieren möchten:
GnuPG
Kleopatra
GPA
GpgOL
GpgEX
Gpg4win-Kompendiun
Beschreibung
Benötigter Speicher: 95.2MB
Gpg4win-2.3.3
< Zurück
Weiter >
Abbrechen

Quelle: http://glenngreenwald.net/

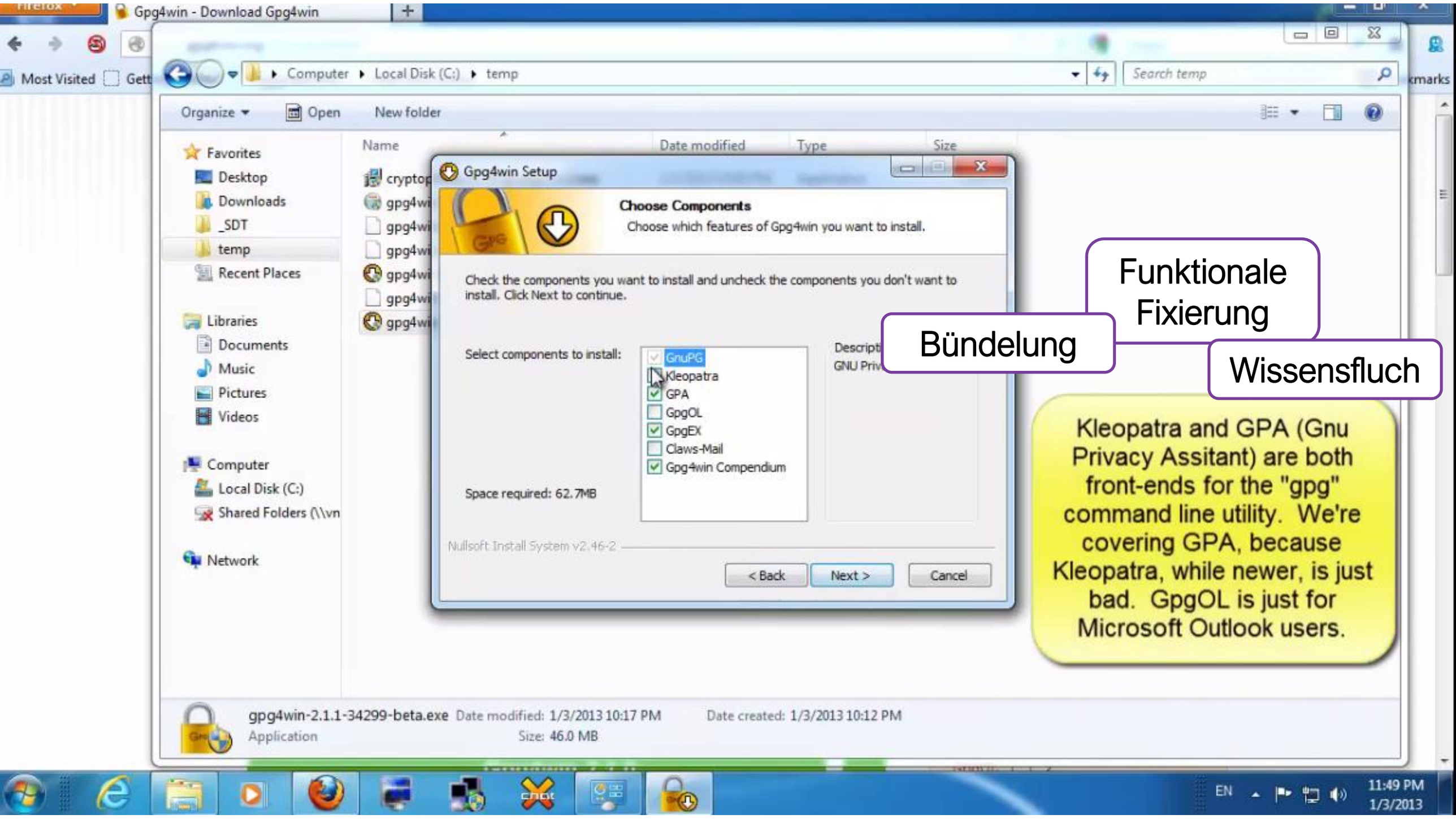
gpg - GNU Privacy Guard



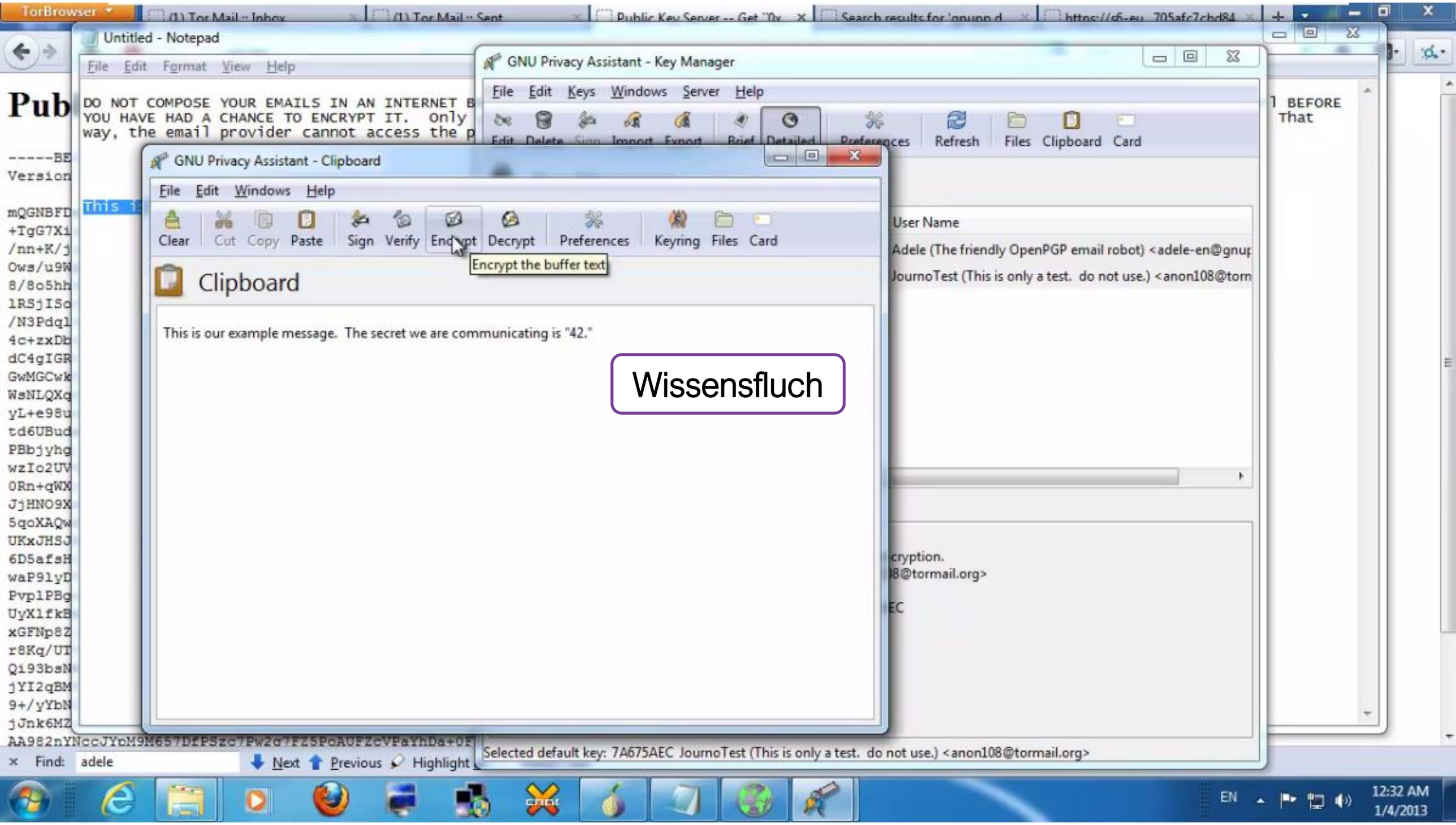
Quelle: https://vimeo.com/56881481



Quelle: https://vimeo.com/56881481



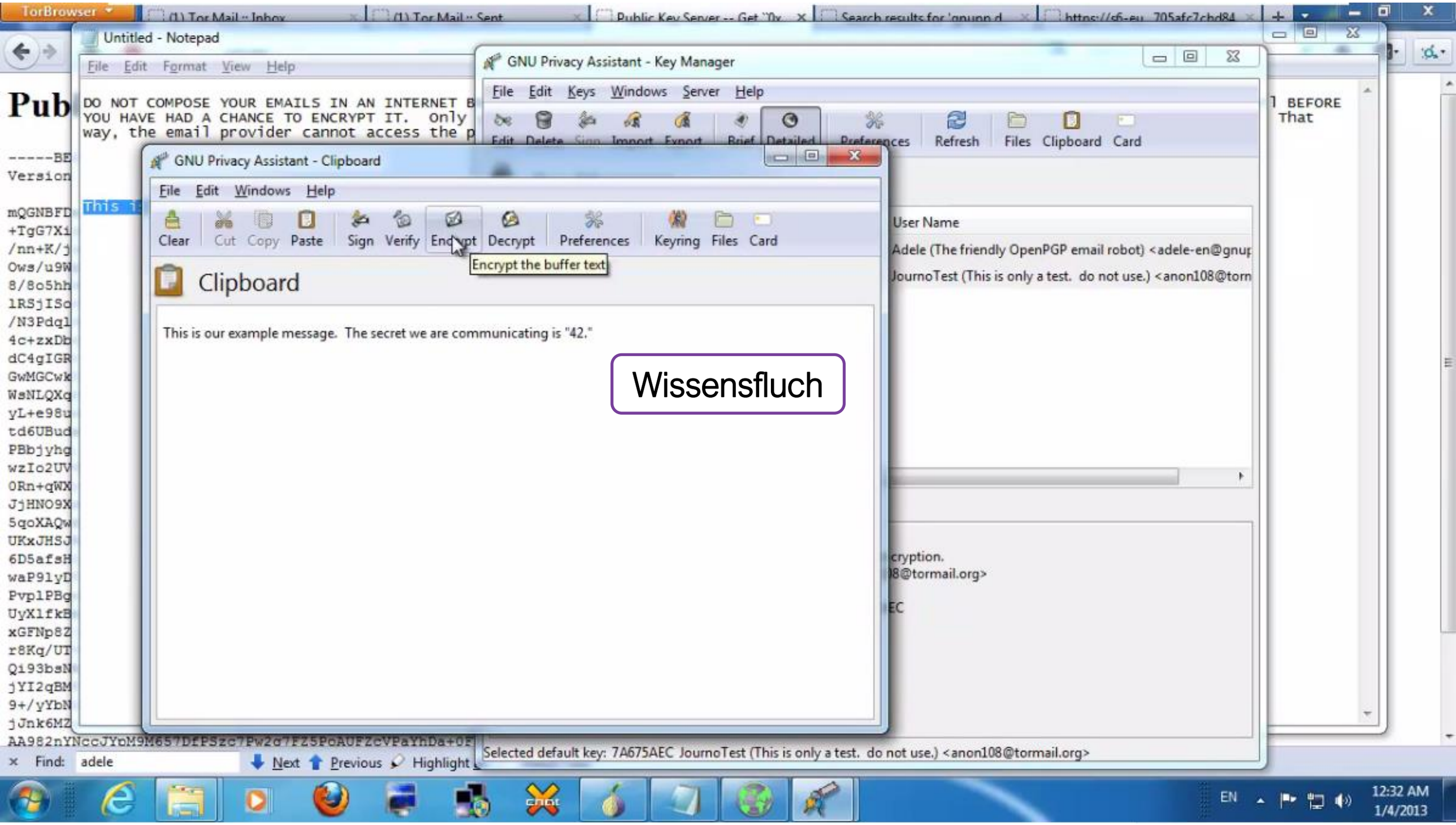
Quelle: https://vimeo.com/56881481



Wissensfluch

Quelle: https://vimeo.com/56881481

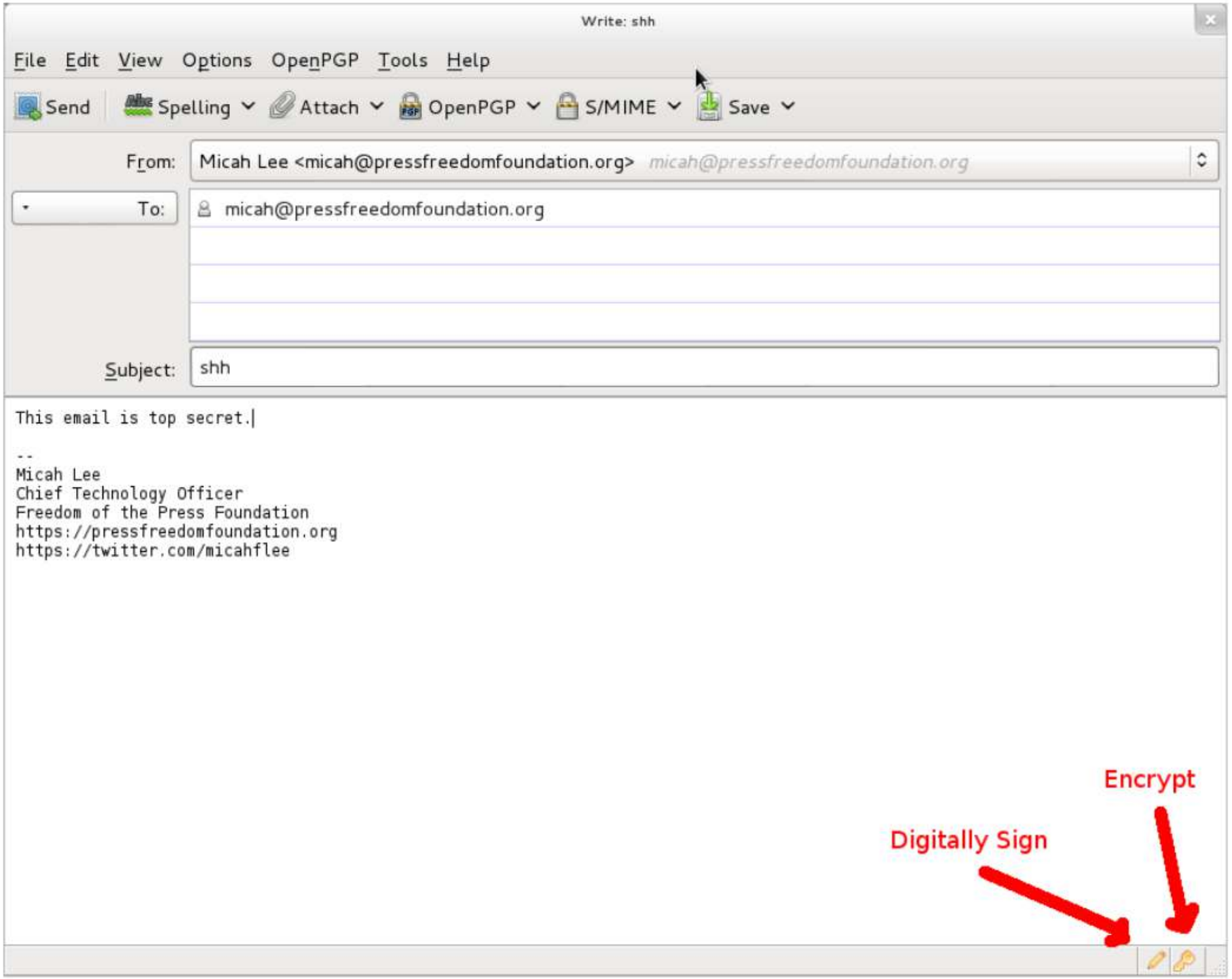
Quelle: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/



Wissensfluch

Quelle: https://vimeo.com/56881481

Wissensfluch umschifft



Quelle: https://wiki.piratenpartei.de/wiki/images/3/33/Encryption_Works_-_by_Micah_Lee.pdf

Gegenmittel?

Mittel gegen den Wissensfluch

Testen an

- echten Usern,
- neuen Mitarbeitern,
- sich selber, sobald man 6 Monate aus einem Thema raus ist.

(Und dann: Noch mehr testen!)

Mittel gegen den Wissensfluch

- Konkret sein und Details zeigen.
- Vor allem: Beispiele!

Verständlichkeitsforschung hat gezeigt:

Wenn abstrakte Erklärungen und ein Beispiel geliefert werden und beide widersprechen sich, dann folgen die meisten User dem Beispiel.

Mittel gegen den Wissensfluch

- Keine Angst davor, einen Sachverhalt auf "zu" niedrigem Niveau zu erklären.

- Selbst wenn die meisten Nutzer ein Konzept schon kennen:

"[…] there are babies being born every minute who will someday encounter the name for the first time."

(Strunk & White, 1979)

Danke für Ihre Aufmerksamkeit!

Dr. med. Christina Czeschik, M.Sc.
Ärztin für Medizinische Informatik
Serapion | Technisches Marketing
Herkulesstr. 3-7
45127 Essen

czeschik@serapion.de
www.serapion.de/usable-security-zusatzmaterial

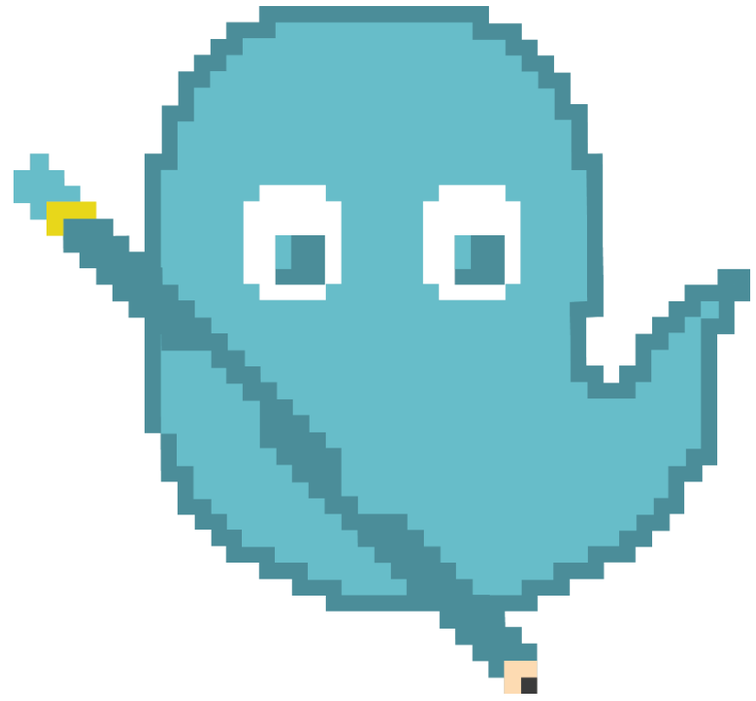
@serapionblog

Serapion | Technisches Marketing

www.serapion.de

Wir erklären IT-Sicherheit.

- Fachartikel
- Broschüren
- Blogbeiträge
- Tutorials
- Pressemitteilungen
- …



Neu: INTELLICORE PRESS www.intellicore.press