ETH zürich

Identitätsdiebstahl und «digitale Sorglosigkeit» – Wie kann man sich schützen?

Prof. em. Dr. Bernhard Plattner, ETH Zürich

Emeritenstamm ETH Zürich, 28. Januar 2019

Definition Identity Theft

- Aus Merriam-Webster

Simple Definition of IDENTITY THEFT

: the illegal use of someone else's personal identifying information (such as a Social Security number) in order to get money or credit

Erweiterte Definitionen aus Wikipedia

- *Identity cloning and concealment*
  - Verwendung von persönlicher Information über eine andere Person, um sich für diese auszugeben
- *Criminal identity theft*
  - Vermeidung einer Strafverfolgung durch Vorspiegeln einer anderen Identität
- *Synthetic identity theft*
  - Fabrizierte Identität, z.B. echte Pass-/Social Security Number mit Information über eine andere Person
- *Medical identity theft*
  - Erlangen von medizinischer Unterstützung im Namen einer anderen Person
- *Child identity theft*
  - Verwendung der Social Security Number eines Kindes, um sich zu bereichern (Zugang zu staatlicher Unterstützung, Kredite)
- *Financial identity theft*
  - Missbräuchliche Verwendung von Kreditkartendaten
  - Eindringen in e-banking Systeme oder Vorgänge

Szenarien

- Meine Identität wurde mir gestohlen
  - Ich selbst bin Opfer einer Folgeaktion
  - Dritte sind Opfer (z.B. Familie oder Freunde, Geschäftspartner)
- Meine Identität wurde Dritten gestohlen
  - Ich bin das Opfer
  - Weitere Dritte sind Opfer (z.B. Familie oder Freunde, Geschäftspartner)
- Die Identität einer dritten Person wurde gestohlen
  - Ich bin das Opfer
  - Weitere Dritte sind Opfer

Beispiel 1: US Tax Refund Fraud

- US Social Security Number (SSN): Ohne sie existiert man in den USA nicht
- Tax Fraud
  - Betrüger fordert zu viel bezahlte Steuern im Namen von Steuerpflichtigen zurück
  - Benötigt: Einige Hundert Social Security Numbers
  - SSN und Geburtsdatum genügt für das Ausfüllen eines Tax Return Forms; Name des Steuerzahlers nicht notwendig
  - Formular für die Rückerstattung zeitlich vor dem legitimen Steuerzahler einreichen
  - IRS zahlt mit Check oder Überweisung auf eine Debit Card (mobiles Bankkonto)
- 2.7 Mio frühere Opfer des Betrugs in erhielten 2015 einen 6-stelligen PIN für 2016. Diesen konnte man jedoch im Internet auch mit der Antwort auf vier einfache Fragen erhalten (!).
- 297’000 Fälle in 2015, 100’000 Fälle in 2017

Offenbar funktioniert es …

Defendant Sentenced in $19 Million Tax Fraud Conspiracy

On Sept. 26, 2014, in Anchorage, Alaska, Maximo Amparo-Vazquez, aka Japhet Soto Santiago, aka Luis Angel Cortez, a citizen of the Dominican Republic formerly residing in Alaska, was sentenced to 84 months in prison, three years of supervised release and ordered to pay $559,755 in restitution to the IRS. Amparo-Vazquez pleaded guilty on July 2, 2014, to conspiring to defraud the government with respect to claims. According to court documents, from January 2010 to March 2012, Amparo-Vazquez conspired with others to use stolen identities to file income tax returns for the purpose of obtaining fraudulent income tax refunds. The conspirators in the income tax fraud scheme obtained the stolen identities of more than 2,600 individuals, including people's names and social security numbers. Most of these stolen identities were from citizens of Puerto Rico.

Quelle: The United States Attorney's Office, District of Alaska

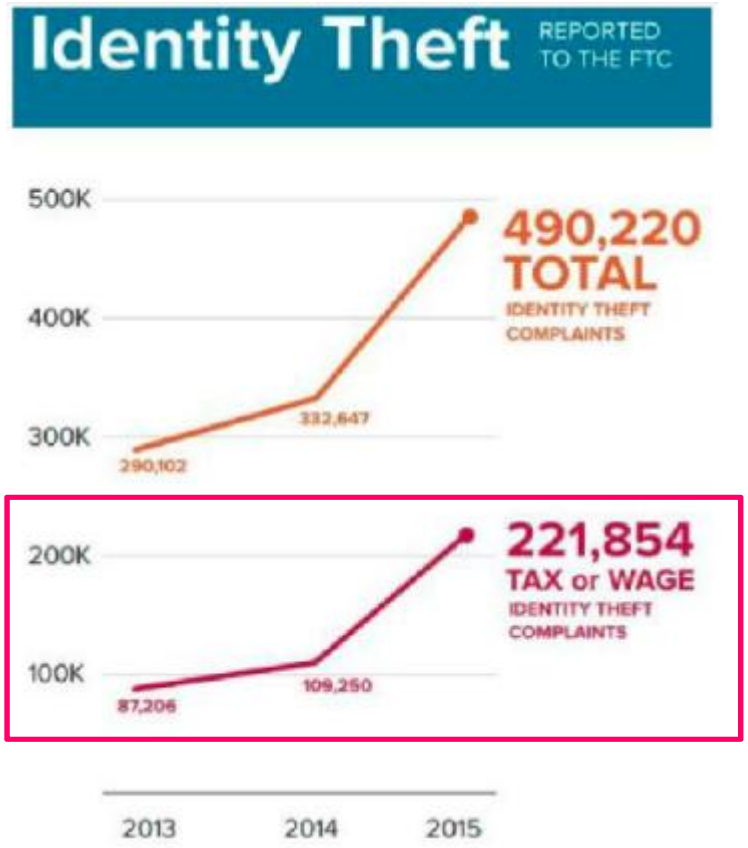
Texan gets 30 months in prison for 5 yr $800,000 tax refund scheme

On September 29, 2014, Stephen Galender Allison, 61, of Lakeway, Texas, was sentenced by U.S. District Court Judge Douglas Rayes to 30 months' imprisonment and was ordered to pay $813,555 in restitution […]

Between 2007 and 2012, Allison filed a total of 29 fraudulent federal and state tax returns claiming a total of $1,113,577 in false refunds and generating $813,555 in actual refund payments. […]

Quelle: https://arizonadailyindependent.com/2014/10/01/texan-gets-30-months-in-prison-for-5-yr-800000-tax-refund-scheme/

Meldungen betreffend Identity Theft an die FTC

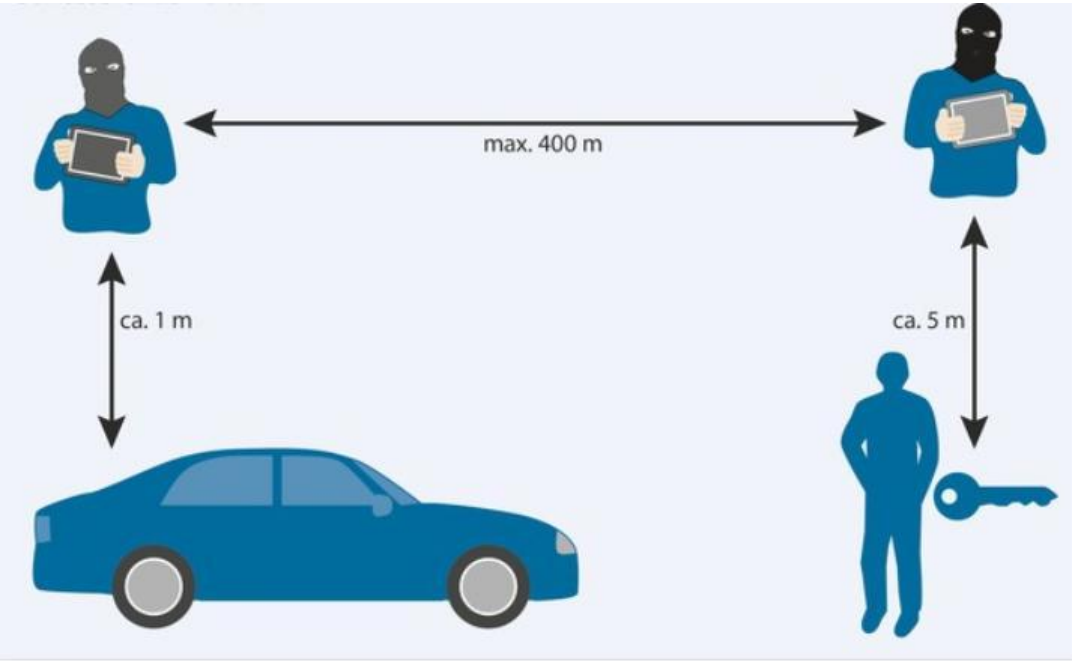


Quelle: https://www.techlicious.com/

Beispiel 2: IoT-bezogener Identitätsdiebstahl

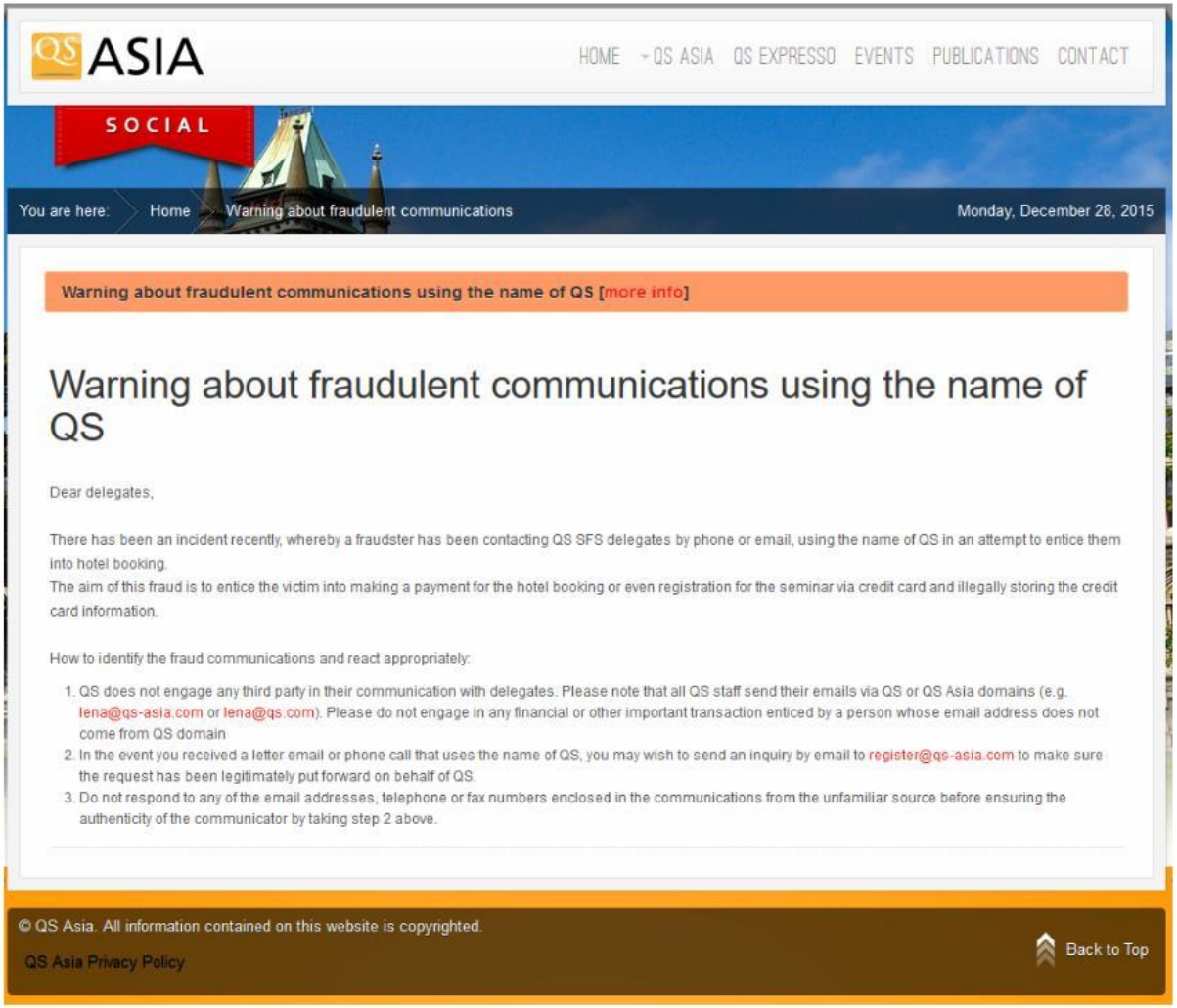
«Keyless Access»: Bequemer Zugang zu Ihrem Wagen!

à «Keyless gone» Heise 2015



Quelle: heise.de und Francillon et. al., ETH Zürich, https://eprint.iacr.org/2010/332.pdf

Beispiel 3: Convention Hotel Services



E-Mail von Convention Hotel Services, 20.1.2019

Sa. 20.01.2019 21:26

Convention Hotel Services <Help@conventionhotelservices.com>

CONVENTION HOTEL SERVICES Inc. - Loyalty program for CHS customers - 20% discount now

To help@conventionhotelservices.com

Thank you for your booking with CONVENTION HOTEL SERVICES Inc. We're pleased to inform you as a result of your booking before with us you have accumulated a reward of 20% off for your upcoming reservation with us.

Please contact us at (help@conventionhotelservices.com) for your upcoming event and gain your discounted rate and gift for any reservation between 1-6 nights for any number of rooms all over the world during 2019.

Beispiel 4: Phishing – ja oder nein?

Di. 15.03.2016 14:27

Herr Mark Carney <dante.mascia@em

To

Hallo, obwohl du mich nicht wissen kann, und diese E-Mail kam als eine
ernannte Vorsitzende der Bank of England. Es gibt eine Summe von (zw
keine Empfänger angegeben, diese Mittel über und niemand würde sie
Unterstützung das Geld auf Ihr Bankkonto zu übertragen in Ihr Land, so
andere Geschäftsbereiche investieren, besteht keine Gefahr, in dieser
für Sie teilen diese diese E-Mail nicht der Geldwäsche ist, antworten (m
Ich werde mich freuen, von Ihnen zu hören.
Es ist zu 100% kein Risiko bei dieser Transaktion und die Übertragung gar

Grüße.
Herr Mark Carney.
Bitte antworten Sie auf meine private E-Mail (mcarney19630@gmail.com

k Carney der
d es gibt
ür Ihre
Teil auf
ür mich, 40%
rmationen.

Mark Carney

Governor of the Bank of Canada

Mark Joseph Carney, OC is a Canadian economist who currently serves as Governor of the Bank of England and Chairman of the G20's Financial Stability Board. Wikipedia

Born: March 16, 1965 (age 51), Fort Smith, Canada

Spouse: Diana Carney (m. 1995)

Succeeded by: Stephen Poloz

Office: Governor of the Bank of Canada since 2008

Education: Nuffield College, Oxford (1993), more

Beispiel 5: Phishing – ja oder nein

Beispiel 6: Phishing – ja oder nein?

Reply Reply All Forward

Mo. 05.11.2018 11:51

Walder Wyss <noreply@regi.in>

Vertraulich: Information für Bernhard Plattner

To bernhard@plattner.org

Vertraulich 05.11.2018 4...
180 KB

Das Dokument mit der Information ist in dem Attachment zu der E-Mail.
Für umgehenden Kontakt nutzen Sie die Kontaktdaten am Ende des Dokuments.

Empfängersdaten:

Vor- und Nachname Bernhard Plattner
Adresse Ob den Reben 18c

walderwyss rechtsanwälte

Nach dem Click auf das Attachment

Datenquellen für Identitätsdiebe

Collection #1 Data Breach Exposes Nearly 733 Million Records, Highlighting Need for Multifactor Authentication

January 22, 2019 @ 10:05 AM

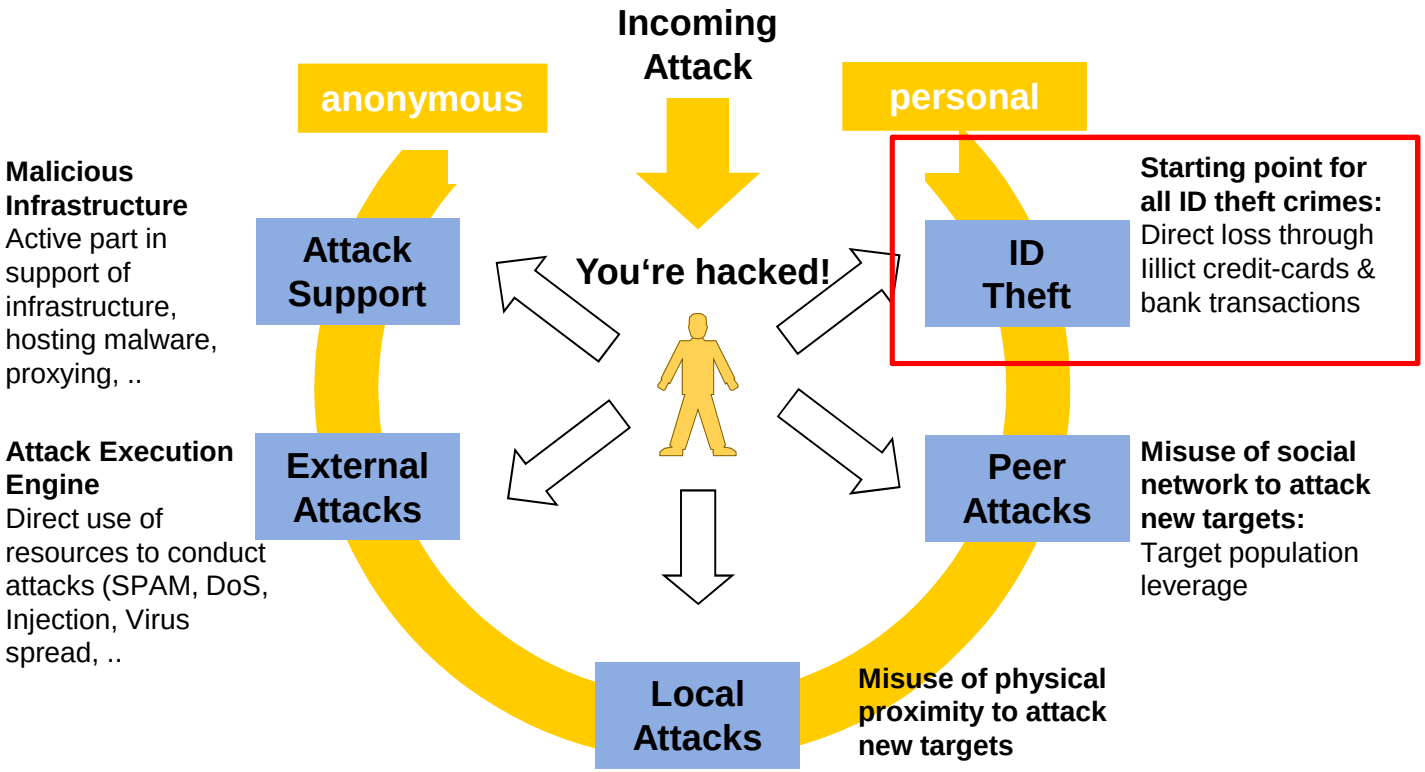
The theft of nearly 733 million unique email messages and 21 million passwords underscores the urgent need for multifactor authentication in the enterprise.

First discovered by security researcher Troy Hunt, records from the data breach were published to a hacker forum as well as the cloud-based service MEGA, though they have since been removed.

Dubbed Collection #1, the perpetrators behind the theft remain unknown, but the volume of 12,000 files suggests that it may have involved multiple incidents and actors. Cleaned-up versions of the files have been loaded into Have I Been Pwned, which users can leverage to check whether their data was compromised in the breach.

wurden dem Office of
onnel Management
M) 21.5 Millionen
nsätze entwendet.

Mehrphasiger Angriff durch Schadsoftware



Credits: Stefan Frei

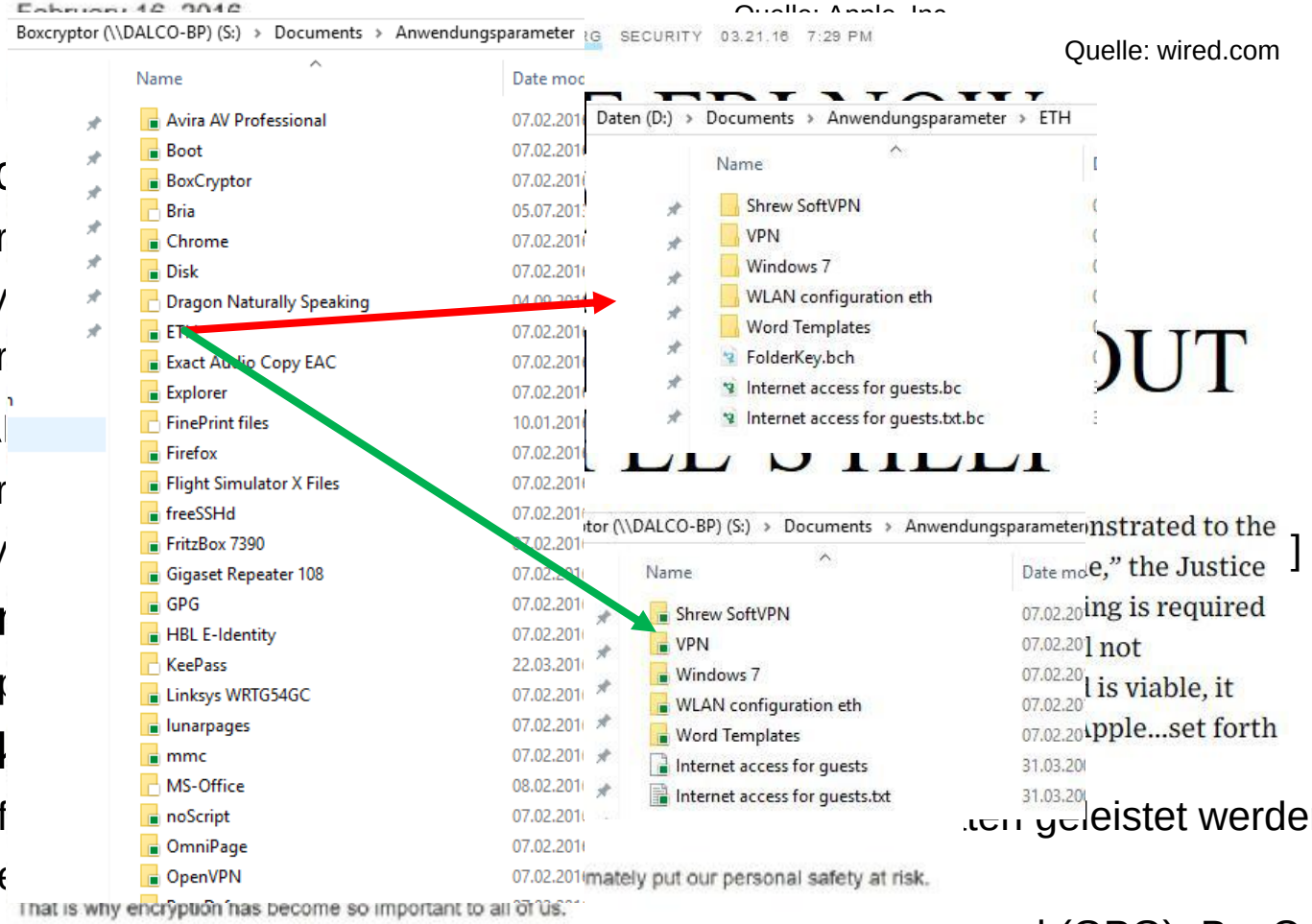
Was tragen wir selbst dazu bei?

- Information über uns im Netz (Soziale Netzwerke, berufliche Präsenz, etc.)
- Information in unseren tragbaren Geräten (Laptop, Mobiltelefon)
- Liederliche Wahl von Zugangsdaten für
  - E-Mail Accounts
  - On-line Shops
  - Konten von sozialen Netzwerken
  - E-banking
- Fehlendes Misstrauen gegenüber dem, was man im Internet antrifft

Wie können wir uns schützen?

- Wem vertraue ich Information über mich selbst an?
- Persönliche Daten in sozialen Netzen
  - Was vertraue ich meinem Profil in Facebook oder LinkedIn an?
- Sorgfältiger Umgang mit Zugangsdaten
  - Zugangsdaten für e-banking
  - Daten zu Kreditkarten
  - Web-Accounts
  - E-Mail Zugangsdaten
  - Etc.
- Sichere Passwortwahl; 2-Faktor-Authentisierung
- Welcher Information vertraue ich?
  - Im Web, social media, e-mail, per Telefon, in der Post, …

Verschlüsselung von Daten in mobilen Geräten



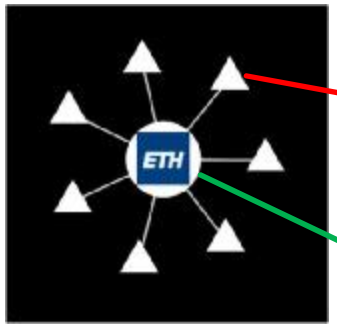
Quelle: wired.com

- § Bitloc
  - § Ver
  - § Kry
  - § Ver
- § Ab A
  - § Ver
  - § Kry
- Ø iPhor
  - § App
- Ø Selek
  - § Auf
  - § Abe
  - § Tools: VeraCrypt (ex. TrueCrypt), AxCrypt, GnuPrivacyGuard (GPG), BoxCryptor

Schutz gegen Phishing

- Seien Sie misstrauisch!
- Ist die Absenderadresse plausibel?
- Denken vor dem Click: Ist der eingeblendete URL plausibel?
- Vorsicht bei e-mail Anhängen (sie sind der häufigste Weg, um eine Schadsoftware zu installieren)
- Keine automatische Ausführung von Macros in MS Word, Excel, Access, …
- Deaktivieren von Skripten im Webbrowser (NoScript) – kann ein Rettungsfallschirm sein

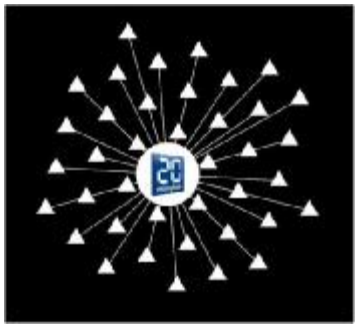
Welchen Effekt haben «Skripte» im Browser?



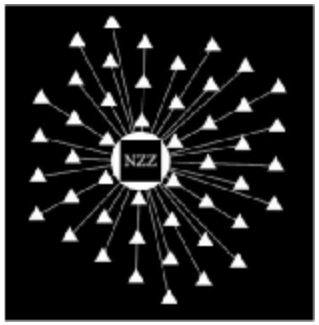
7 andere Sites werden aufgerufen

ethz.ch

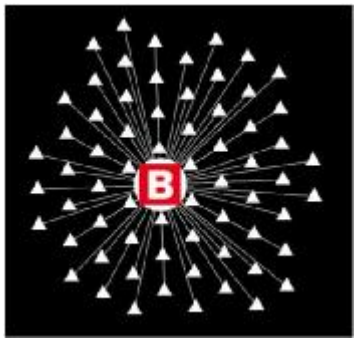
Aufruf von «ethz.ch»



20minuten.ch
39 andere Sites!

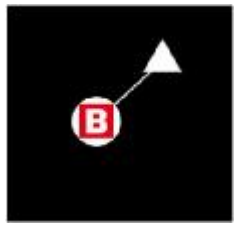


nzz.ch
47 andere Sites!



blick.ch
67 andere Sites!

Installation von NoScript



Ransomware

Ransomware

EDITION:

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITER

US hospital pays $55,000 to hackers after ransomware attack

Hancock Health paid up despite having backups available.

By Charlie Osborne for Zero Day | January 17, 2018 -- 09:53 GMT (09:53 GMT) | Topic: Security

MORE FROM CHARLIE OSBORNE

Innovation
Artificial intelligence will become next new human right

Security
Data security is a major issue in GDPR compliance

Ransomware

The Locky Ransomware Encrypts Local Files and Unmapped Network Shares

Lawrence Abrams | February 16, 2016 | 05:22 PM | Read 152,208 times | 61

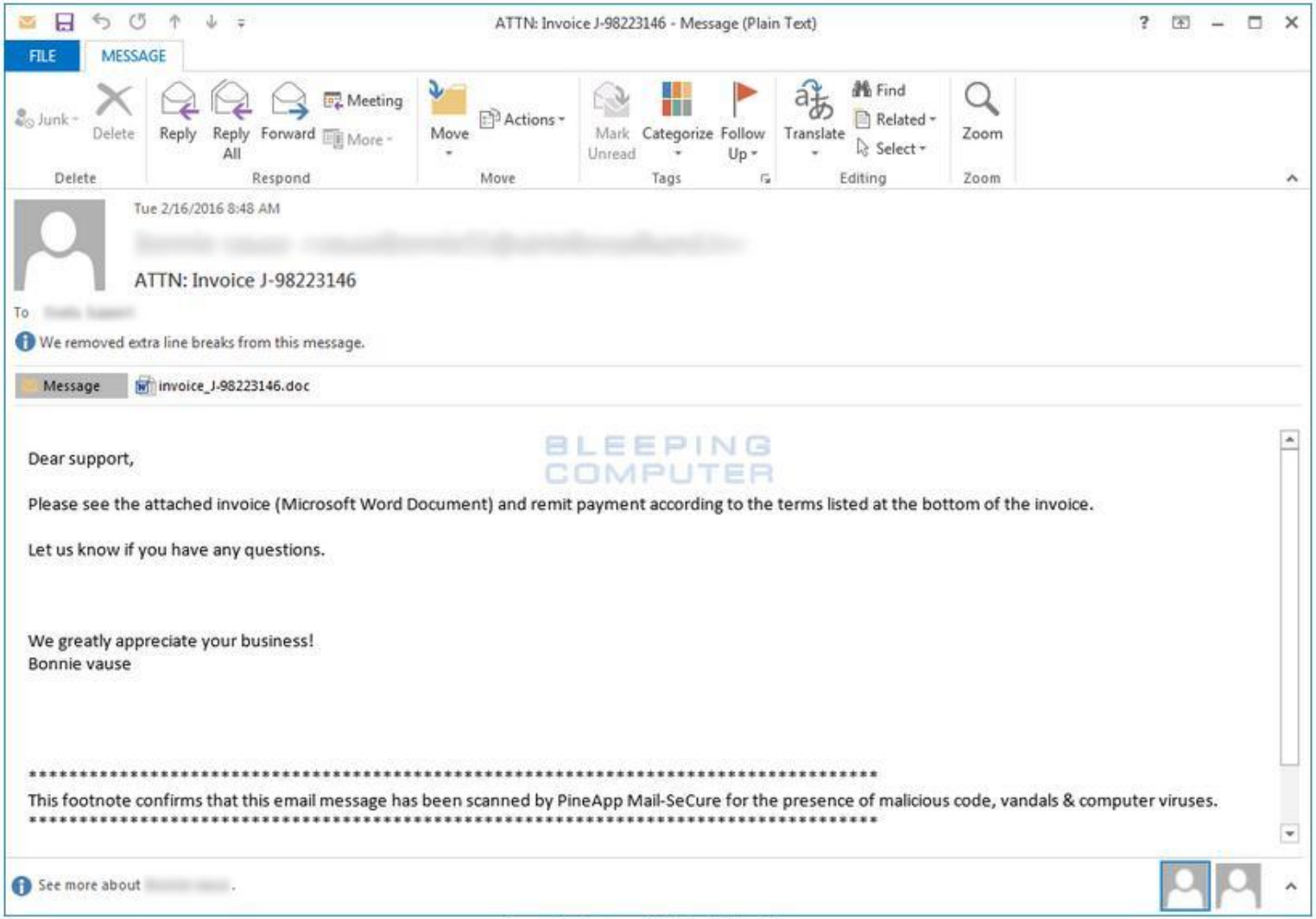
A new ransomware has been discovered called **Locky** that encrypts your data using AES encryption and then demands .5 bitcoins to decrypt your files. Though the ransomware sounds like one named by my kids, there is nothing childish about it. It targets a large amount of file extensions and even more importantly, encrypts data on unmapped network shares. Encrypting data on unmapped network shares is trivial to code and the fact that we saw the recent DMA Locker with this feature and now in Locky, it is safe to say that it is going to become the norm. Like CryptoWall, Locky also completely changes the filenames for encrypted files to make it more difficult to restore the right data.

At this time, there is no known way to decrypt files encrypted by Locky. For those who wish to discuss this ransomware or have questions, please feel free to post in our Locky Ransomware Support and Help Topic.

Locky installed via fake invoices

Locky is currently being distributed via email that contains Word document attachments with malicious macros. The email message will contain a subject similar to **ATTN: Invoice J-98223146** and a message such as "Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice". An example of one of these emails can be seen below.

Ransomware



Locky Email Distribution

Ransomware

- Ransomware war 2016 en vogue, ist jedoch nach wie vor eine Gefahr
- Ziele: Privatpersonen, KMU, öffentliche Einrichtungen
- Anwendung von Phishing
- Infiltrierte Schadsoftware verschlüsselt alle angeschlossenen Disks; Daten können gleichzeitig auch gestohlen werden
- Erpressung: Schlüssel für Entschlüsselung gegen Bitcoins – jedoch keine Garantie
- Locky, DMA Locker, Cryptolocker, Reveton, Cryptowall, KeRanger …
- Wie kann man sich schützen?
  - Sich nicht durch eine Phishing Mail hereinlegen lassen!
  - Ein Backup bietet einen begrenzten Schutz
    - Automatisches Backup ist möglicherweise nutzlos **à** «Intelligentes Backup»?
    - Off-line Backups
  - Empfohlen: Datenspeicher mit periodischen «read-only snapshots»; ersetzt jedoch das Backup nicht!

Passwörter: Die Top 15 in 2015

1. **123456** (Unchanged)
2. **password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 1)
5. **12345** (Down 2)
6. **123456789** (Unchanged)
7. **football** (Up 3)
8. **1234** (Down 1)
9. **1234567** (Up 2)
10. **baseball** (Down 2)
11. **welcome** (New)
12. **1234567890** (New)
13. **abc123** (Up 1)
14. **111111** (Up 1)
15. **1qaz2wsx** (New)

- Top 15 von mehr als 2 Millionen Passwörtern
- Quellen: Datenlecks nach Cyber-Einbrüchen (Ashley Madison, Target, …)
- Warum ist «1qaz2wsx» im Rang 15?

Quelle: http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514

Passwörter: Top 15 in 2018

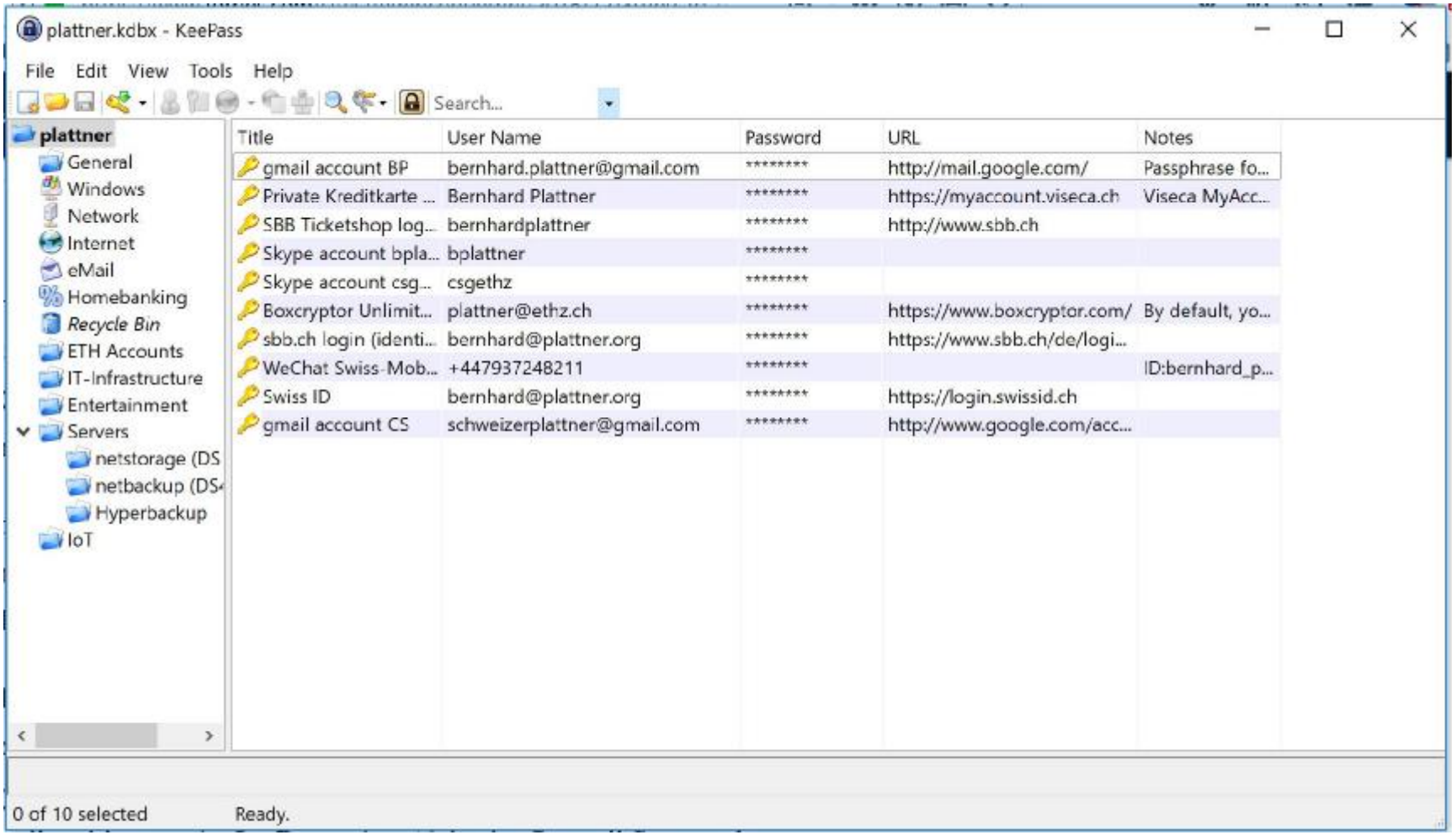
1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123

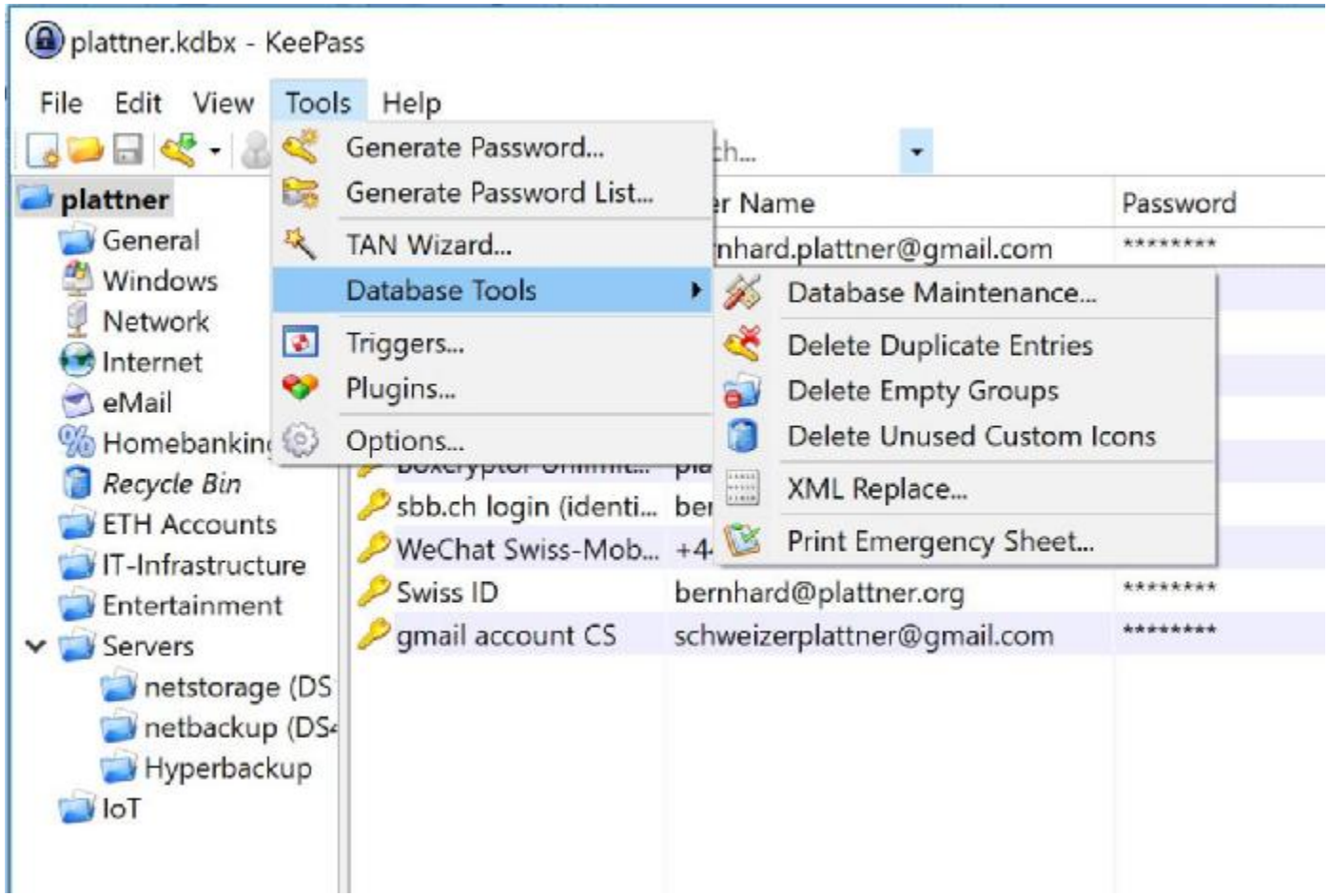
Quelle: https://www.dignited.com

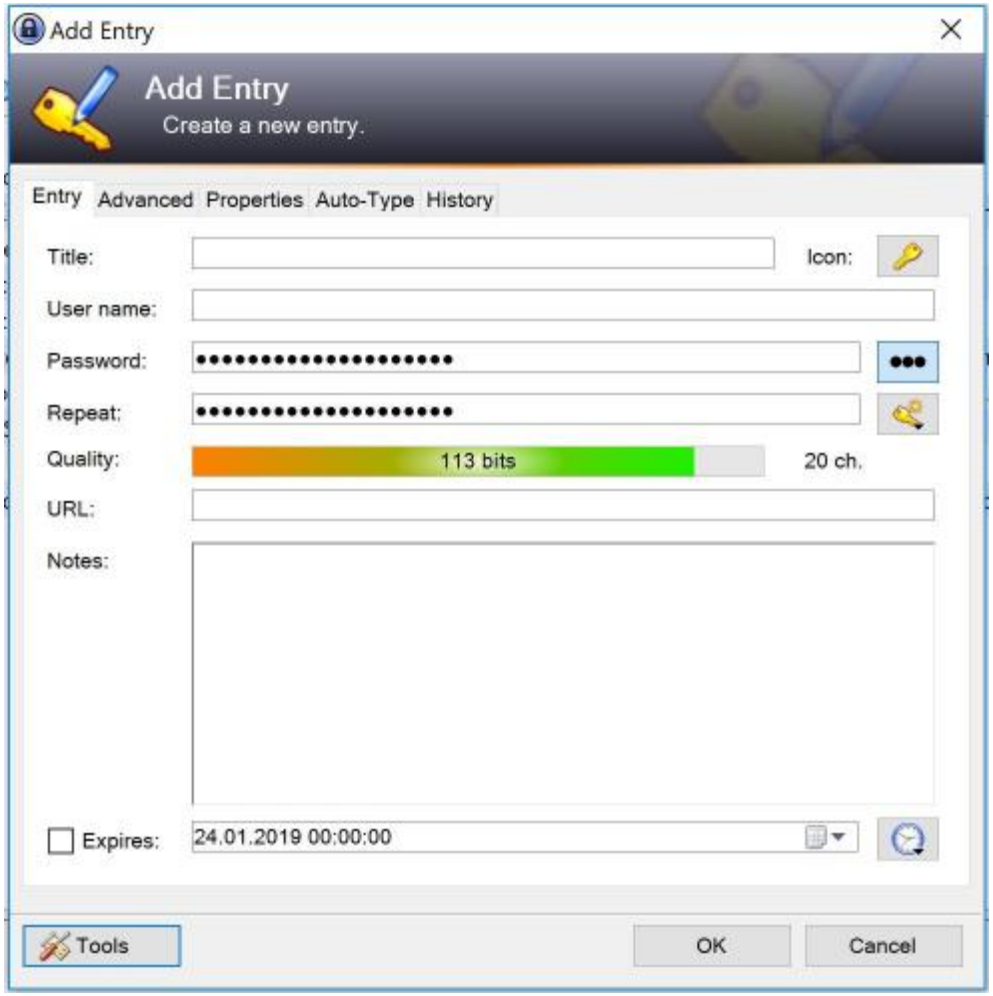
Wahl der Passwörter

- 123456?
- Julia15?
- 30.11.1949 (Ihr Geburtstag)?
- Beatrice+Andi?
- Vancouver, Kanada, gefällt mir seit 1996 **à** V,K,gms1996 ?
- [+503>%Z@4!7MiTB?
- Wie viele Passwörter benötigen Sie?
- Wie viele Passwörter können Sie sich merken?
- (Einzige) gangbare Lösung: Ein Password Safe
- Viele Angebote: KeePass, Password Manager, pwSafe …
- Für Windows, Mac, Linux, Android, iOS, cross-platform

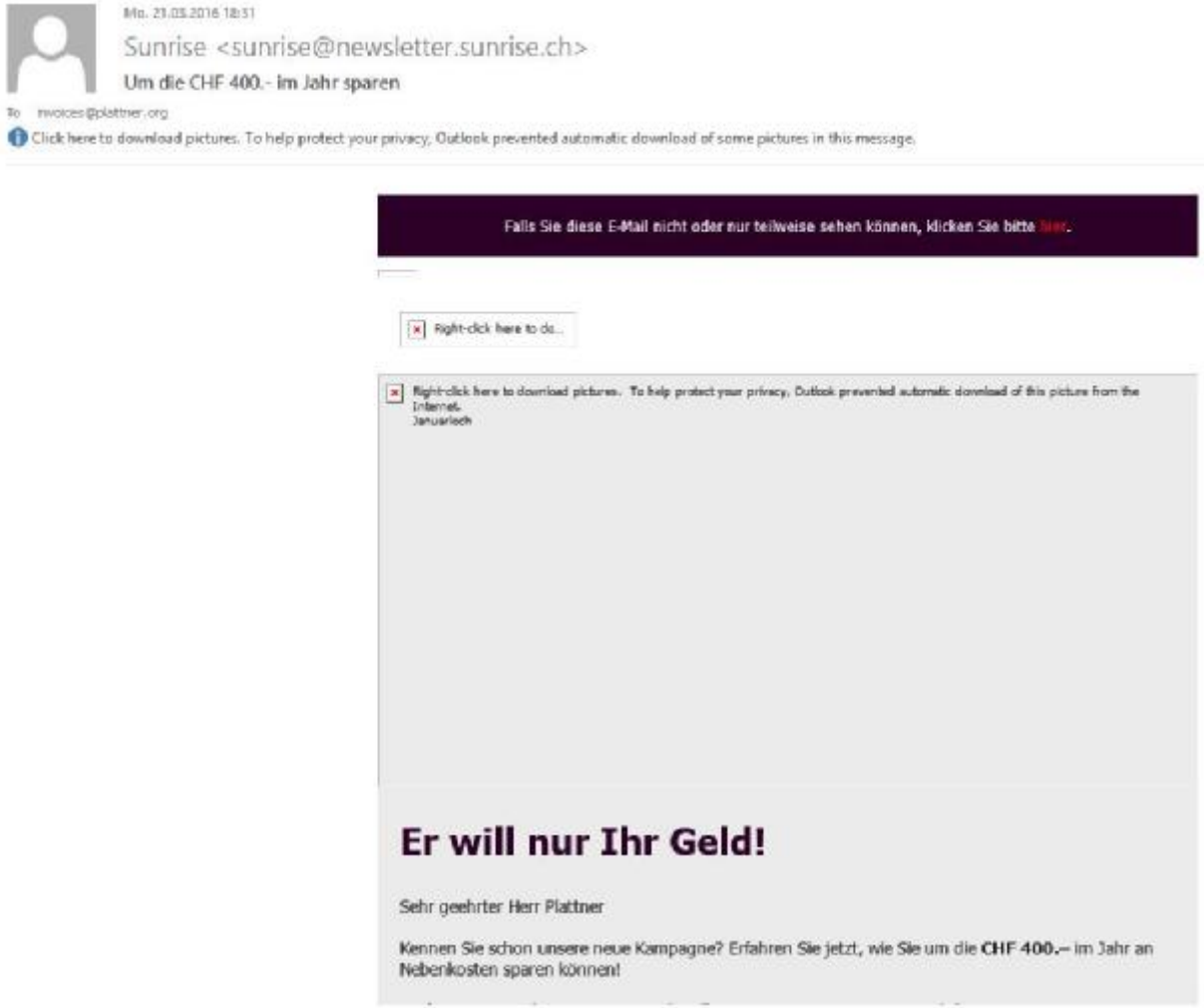
Beispiel: KeePass




plattner.kdbx - KeePass
File Edit View Tools Help
Generate Password...
Generate Password List...
TAN Wizard...
Database Tools
Triggers...
Plugins...
Options...
Database Maintenance...
Delete Duplicate Entries
Delete Empty Groups
Delete Unused Custom Icons
XML Replace...
Print Emergency Sheet...
plattner
General
Windows
Network
Internet
eMail
Homebankin
Recycle Bin
ETH Accounts
IT-Infrastructure
Entertainment
Servers
netstorage (DS
netbackup (DS
Hyperbackup
IoT
Name
Password
nhard.plattner@gmail.com
****
sbb.ch login (identi...
WeChat Swiss-Mob...
Swiss ID
bernhard@plattner.org
****
gmail account CS
schweizerplattner@gmail.com
****


Add Entry
Add Entry
Create a new entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
Icon:
User name:
Password:
Repeat:
Quality:
113 bits
20 ch.
URL:
Notes:
Expires:
24.01.2019 00:00:00
Tools
OK
Cancel

Noch einmal Thema Phishing



Analyse der Mail-Header

Received: from mail18-146.srv2.de ([193.169.181.146]:55310)
by valkanos.lunarpages.com with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
(Exim 4.86_1)
(envelope-from <return@newsletter.sunrise.ch>)
id 1ai3fv-000Mr8-W5
for invoices@plattner.org; Mon, 21 Mar 2016 10:31:47 -0700

vertrauenswürdig

kann manipuliert sein

Return-Path: <return@newsletter.sunrise.ch>
Reply-To: <re-1MIMY447-1M5Z96X8-10ZMN3Y@newsletter.sunrise.ch>
From: "Sunrise" <sunrise@newsletter.sunrise.ch>
To: <invoices@plattner.org>
Subject: Um die CHF 400.- im Jahr sparen
Date: Mon, 21 Mar 2016 18:30:35 +0100
Message-ID: <re-pTfh2FFCGlp868wucDvsRuj4JZvq-1MIMY447-1M5Z96X8-I4S1700@newsletter.sunrise.ch>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0007_01D18416.B33CD3B0"
X-Mailer: Microsoft Outlook 15.0
X-Ham-Report:
Spam_detection_software_running_on_the_system_valkanos.lunarpages.com_has_NOT_identified_this_incoming_email_as_spam.
[...]
X-Spam-Score: -14
X-Spam-Status: No, score=-1.5
X-Spam-Bar: -
X-Spam-Flag: NO
List-Unsubscribe: <http://newsletter.sunrise.ch/go/12/1MIMY447-1M5Z96X8-1UWUIDA-5DZQ8N-U.html#List-Unsubscribe=One-Click>
X-CSA-Complaints: whitelist-complaints@eco.de
Thread-Index: AQHa4youPFuiNYXLG7Nl7ZvOyRQ4tA==
X-ulpe: re-pTfh2FFCGlp868wucDvsRuj4JZvq-1MIMY447-1M5Z96X8-I4S1700@newsletter.sunrise.ch

Phishing oder nicht?

Analyse der Mail Header

[...]
Received: from smtp.pcp.ch ([92.42.189.133]:55176)
by valkanos.lunarpages.com with esmtp (Exim 4.86_1)
(envelope-from <Neuigkeiten@PCP.CH>) id 1aip3o-0004Vh-0i
for bernhard@plattner.org; Wed, 23 Mar 2016 13:07:26 -0700

vertrauenswürdig

kann manipuliert sein

Received: from WEB03.office.pcp.com (unknown [10.100.8.6])
by smtp.pcp.ch (Postfix) with ESMTP id 34CB01227C1
for <bernhard@plattner.org>; Wed, 23 Mar 2016 21:06:40 +0100 (CET)
Date: Wed, 23 Mar 2016 21:07:27 +0100 (CET)
From: "PCP.CH" <Neuigkeiten@PCP.CH>
To: bernhard@plattner.org
Message-ID: <1262117225.98135.1458763647579.JavaMail.WEB03$@10.100.8.5>
Subject: =?UTF-8?Q?Neuheiten_aus_der_Fotoabteilun?=
=?UTF-8?Q?g_-_passend_zum_Fr=C3=BChlingsanfang?=
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-Mailer: ColdFusion 11 Application Server
[...]

Verhalten beim Surfen

- Nur vertrauenswürdige Seiten besuchen
- Beim Besuch von nicht vertrauenswürdigen Seiten: Browser in einer Virtuellen Maschine ausführen
- Wie?
  - Oracle Virtualbox installieren
  - Linux herunterladen und in Virtualbox installieren
  - Jeweils nur einmal nutzen (immer mit einer frischen Kopie)
- Hilft das „private“ Browser-Fenster?
  - Nein!
- Helfen Virenscanner (Anti-Virus-Produkte)?
  - Nur bedingt!

ETH zürich

Vielen Dank für Ihre Aufmerksamkeit!