Cybersikkerhed

CYBERTRUSLER 2021

Keld Norman
Dubex A/S
Security Consultant
kno@dubex.dk

10. maj 2019

Nye krav til hackersikring af maskiner

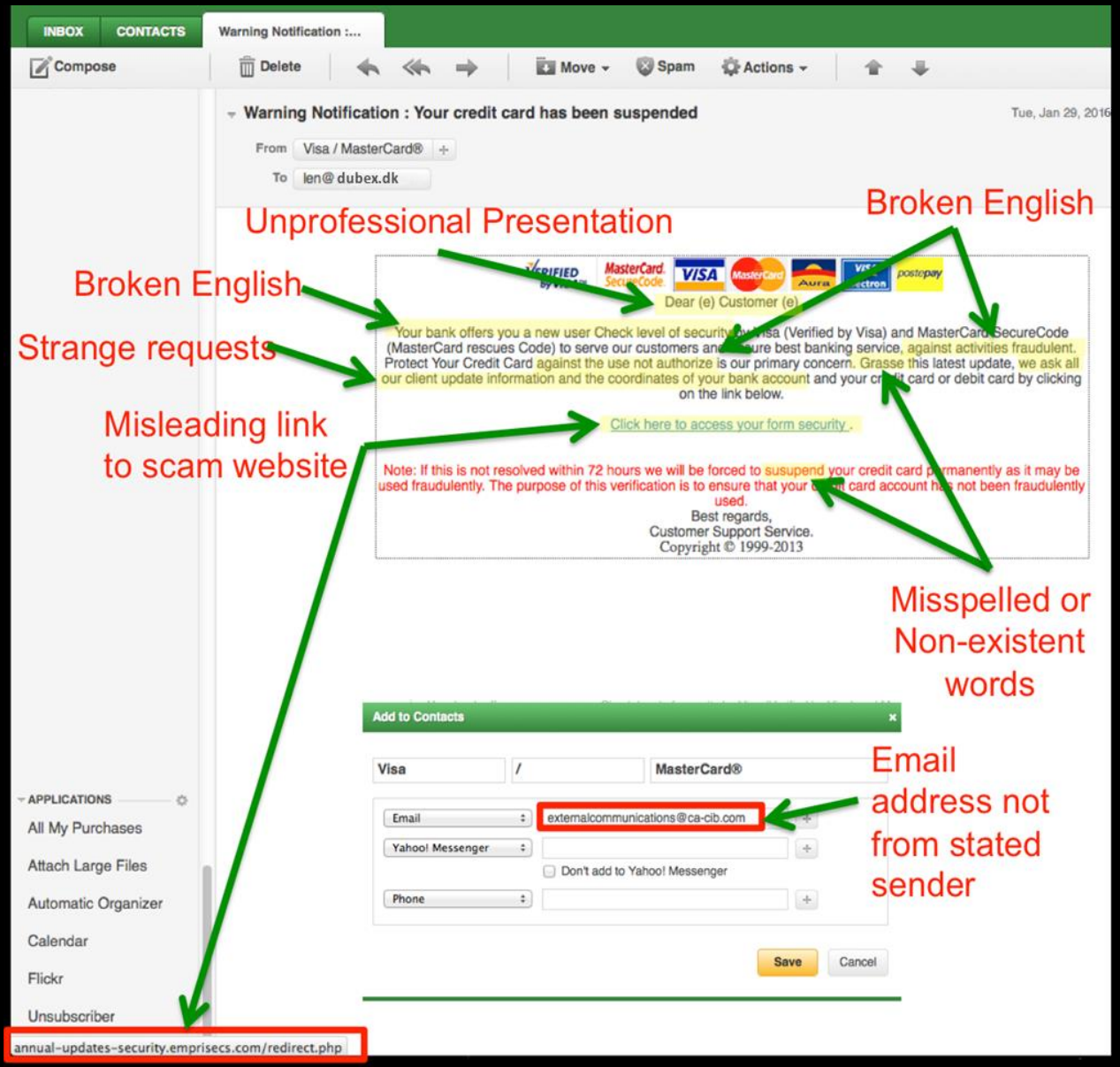
Sikkerhedsstyrelsen har for nyligt afgjort, at maskinfabrikanter har pligt til at sikre, at maskiners sikkerhedsstyresystemer ikke kan hackes.

Der er nye krav til hackersikring af maskiner. Det kan være en udfordring for mange maskinfabrikanter. Men der er hjælp at hente: ISO har udgivet en teknisk rapport om hackersikring og Dansk Standard og Maskinsikkerhed ApS inviterer til gratis informationsmøde om de nye krav.

ISO's tekniske rapport, ISO TR 22100-4 Hackersikring af maskiner, der udkom sidste år, giver vejledning til

PHISHING

IKKE SÆRLIG OVERBEVISENDE...



●●○○○ 3 01.46 100 %

Reklame (30)

Fra: Ikea

Til: Keld Norm… Skjul

Deltag i vores under…else og kræve din kupon

23. oktober 2016 kl. 19.16

IKEA

gavekort

keld.norman, har du en gave at pakke!

Tillykke!

Pak din gave fra Ikea! Du kan få 25kr, 50kr eller 100kr.

Sikke en perfekt gave fra Ikea!

Pak din gave!

●●○○○ 3 01.46 100 %

OK

Ikea

andet opkald video andet

andet

gadsden@dIsH.1e30.CaRlScOrNeR.iTsG...

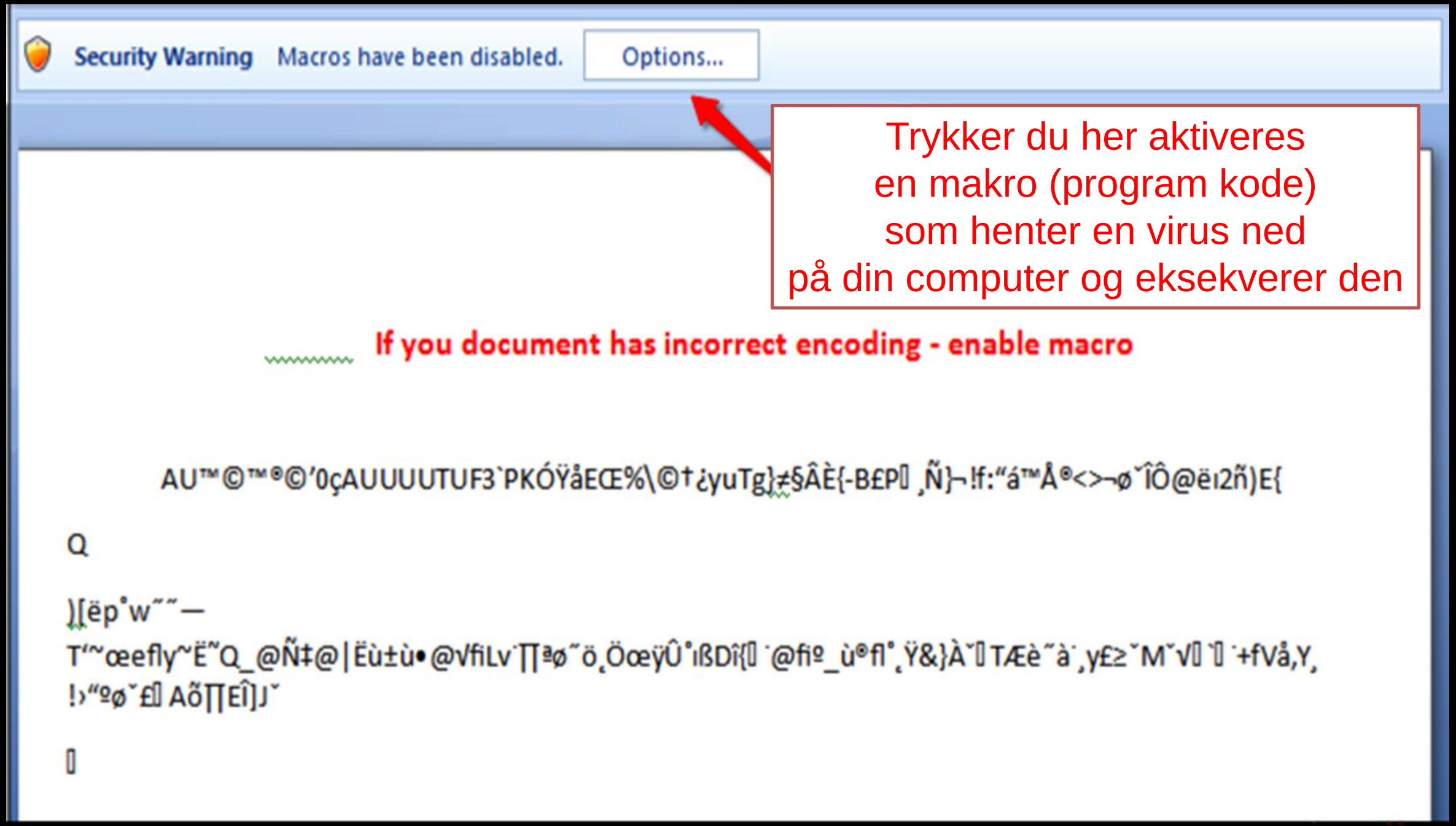
Føj til VIP

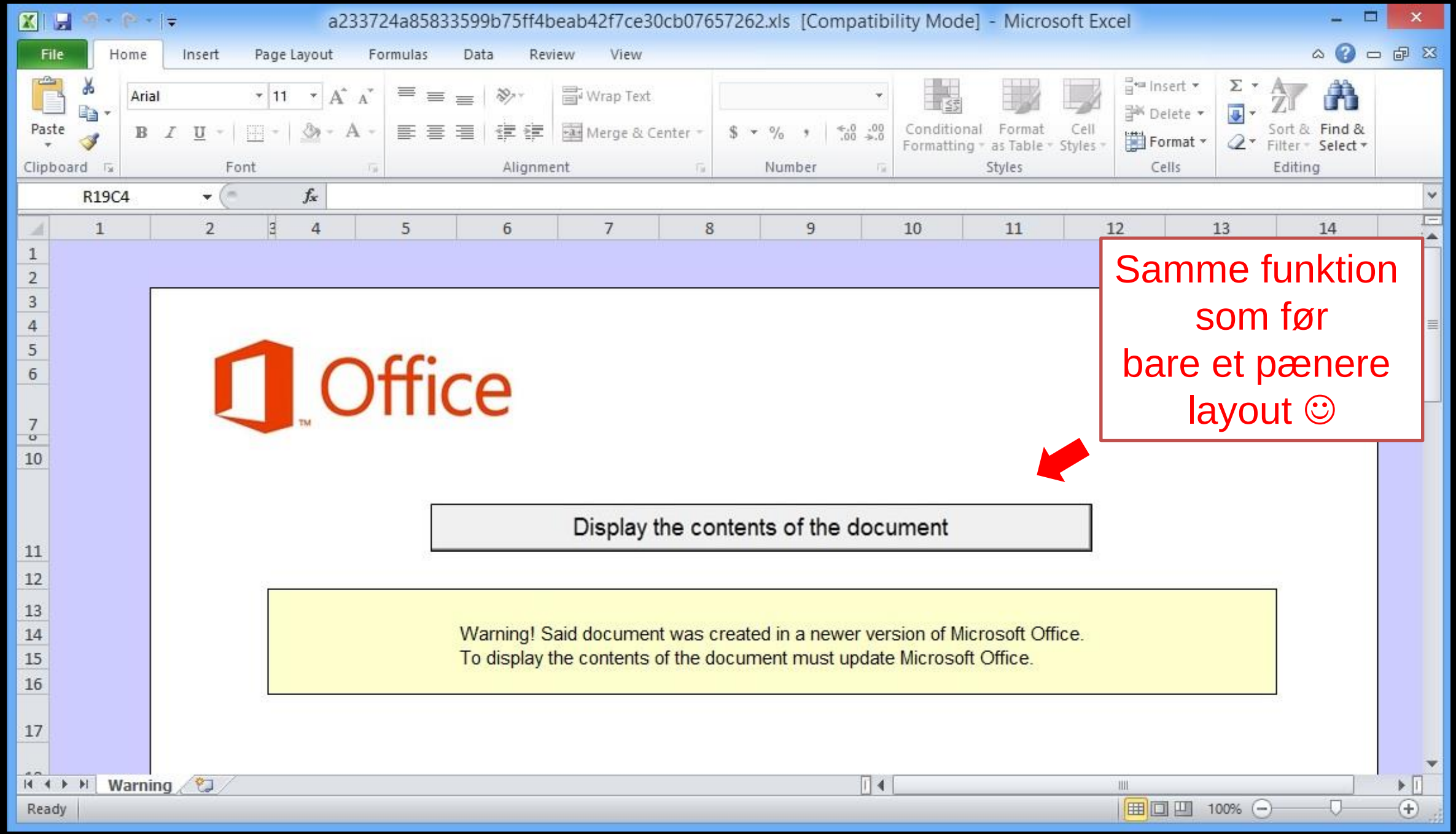
Send besked

Del kontakt

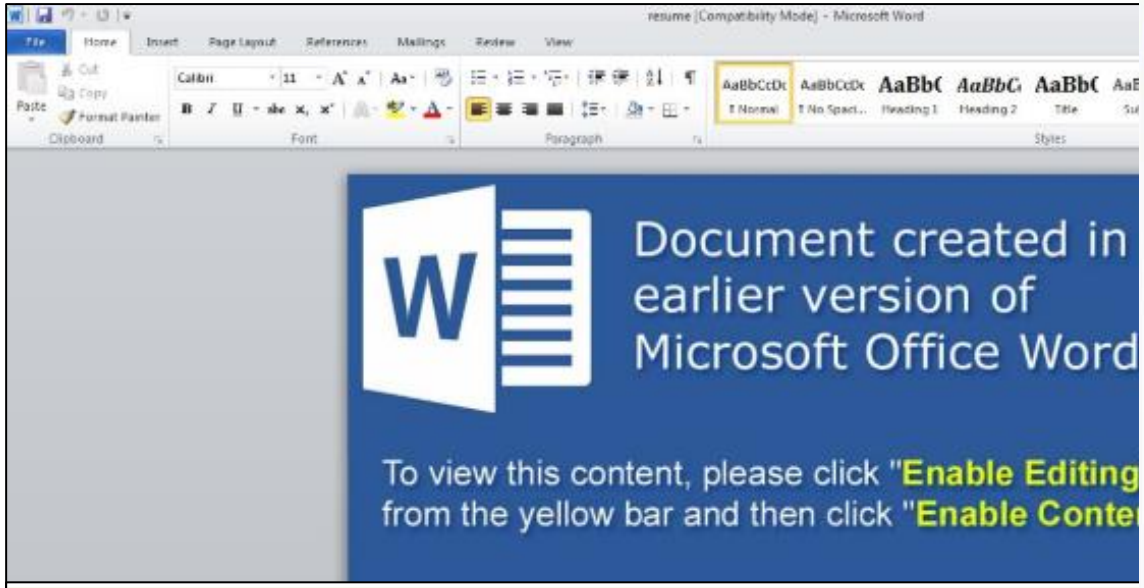
Del min lokalitet

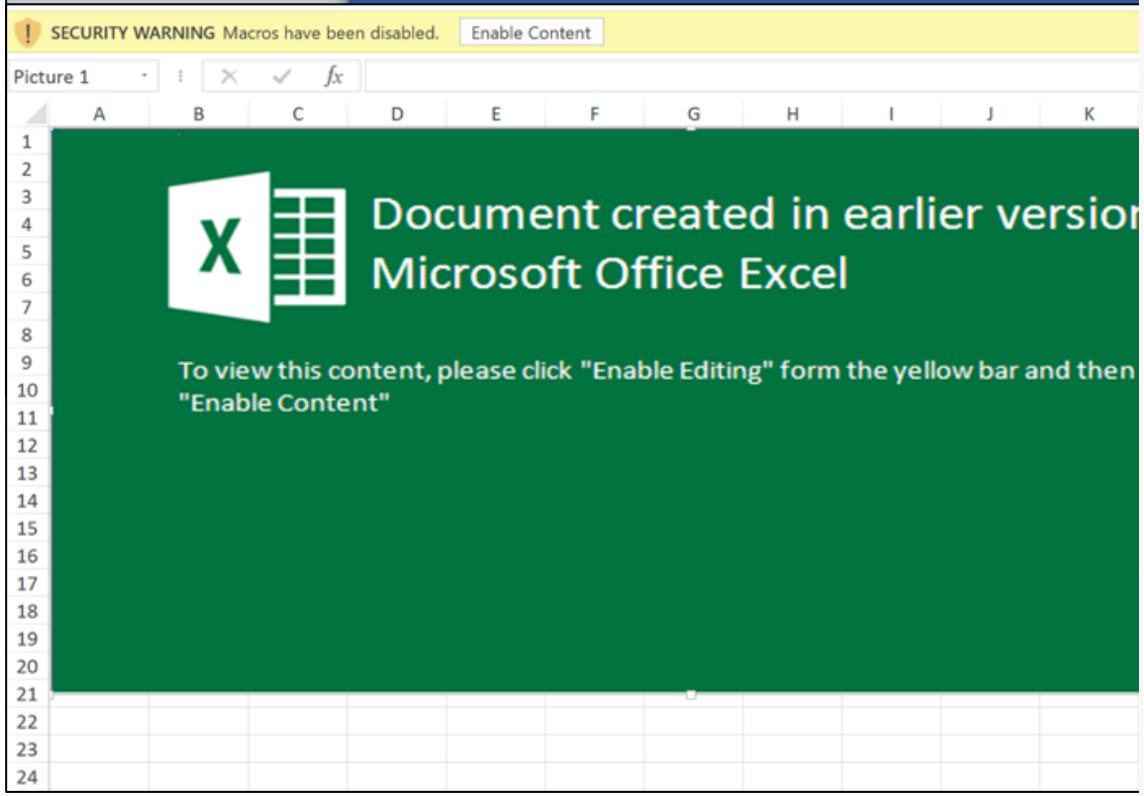
Den her mail er ikke fra Ikea !

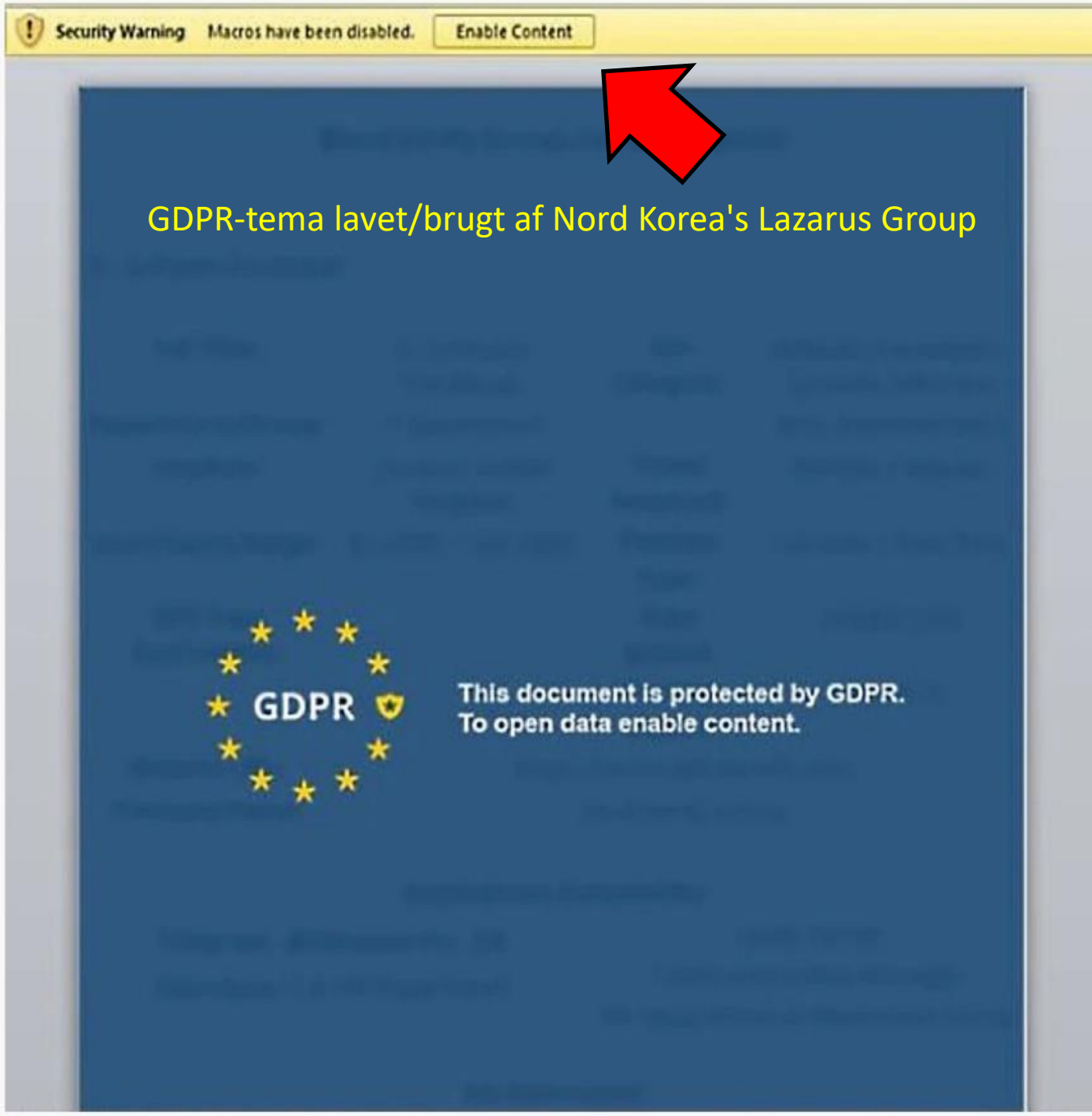

Security Warning
Macros have been disabled.
Options...
Trykker du her aktiveres
en makro (program kode)
som henter en virus ned
på din computer og eksekverer den
If you document has incorrect encoding - enable macro
AU™©™®©'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg}≠§ÂÈ{-B£P ,Ñ}¬!f:"á™Å®<>¬ø˜ÎÔ@ë¡2ñ)E{
Q
)[ëp°w˜˜—
T'˜œeefly˜Ë˜Q_@Ñ‡@|Ëù±ù•@√fiLv¨∏ªø˜ö¸ÖœÿÛ°ıßDî{ ¨@fiº_ù®fl°¸Ÿ&}À˜ TÆè˜à¨¸y£≥˜M˜√ ¨ ¨+fVå,Y¸
!›"ºø˜£ Aõ∏EÎ]ȷ˜



Samme funktion
som før
bare et pænere
layout ☺


Document created in earlier version of Microsoft Office Word
To view this content, please click "Enable Editing
from the yellow bar and then click "Enable Conte


SECURITY WARNING Macros have been disabled.
Enable Content
Document created in earlier versio
Microsoft Office Excel
To view this content, please click "Enable Editing" form the yellow bar and then
"Enable Content"


Security Warning
Macros have been disabled.
Enable Content
GDPR-tema lavet/brugt af Nord Korea's Lazarus Group
GDPR
This document is protected by GDPR.
To open data enable content.

Upload filerne her og test også URL's

virustotal **https://www.virustotal.com**

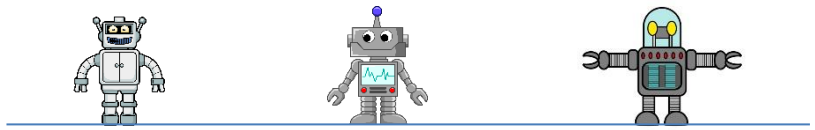
SHA256:	700b00abb2b0ea751469132f26973639cfad4f876a1a448efe3becde98df4945
Filnavn:	5f90e1bb293424e66b07e767816a197b1df445a2
Opdagelses forhold:	8 / 55
Undersøgelses dato:	2014-11-12 00:29:01 UTC (2 måneder, 1 ugeiden)

Testes af
75 forskellige
anti-virus produkter

Undersøger | File detail | Yderlig information | Kommentarer 0 | Stemmer

Antivirus	Resultat	Opdatere
AhnLab-V3	Trojan/Win32.Proxy	20141111
ESET-NOD32	Win32/TrojanProxy.Agent.NWO	20141112
F-Prot	W32/Bunitu.B.gen!Eldorado	20141111
Kaspersky	Trojan-Proxy.Win32.Bunitu.un	20141112
Malwarebytes	Trojan.Agent.ED	20141111
Microsoft	TrojanProxy:Win32/Bunitu.F	20141112
Panda	Trj/Genetic.gen	20141110
Qihoo-360	Malware.QVM40.Gen	20141112
AVG	✓	20141112
AVware	✓	20141112
Ad-Aware	✓	20141111
AegisLab	✓	20141112

Acronis (Acronis)
AegisLab (AegisLab)
Agnitum (Agnitum)
AhnLab (V3)
Alibaba Group (Alibaba)
Antiy Labs (Antiy-AVL)
Avast Software (Avast, Avast Mobile Security)
Arcabit (Arcabit)
AVG Technologies (AVG)
Avira (AntiVir)
Babable (Babable)
BluePex (AVware)
Baidu (Baidu-International)
BitDefender GmbH (BitDefender)
Bkav Corporation (Bkav)
ByteHero Information Security Technology Team (ByteHero)
Cat Computer Services (Quick Heal)
Check Point Software Technologies (ZoneAlarm)
ClamAV (ClamAV)
CMC InfoSec (CMC Antivirus)
Comodo (Comodo)
Cybereason (Cybereason)
Cylance (Cylance)
Cynet (Cynet)
Cyren (Cyren)
CrowdStrike (CrowdStrike Falcon (ML))
Doctor Web, Ltd. (DrWeb)
TEHTRI-Security (eGambit)
Elasticsearch (Elastic)
ESTsecurity (ALYac)
Emsisoft Ltd (Emsisoft)
Eset Software (ESET NOD32)
FireEye (Fireeye)
Fortinet (Fortinet)
FRISK Software (F-Prot)
F-Secure (F-Secure)
G DATA Software (GData)
Gridinsoft (Gridinsoft Antimalware Neural Network)
Hacksoft (The Hacker)
Hauri (ViRobot)
IKARUS Security Software (IKARUS)
Invincea (X by Invincea)
INCA Internet (TACHYON)
Jiangmin
K7 Computing (K7AntiVirus, K7GW)
Kaspersky Lab (Kaspersky)
Kingsoft (Kingsoft)
Lavasoft (Ad-Aware)
Malwarebytes Corporation
Intel Security (McAfee)
MAX (SaintSecurity)
MaxSecure (MaxSecure)
Microsoft (Malware Protection)
Microworld (eScan)
Nano Security (Nano Antivirus)
Palo Alto Networks (Palo Alto Networks)
Panda Security (Panda Platinum)
Qihoo 360 (Qihoo 360)
Rising Antivirus (Rising)
Sangfor (Sangfor)
SentinelOne (SentinelOne (Static ML))
Sophos (SAV)
SUPERAntiSpyware (SUPERAntiSpyware)
Symantec Corporation (Symantec Mobile Insight)
Tencent (Tencent)
ThreatTrack Security (VIPRE Antivirus)
TotalDefense (TotalDefense)
Trapmine (Trapmine)
Trend Micro (TrendMicro, TrendMicro-HouseCall)
Trustlook (Trustlook Antivirus)
VirusBlokAda (VBA32)
Webroot (Webroot)
Zillya! (Zillya)
Zoner Software (Zoner Antivirus)



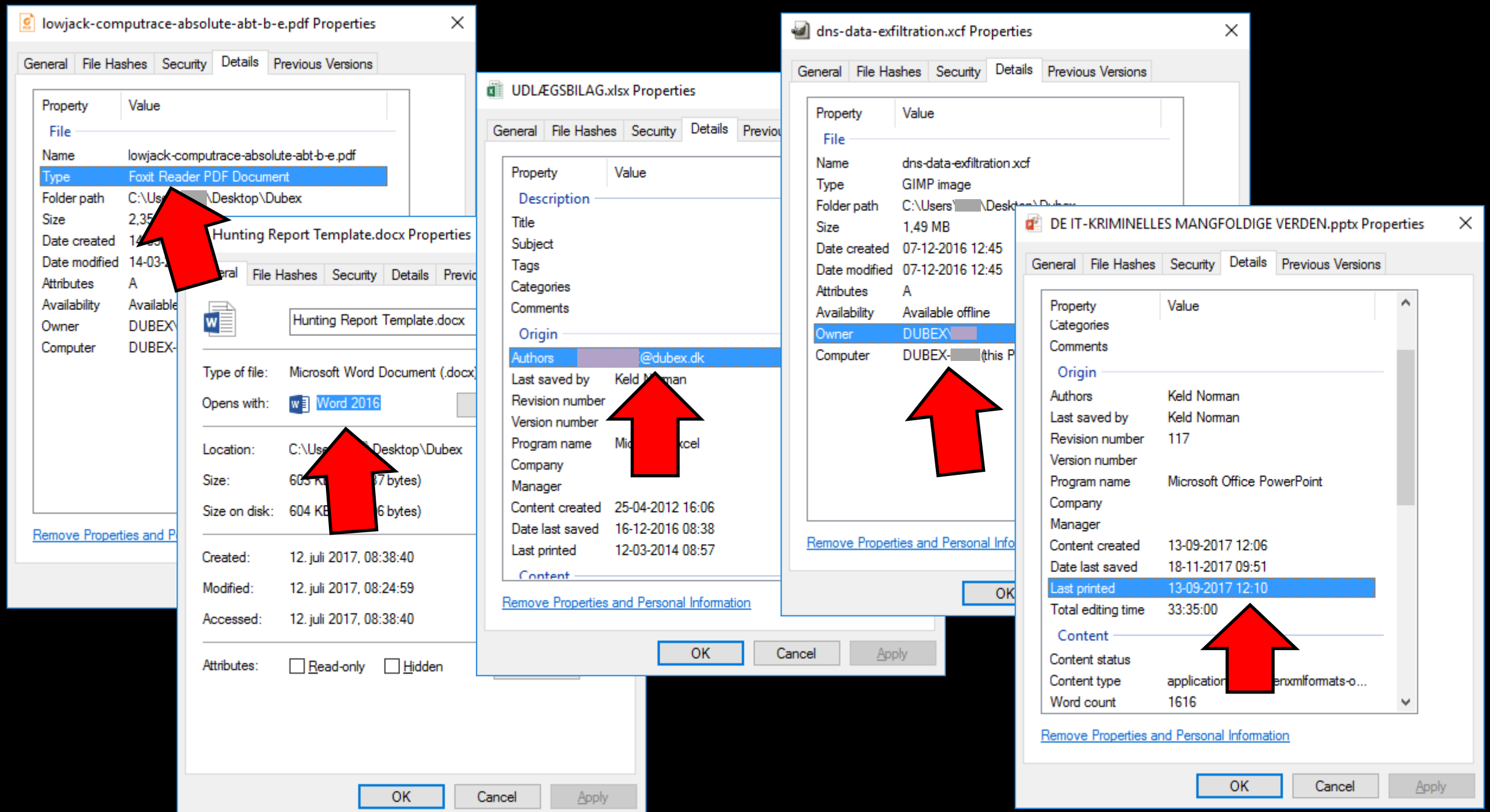
Filer der uploades bliver scannet af ~75 forskellige anti-virus produkter

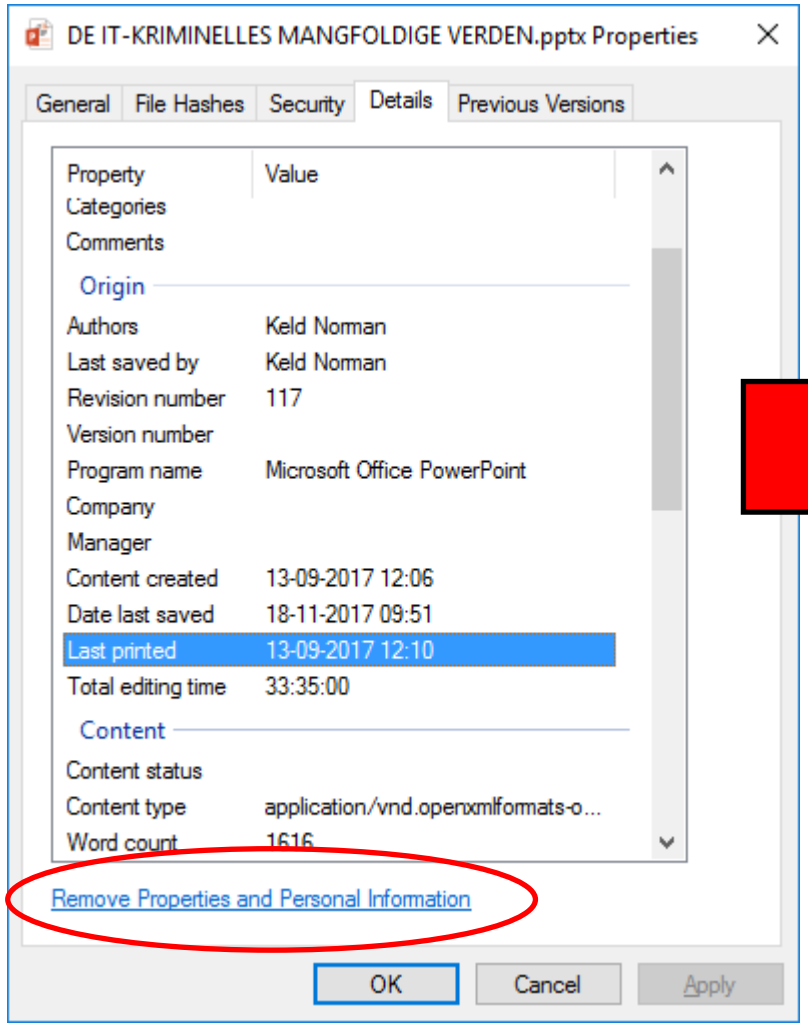
https://www.virustotal.com

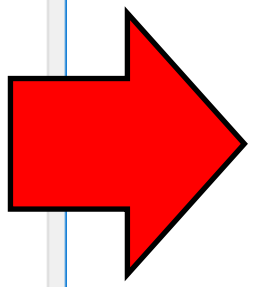
VIRUSTOTAL

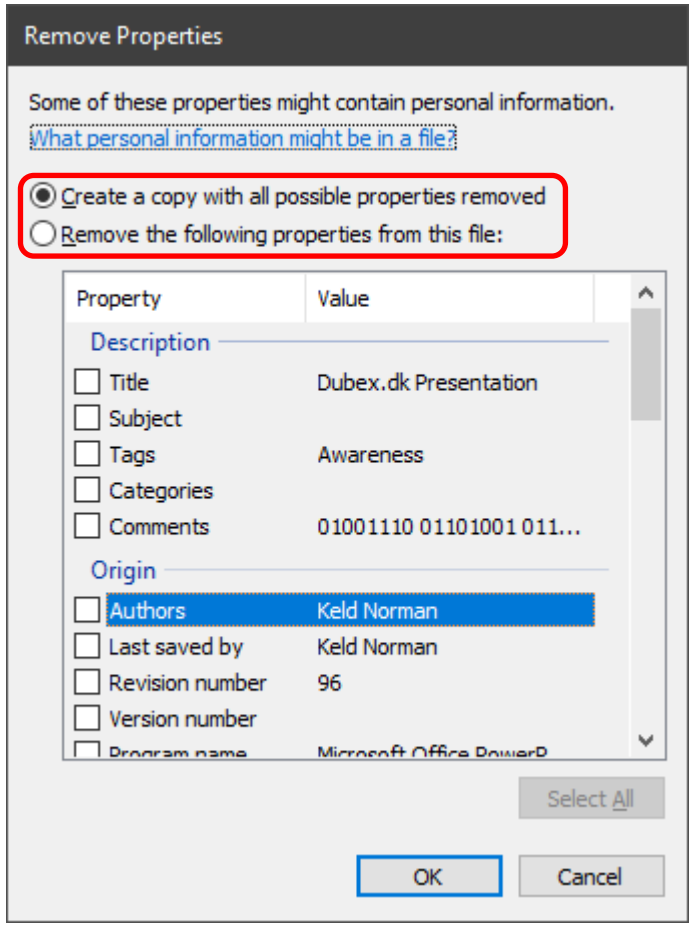
METADATA

...


lowjack-computrace-absolute-abt-b-e.pdf Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
File
Name
lowjack-computrace-absolute-abt-b-e.pdf
Type
Foxit Reader PDF Document
Folder path
Size
Date created
Date modified
Attributes
Availability
Owner
Computer
Remove Properties and P
Hunting Report Template.docx Properties
File Hashes
Security
Details
Hunting Report Template.docx
Type of file:
Microsoft Word Document (.docx)
Opens with:
Word 2016
Location:
Size:
Size on disk:
Created:
12. juli 2017, 08:38:40
Modified:
12. juli 2017, 08:24:59
Accessed:
12. juli 2017, 08:38:40
Attributes:
Read-only
Hidden
OK
Cancel
Apply
UDLÆGSBILAG.xlsx Properties
General
File Hashes
Security
Details
Property
Value
Description
Title
Subject
Tags
Categories
Comments
Origin
Authors
@dubex.dk
Last saved by
Revision number
Version number
Program name
Company
Manager
Content created
25-04-2012 16:06
Date last saved
16-12-2016 08:38
Last printed
12-03-2014 08:57
Content
Remove Properties and Personal Information
OK
Cancel
Apply
dns-data-exfiltration.xcf Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
File
Name
dns-data-exfiltration.xcf
Type
GIMP image
Folder path
Size
1,49 MB
Date created
07-12-2016 12:45
Date modified
07-12-2016 12:45
Attributes
A
Availability
Available offline
Owner
Computer
Remove Properties and Personal Info
OK
DE IT-KRIMINELLES MANGFOLDIGE VERDEN.pptx Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
Categories
Comments
Origin
Authors
Keld Norman
Last saved by
Keld Norman
Revision number
117
Version number
Program name
Microsoft Office PowerPoint
Company
Manager
Content created
13-09-2017 12:06
Date last saved
18-11-2017 09:51
Last printed
13-09-2017 12:10
Total editing time
33:35:00
Content
Content status
Content type
Word count
1616
Remove Properties and Personal Information
OK
Cancel
Apply


DE IT-KRIMINELLES MANGFOLDIGE VERDEN.pptx Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
Categories
Comments
Origin
Authors
Keld Norman
Last saved by
Keld Norman
Revision number
117
Version number
Program name
Microsoft Office PowerPoint
Company
Manager
Content created
13-09-2017 12:06
Date last saved
18-11-2017 09:51
Last printed
13-09-2017 12:10
Total editing time
33:35:00
Content
Content status
Content type
application/vnd.openxmlformats-o...
Word count
1616
Remove Properties and Personal Information
OK
Cancel
Apply




Remove Properties
Some of these properties might contain personal information.
What personal information might be in a file?
Create a copy with all possible properties removed
Remove the following properties from this file:
Property
Value
Description
Title
Dubex.dk Presentation
Subject
Tags
Awareness
Categories
Comments
01001110 01101001 011...
Origin
Authors
Keld Norman
Last saved by
Keld Norman
Revision number
96
Version number
Select All
OK
Cancel

HER INDSAMLES EMAILS TIL NÆSTE SPAM KAMPAGNE

Deal.dk

Vind den nye iPad Air

Skriv din e-mail og deltag i lodtrækningen om den smarte iPad Air med 16 GB, WiFi og en vægt på under 500 gram. Med den i hånden er det altid nemt at tjekke dagens deal!

Ved deltagelse accepterer du samtidig at modtage den daglige tilbudsmail fra Deal.dk. Du kan altid afmelde dig igen.

Vinderen findes blandt alle, der har tilmeldt sig, senest den 1. november.

Tilmeld dig nu

Indtast din e-mail

Indtast postnr.

Ved tilmelding accepterer jeg at modtage daglige tilbud og nyheder fra Deal.dk via e-mail. Jeg kan altid afmelde mig denne service igen

Tilmeld og deltag

ODYSSEY TRAVEL

Enter for a chance to WIN an iPad Mini !

* 1. Title

Name:

Address 1:

Address 2:

City/Town:

State/Province:

ZIP/Postal Code:

Country:

Email Address:

Phone Number:

* 2. Which range best describe your age?

Below 20 | 21 - 29 | 30 - 39 | 40 - 49 | 50 - 59

60 - 69 | 70 or older | 65 or older

Vind et gavekort på 8.000kr til Imerco

Kære Veta R.

Du er en af finalisterne i den månedlige lodtrækning, som bliver gennemført af vores konkurrenceafdeling!

Spild ikke tiden og gå på nettet for at kunne modtage dit mulige gavekort på 8.000 kr til Imerco!

Dette er din eksklusive adgang som finalist

Tillykke med at du er blandt finalisterne!

Blockbuster: Ny ordre # 101620915 Indbakke x

BLOCKBUSTER - denne mail kan desværre ikke besvares <donotreply@blockbuster.dk>
til mig

Eksterne billeder. Vis billeder herunder - Vis altid billeder fra donotreply@blockbuster.dk

KVITTERING

Tak fordi du anvendte Blockbuster.

Ordrenummer: 101620915
Ordre dato: 23/05/2017 21.51.

Produkt		Varenummer	Antal	Subtotal
Dræberne fra Nibe	**Dræberne fra Nibe** Leje: 28 dage til at starte, derefter 48 timer til at se	VODK0000107770010001-RENT	1	49,00 ,-
			Subtotal	49,00 ,-

Blockbuster: Ny ordre # 101620915 Indbakke x

BLOCKBUSTER - denne mail kan desværre ikke besvares <donotreply@blockbuster.dk>
til mig

BLOCKBUSTER®

KVITTERING

Tak fordi du anvendte Blockbuster.

Ordrenummer: 101620915
Ordre dato: 23/05/2017 21.51.

Produkt	Varenummer	Antal	Subtotal
 **Dræberne fra Nibe** Leje: 28 dage til at starte, derefter 48 timer til at se	VODK0000107770010001-RENT	1	49,00 ,-
		Subtotal	49,00 ,-
		Moms	9,56 ,-
		Momsfri KODA-afgift	1,20 ,-
		Total	**49,00 ,-**


USERAGENTEN

Metadata afslører bl.a. mit operativsystem og min browser…

Sikker | https://developers.whatismybrowser.com/useragents/parse/

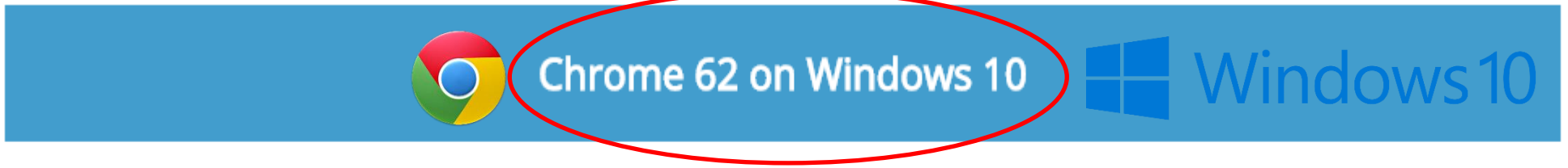
User Agents Search/Parse Detection API Log In/Sign Up | API

Homepage > User Agents > Parse User Agent

We detect the user agent:

```
www.lostserver.com:443 62.243.127.120 - - [07/Nov/2017:09:26:36 +0100] "GET / HTTP/1.
1" 200 8872 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
                like Gecko) Chrome/62.0.3202.75 Safari/537.36"
```

As:



LOCAL IP ADDRESS, COMPUTER SCREEN SIZE, BROWSER WINDOW SIZE, FONTS INSTALLED ETC..

Sårbarheds databaser

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database

FortiGate OS Version 4.3

exploit-db.com/exploits/39224

EXPLOIT DATABASE

Home Exploits Shellcode

FortiGate OS Version 4.x

EDB-ID: 39645

EDB Verified: ✖

Download Exploit:

« Previous Exploit

```
<?php

// PHP <=
// By Andr
// Should

// This ex
// format
// We fake
// through
// bug to
// then ed
// before
// makes i
// To my k
// credit
// https:/

// All the
```

EDB-ID: 39224 CVE: 2016

EDB Verified: ✖ Autho

Download Exploit: Source Raw Do

« Previous Exploit

```
#!/usr/bin/env python

# SSH Backdoor for For
# Usage: ./fgt_ssh_ba

import socket
import select
import sys
import paramiko
from paramiko.py3comp
import base64
import hashlib
import termios
import tty

def custom_handler(title, instructions, prompt_li
    n = prompt_list[0][0]
    m = hashlib.sha1()
```

SecurityFocus

About Contact

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

Join the conversation ›

info discussion exploit solution references

WordPress WP e-Commerce Plugin 'wpsc-user_log_functions.php' SQL Injection Vulnerability

Attackers can use a browser to exploit this issue.

The following exploit is available:

- /data/vulnerabilities/exploits/48717.txt

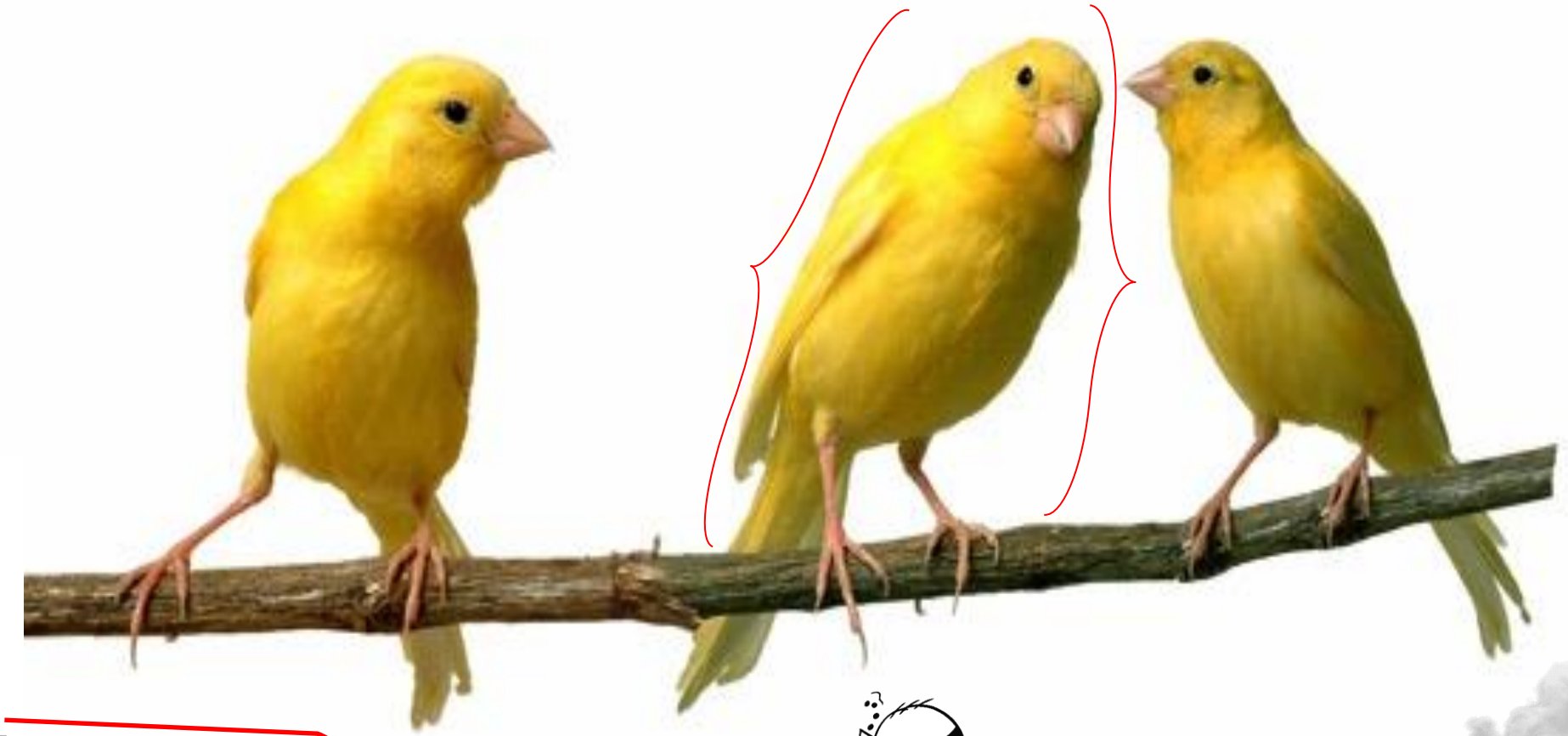
downloads.securityfocu

downloads.securityfocus.com/vulnerabilities/exploits/48717.txt

```
Original Advisory:
http://www.ihteam.net/advisory/wordpress-wp-e-commerce-plugin/
Plain text here:
http://www.ihteam.net/advisories/_561684984189_wp-e-commerce_384_sqli.tar.gz

    <?php
    /*
    WP e-Commerce <= 3.8.4 SQL Injection
    Download link: http://wordpress.org/extend/plugins/wp-e-commerce/
    Author contact: 29/06/2011
    Exploit published: 18/07/2011

    gged code (wpsc-theme/functions/wpsc-user_log_functions.php):
    each ( (array)$_POST['collected_data'] as $value_id => $value ) {
    sql = "SELECT * FROM `" . WPSC_TABLE_CHECKOUT_FORMS . "` WHERE
    '$value_id' LIMIT 1;
    ta = $wpdb->get_row( $form_sql, ARRAY_A );

    ade to new version

    by: IHTeam
    0T_ATI` Quatrini
    te_sheep` Rondini
    `merlok` Morucci
    picfail` Gasperini
    Shopped as their security auditors

    This code has been released under the authorization of GetShopped staff.
    It will show user_login and user_pass of wp_users table;

    Google Dork: inurl:page_id= "Your billing/contact details"
```

Vidste du at ”free wifi” er en sikkerhedsrisiko, selv efter du er logget af ?

MAN-IN-THE-MIDDLE



Dig
(og din computer
telefon, tablet etc..)

En hacker..

Internettet


På HOTEL
Wi Fi
Free Internet Access


PÅ CAFÉ
FREE
WiFi


TOG


TAXI

Free
Wi Fi

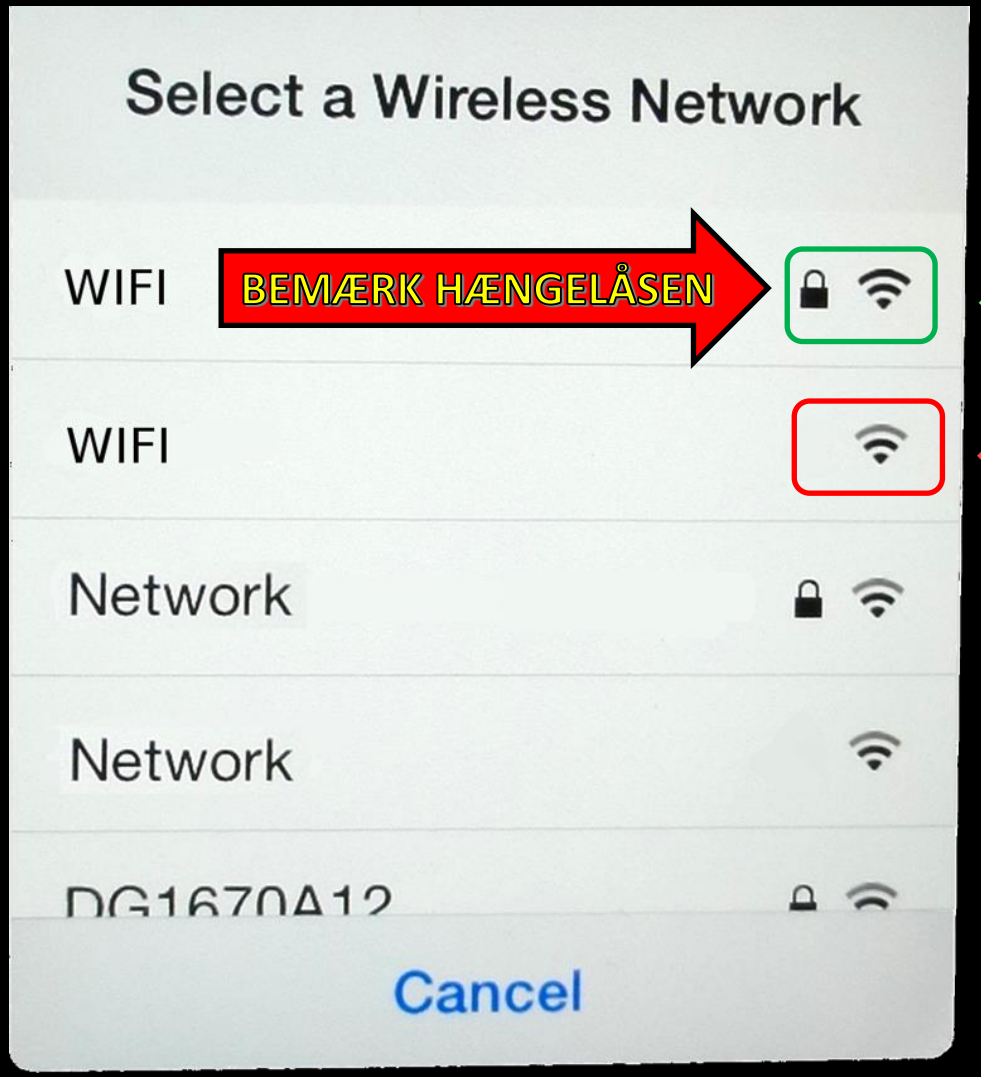

LUFTHAVN


HIMALAYA BJERGET


McDonald's
Free Wi-Fi served at all restaurants

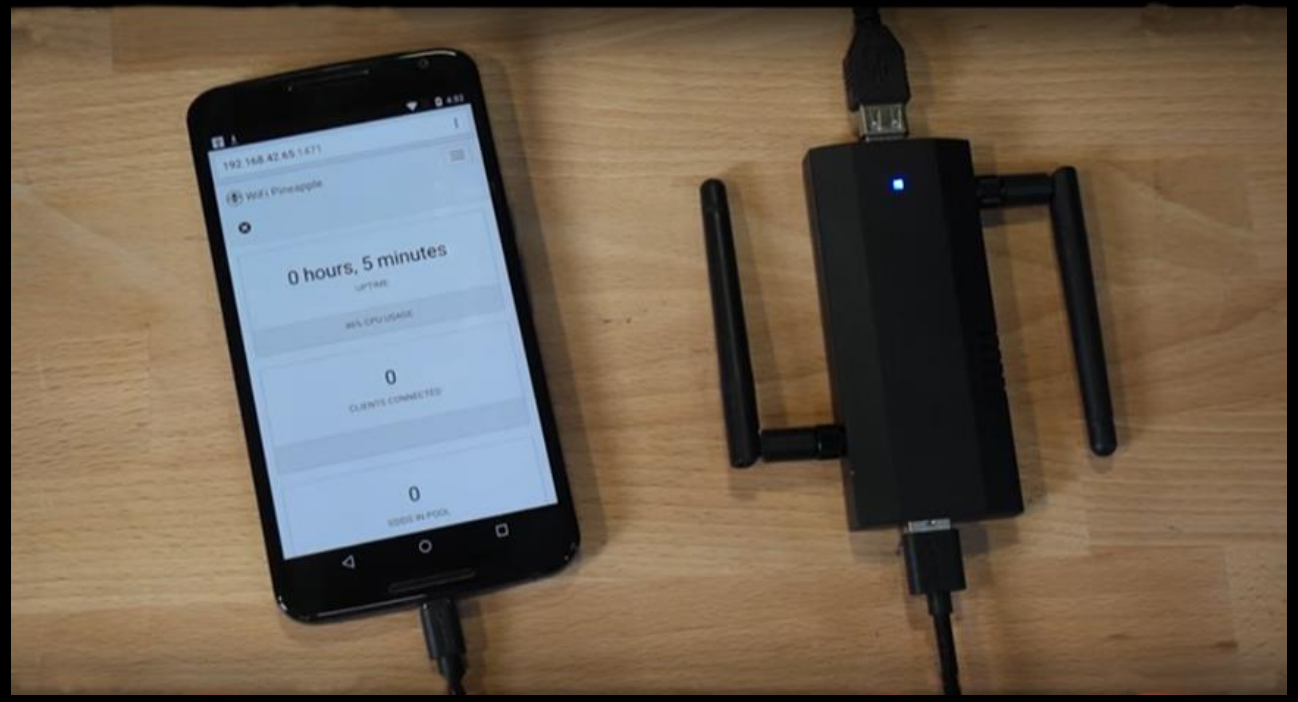

HJEMME

FORSKELLEN PÅ SIKRE OG ÅBNE NETVÆRK...



← SIKKER

← USIKKER



Den her hacker appliance kan kaldes for en Pinapple Nano

En ”NANO” koster $99

En ‘Pineapple Nano’ laver falske Wireless Access Points

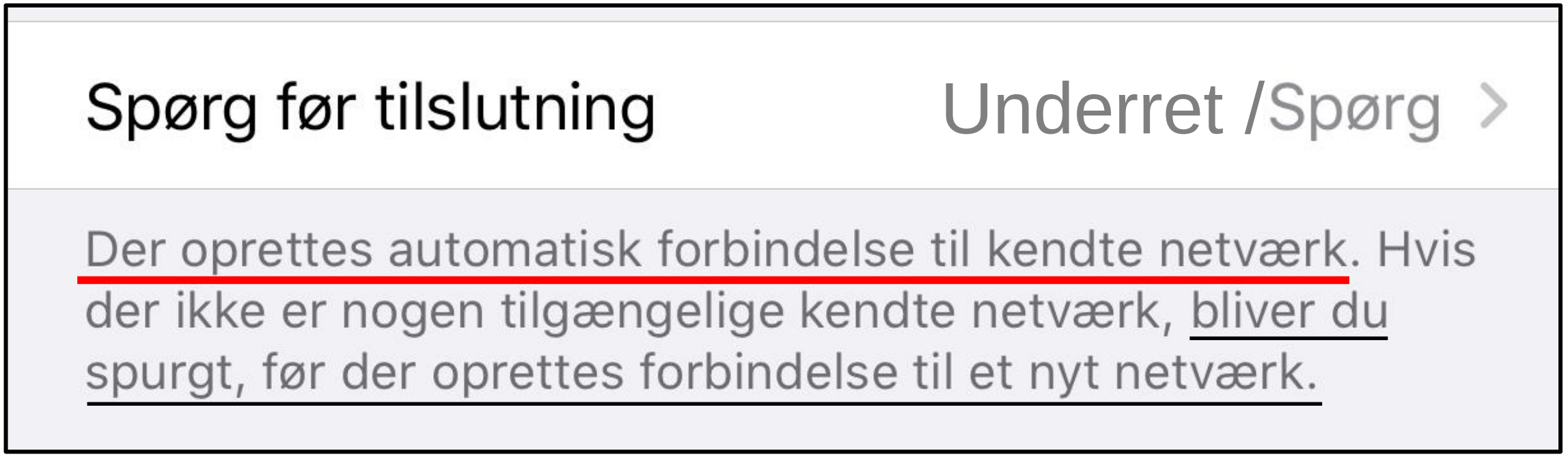
...og giver alle der forbinder sig til disse AP’er internet adgang.

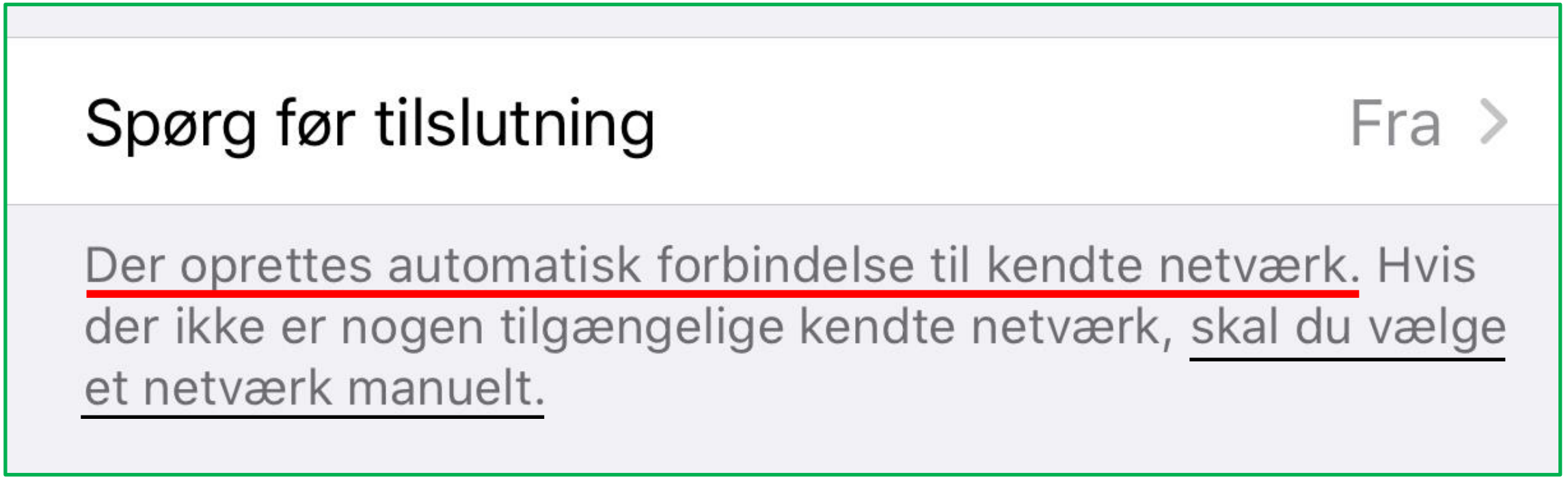
Dubex:


En hacker laver en masse falske trådløse netværk
De har navne som din telefon (måske) allerede kender og har Været logget i fordoms tid..
Eksempeltvis “CPH Hotspot”
(københavns lufthavns WiFi)


Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
Ikke sikre !
Futurelearn
Abraham Lynksys
BL Registered User
BL Staff BYOD
BL Visitor
Drop it like its Hot.....Spot
eduroam
Futurelearn Guest
FutureLearn Ruckus
I believe Wi can Fi
Life in the fast LAN
Martin Router King
Mum Click Here For Internet
No More Mr WI-Fi
Silence of the LANs
Tell my Wi-Fi love her
The LAN Before Time
The Promise LAN
Titanic Syncing
Wham Bam Thank you LAN
Wi-Fight the Feeling
Join Other Network...
Create Network...
Open Network Preferences...

TELEFONEN FORBINDER SIG AUTOMATISK TIL DE FALSKE(kendte) WIFI NAVNE


Spørg før tilslutning
Underret /Spørg
Der oprettes automatisk forbindelse til kendte netværk. Hvis der ikke er nogen tilgængelige kendte netværk, bliver du spurgt, før der oprettes forbindelse til et nyt netværk.


Spørg før tilslutning
Fra
Der oprettes automatisk forbindelse til kendte netværk. Hvis der ikke er nogen tilgængelige kendte netværk, skal du vælge et netværk manuelt.

MAILS OPSAMLES

BRUGERNAVN OG KODEORD OPSAMLES

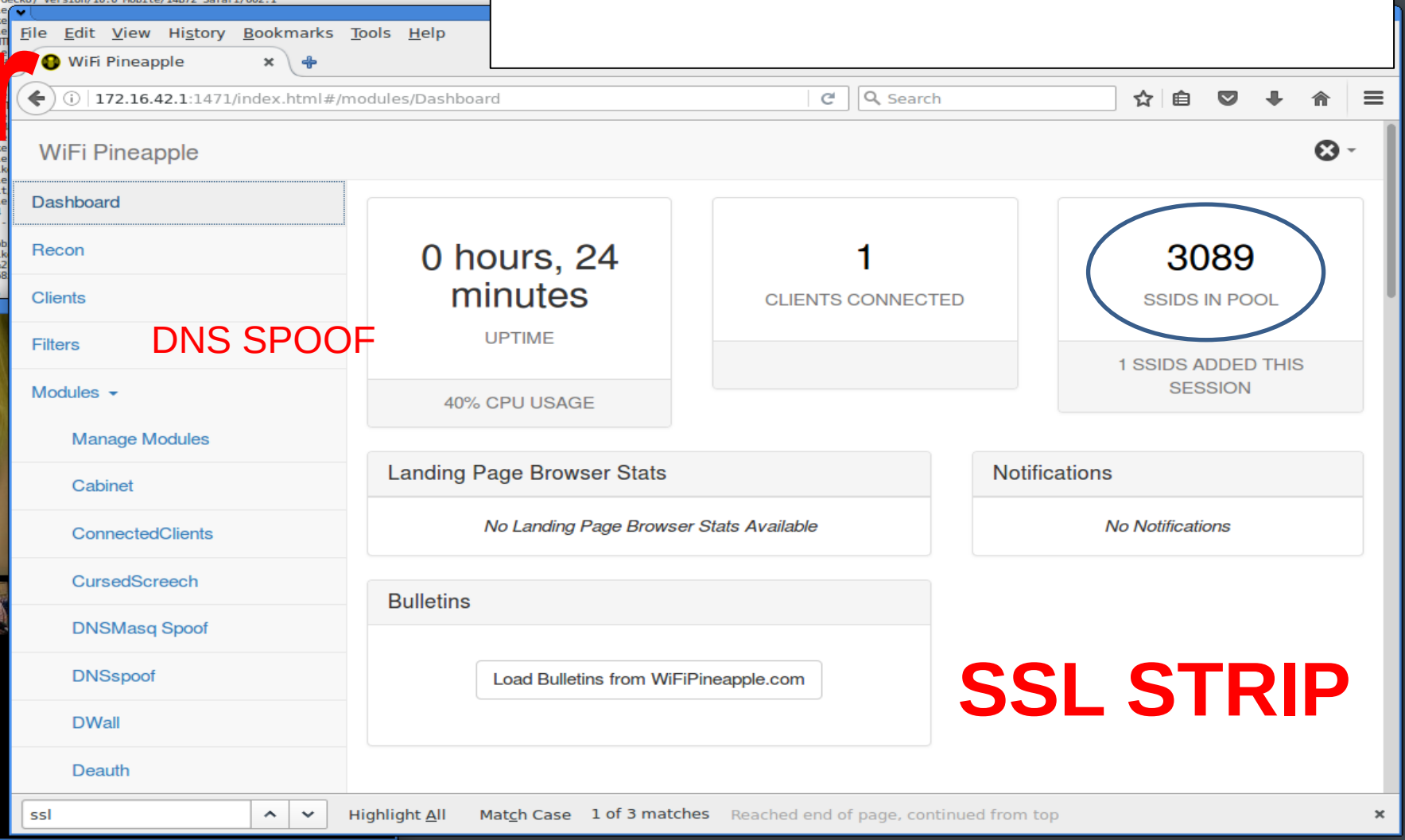
DATA ÆNDRES I REALTID

URL'er

DNS SPOOF

BILLEDER

SSL STRIP



[Qubes VM Manager] [user@Wifi: ~] driftnet Terminal Terminal Terminal WiFi Pineapple - Mozilla ... [user@Wifi: ~] [user@Wi

Office 365

Arbejds-, skole- eller personlig Microsoft-konto

cfo@dit-firma.dk

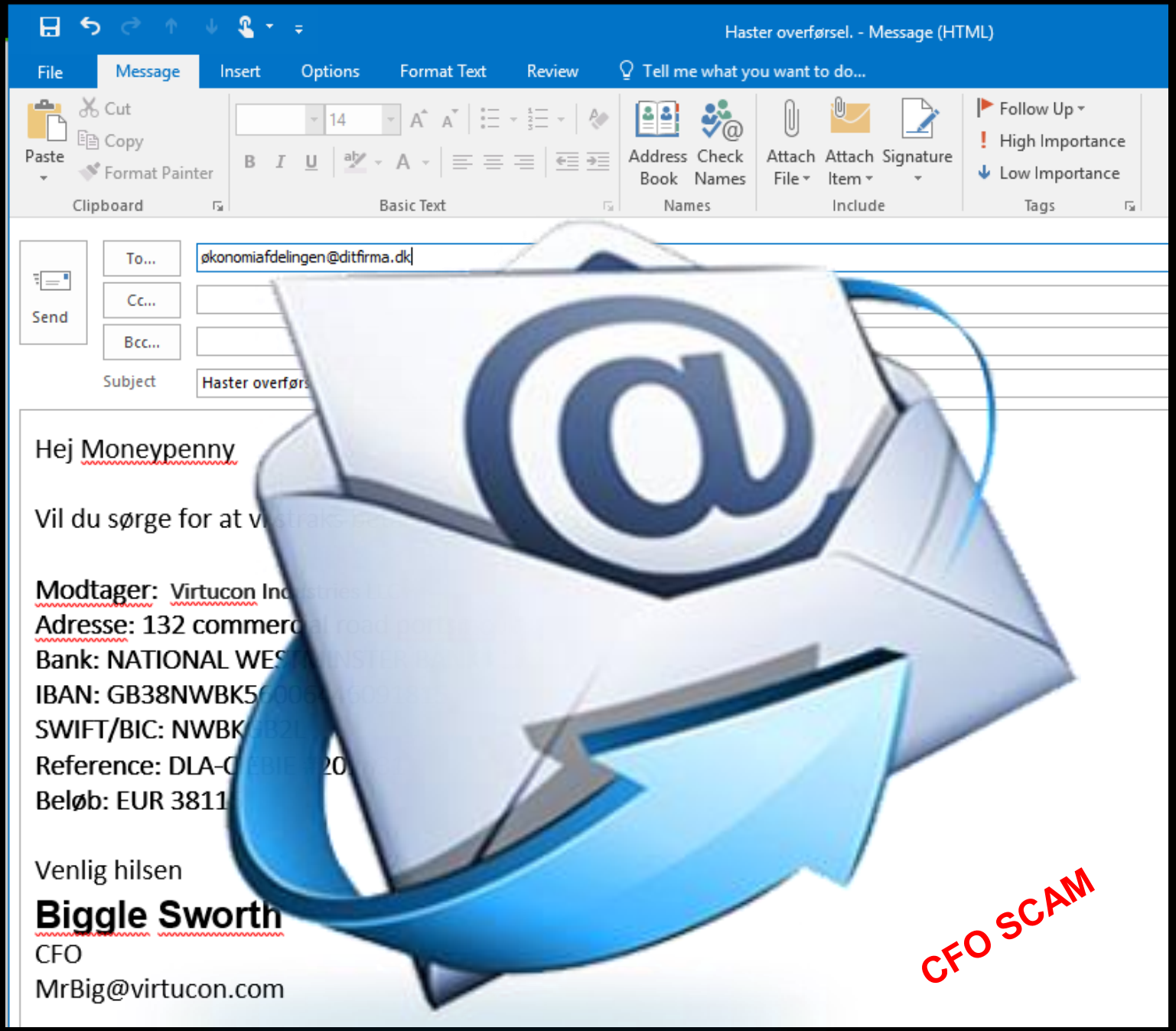
****

Log mig ikke af

Log på

Kan du ikke få adgang til din konto?

EN FALSK OFFICE 365 SIDE STJÆLER DIT BRUGERNAVN OG KODEORD



NU SENDER HACKEREN EN MAIL "INDEFRA"

AFSENDER ER EN KOLLEGA.

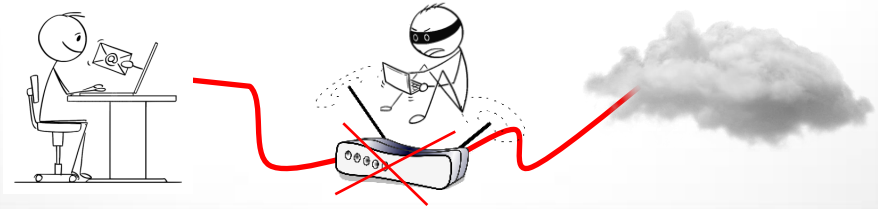
DET GØR PHISHINGEN MERE TROVÆRDIG.

Dubex:
MANAGING RISK. ENABLING GROWTH.

Here we go again...

Virtual Private Network

VPN SIKRE DIN KOMMUNIKATION VED AT KRYPTERE LINIEN MELLEM DIN ENHED OG ET SIKKERT EXIT POINT, HVOR DU SÅ TILGÅR INTER-NETTET FRA

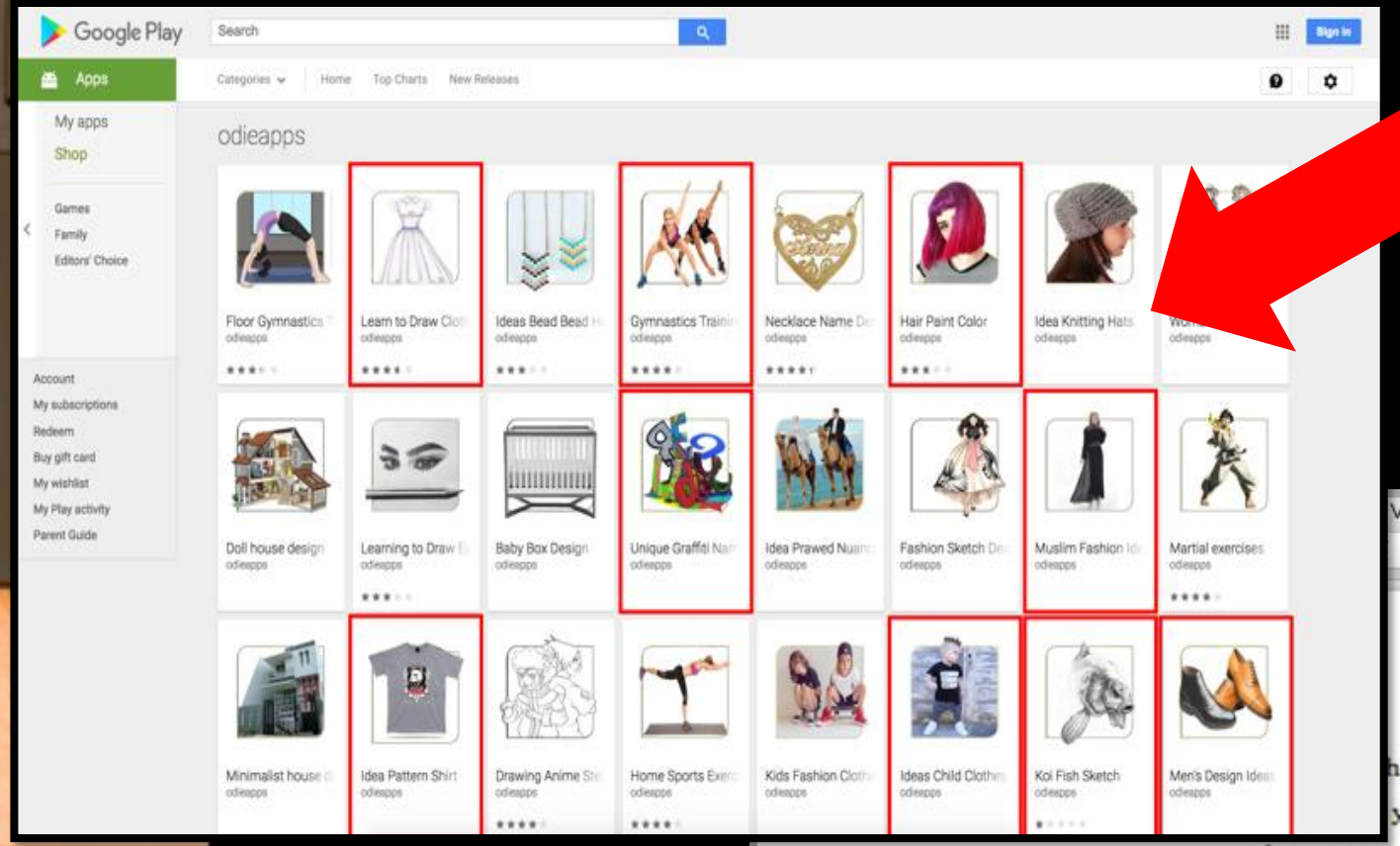


Dubex:
MANAGING RISK. ENABLING GROWTH.

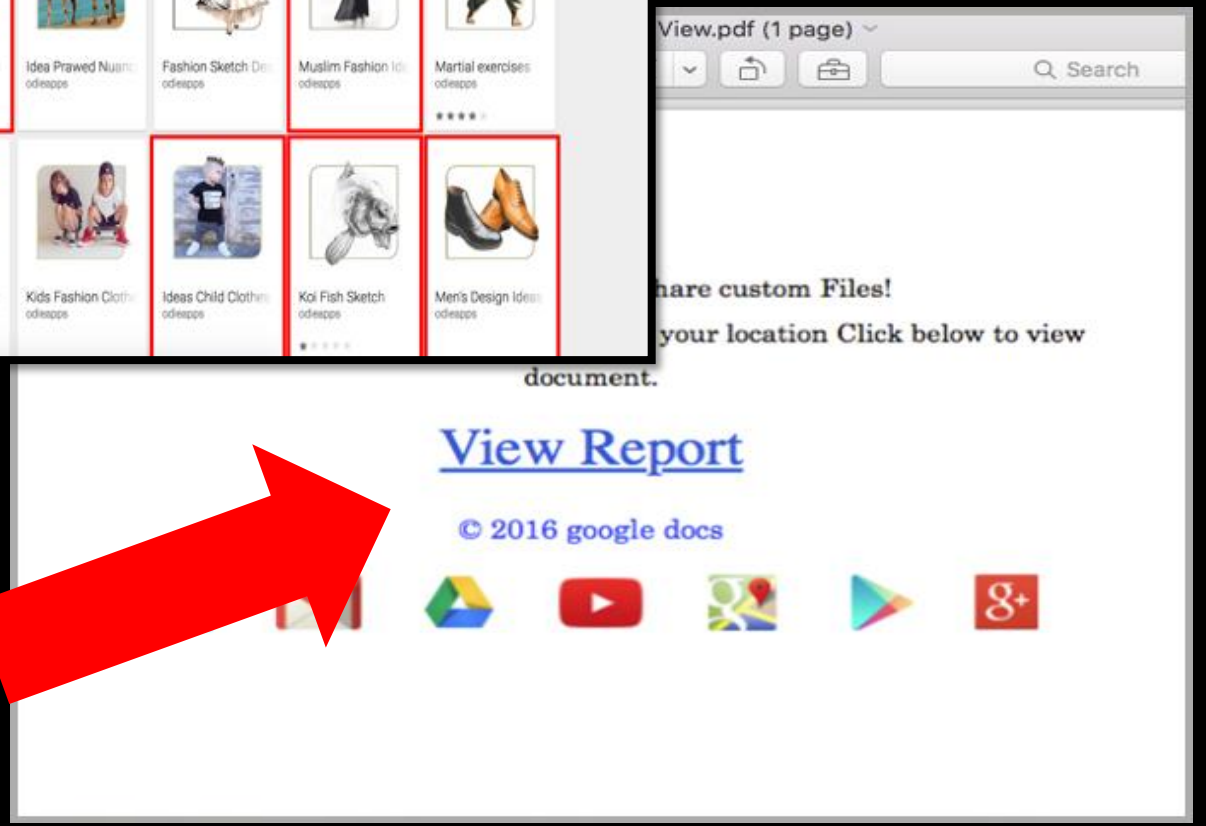
LINK

Telefonen inficerer PC'en

Her ses 145 programmer til Android telefoner i Google Play store inficeret med Windows malware..



..med indbygget windows keylogger

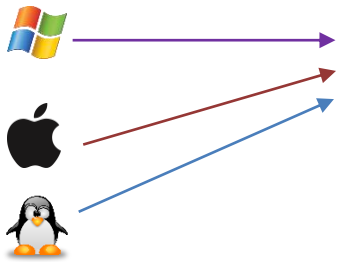


Dokumenter der "kun" Kan læses på en PC

..med makroer i der inficerer PCen

ZERODIUM Payouts for Desktops/Servers*

Hack en Windows 10 Klient
Pris: 6 mil. DKK



Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000										1.001 Win RCE Zero Click Win
Up to $500,000								3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux	
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux		4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux		
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux	
Up to $80,000	6.002 VMware WS VME Win/Linux				5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win		
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win		5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD		
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux	

*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

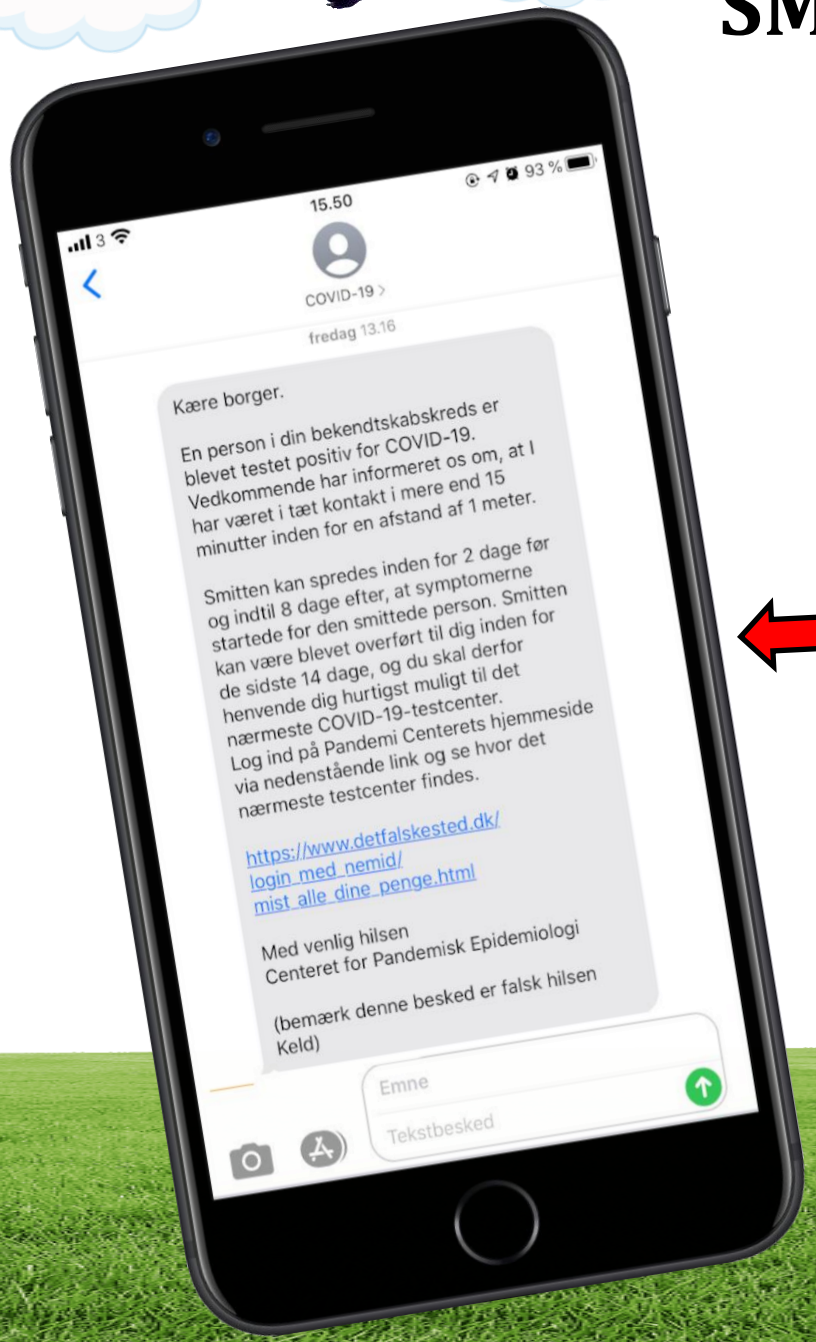
IOS
Android
Any OS

iPhone (ios)
12 mil. DKK

Android
ca. 15 mil. DKK

Up to $2,500,000									1.001 Android FCP Zero Click Android	
Up to $2,000,000										1.002 iOS FCP Zero Click IOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click IOS/Android		2.002 iMessage RCE+LPE Zero Click IOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE IOS/Android		2.004 SMS/MMS RCE+LPE IOS/Android
Up to $500,000	3.001 Persistence IOS	2.005 WeChat RCE+LPE IOS/Android	2.006 iMessage RCE+LPE IOS	2.007 FB Messenger RCE+LPE IOS/Android	2.008 Signal RCE+LPE IOS/Android	2.009 Telegram RCE+LPE IOS/Android	2.010 Email App RCE+LPE IOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE IOS	
Up to $200,000	5.001 Baseband RCE+LPE IOS/Android		6.001 LPE to Kernel /Root IOS/Android	2.011 Media Files RCE+LPE IOS/Android	2.012 Documents RCE+LPE IOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari IOS	4.006 Safari RCE w/o SBX IOS	
Up to $100,000	7.001 Code Signing Bypass IOS/Android	5.002 WiFi RCE IOS/Android	5.003 RCE via MitM IOS/Android	6.002 LPE to System Android	8.001 Information Disclosure IOS/Android	8.002 [k]ASLR Bypass IOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass IOS	9.003 Touch ID Bypass IOS	

SMS & Caller ID spoofing



Smishing

Vishing

verizon Data Breach Investigation Report

81 %

af alle digitale indbrud sker med stjålne eller “dårlige” kodeord

KODEORD

Gode kodeord og to faktor…

Den mest brugte kodeordspolitik:

Settings

Your info

KELD NORMAN

DUBEX\kno

- Brugerens rigtige navn må ikke indgå i koden
- Minimum 8 karakterer
- Mindst 1 lille og 1 stort bogstav
- Mindst 1 tal + 1 special tegn

Den typiske password adfærd

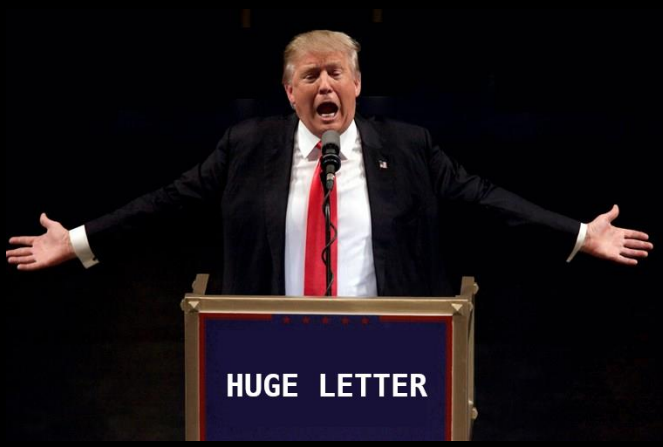
8

Hvis passwordet skal være på minimum otte tegn

…er det oftest kun på otte tegn

Ref.. Fra forsvarets efterretningstjenestes kodeords vejledning 2016

A a



Skal passwordet indeholde et stort bogstav, bliver det store bogstav typisk anbragt som det første bogstav i passwordet

Alle_mine_k0der_starter_med_1_stort_bogstav

Dubex:

Mon du har tallet 0
eller 1 i dit kodeord ?

min1k0de

P@ssw0rd2021

1

Hvis passwordet skal indeholde tal, bliver disse ofte angivet mellem 0 og 99 eller som årstal og gerne placeret til sidst.

0

Det er også almindeligt at ændre bogstaver med tal.
”e” bliver f.eks. til ”3”, ”o” bliver til ”0” osv.

Telefon
nummeret

123

Post
nummeret

@ ! .

Kravet om specialtegn løses i mange tilfælde ved at bruge ét.

Snabel-a (”@”) og udråbstegn (”!”) er nogle af de mere populære.

Hemmelig1.

V@ndmand1

Mink0de!

Shift + 4

Dubex:

Vinter2021!

Skal passwordet ændres med faste mellemrum,

er der mange brugere, der anvender cykliske ord
i form af ord for årstider, kvartaler, måneder osv.

(der vælges tit et kodeord som er næsten identisk med det tidligere)

H@nsJens1!

MinK@tBing0

Vuffe123!

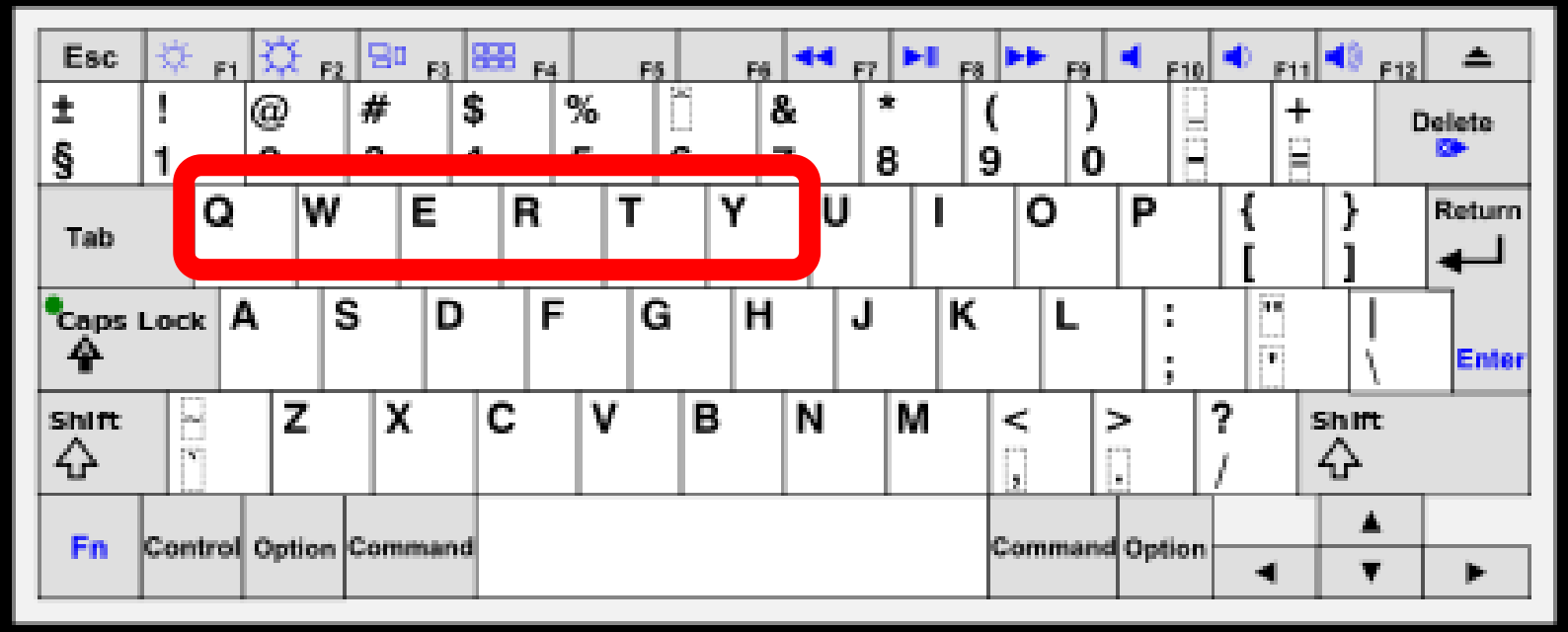
Passwordet er det samme som brugernavnet eller en del af det.

Passwordet består af navne på familie, venner, husdyr osv.

(og ting der er omkring folk når de skal "finde på..")

Dubex:

De mest brugte passwords er bl.a. ”123456”, ”password”,
og bogstavrækker som f.eks. ”qwerty”,
der følger rækkerne på tastaturet.



Den perfekte verden: alle dine kodeord er forskellige!

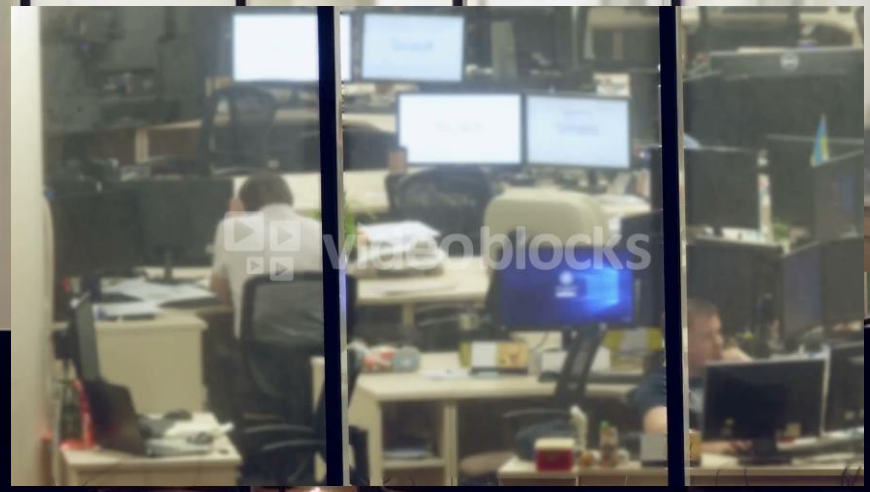
…Og du kan huske dem

Den faktuelle verden...

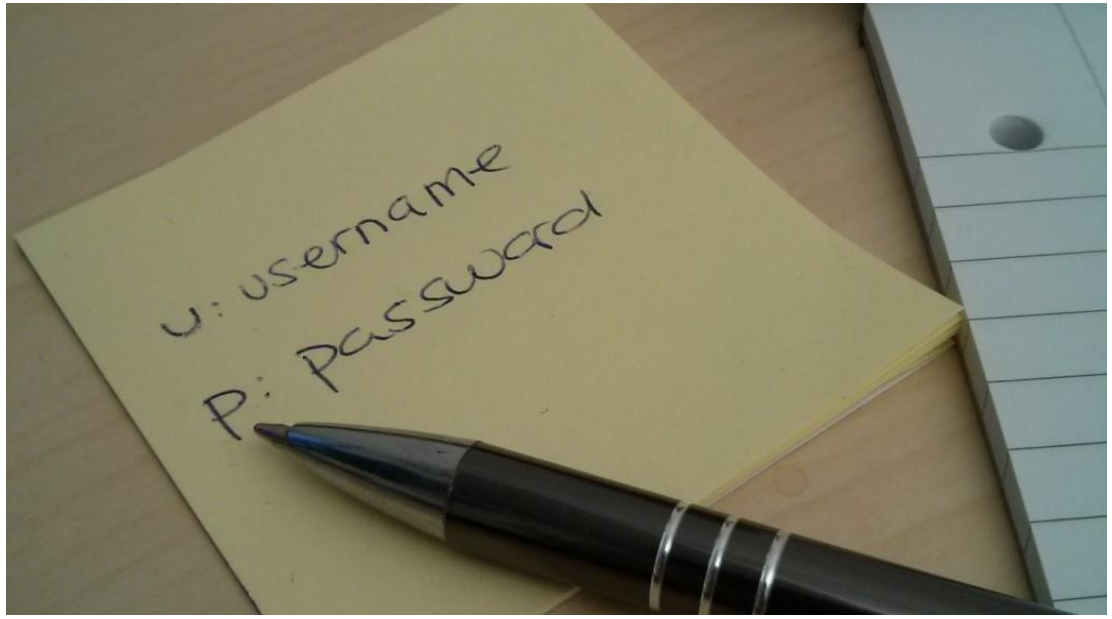
Mange bruger samme login og kodeord på forskellige hjemmesider.

Når en hjemmeside bliver hacket, (login og kodeord bliver kendt af hackerne) kan hackerne få adgang til alle de andre sider...

Kig ind ad vinduet…



Det er godt at have forskellige kodeord, men at huske dem er svært..



Den franske TV station
TV5 Mondes kodeord til deres
YouTube konto

De stoppede
udsendelsen
senere den dag...

DATA SECURITY BREACH

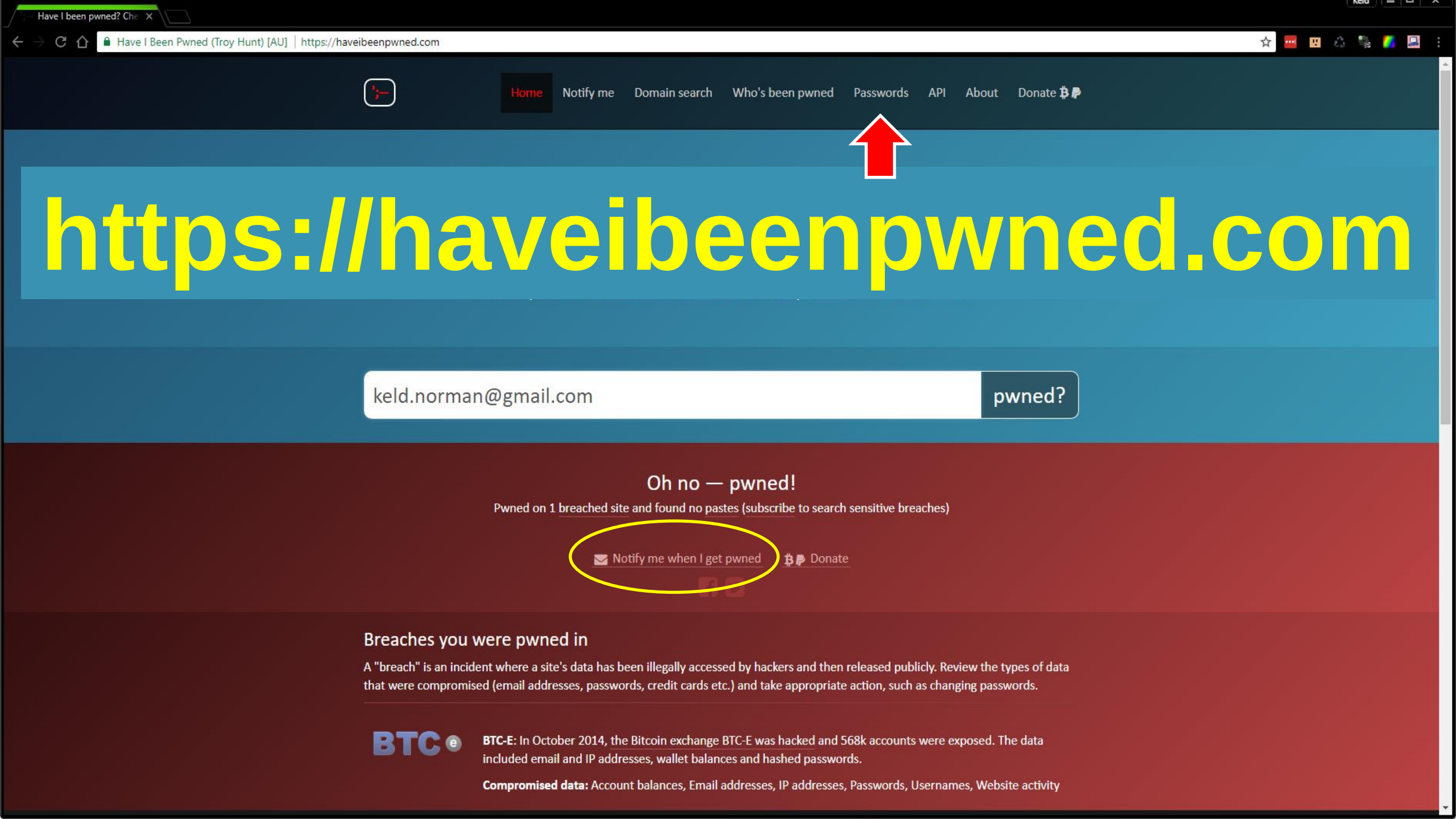
Kodeords databasen bliver stjålet og lagt på nettet ..

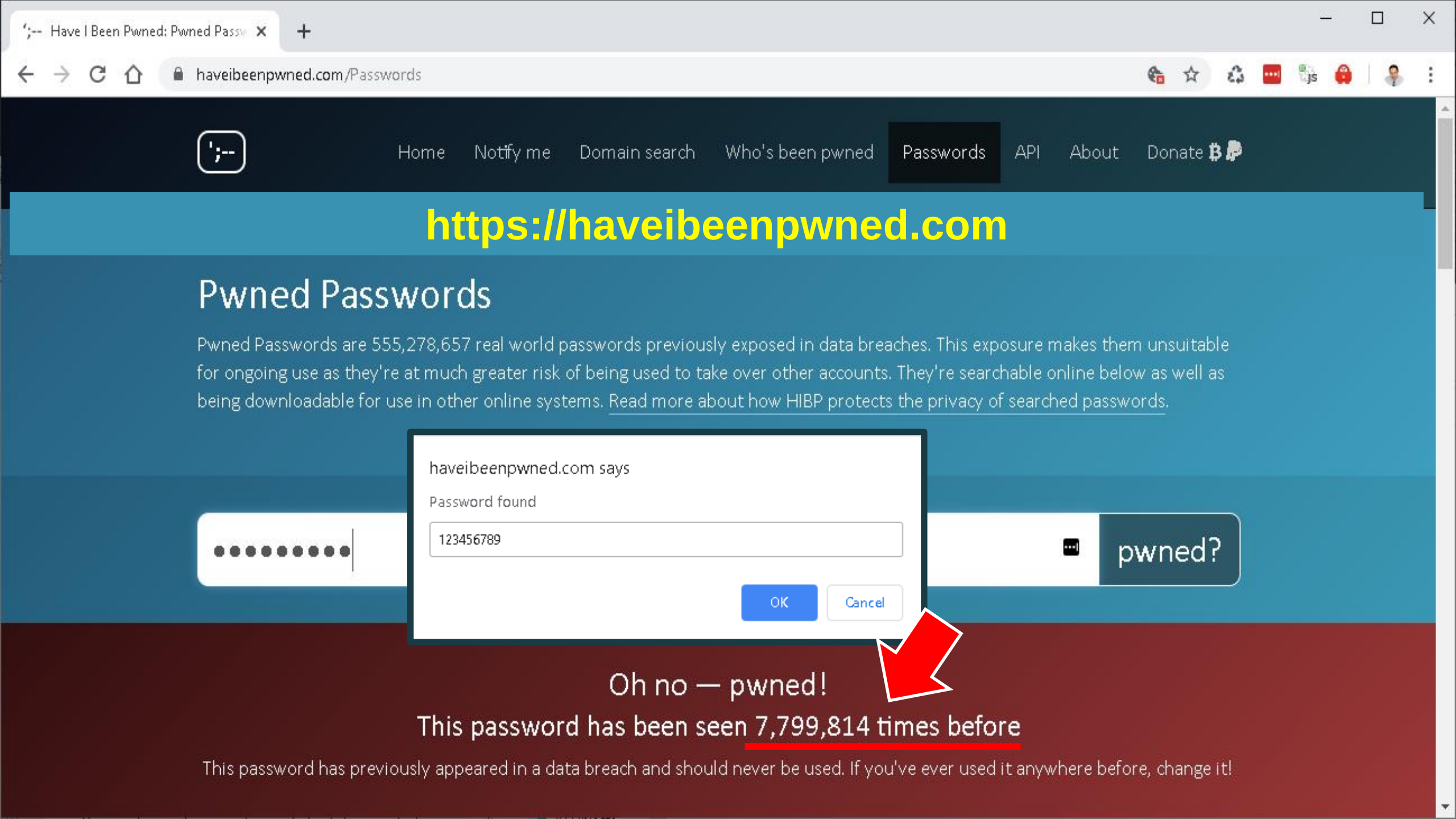
Bruges til SPAM mails

Prøv login på alle sociale medier og gratis mail tjenester

Sextorsion / hacking påstand

Herefter sælges/ligges dataleak dataen ud til offentlig skue


Have I been pwned? Che
Have I Been Pwned (Troy Hunt) [AU]
https://haveibeenpwned.com
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
https://haveibeenpwned.com
keld.norman@gmail.com
pwned?
Oh no — pwned!
Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)
Notify me when I get pwned
Donate
Breaches you were pwned in
A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.
BTC e
BTC-E: In October 2014, the Bitcoin exchange BTC-E was hacked and 568k accounts were exposed. The data included email and IP addresses, wallet balances and hashed passwords.
Compromised data: Account balances, Email addresses, IP addresses, Passwords, Usernames, Website activity


Have I Been Pwned: Pwned Passw
haveibeenpwned.com/Passwords
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
https://haveibeenpwned.com
Pwned Passwords
Pwned Passwords are 555,278,657 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.
haveibeenpwned.com says
Password found
123456789
OK
Cancel
pwned?
Oh no — pwned!
This password has been seen 7,799,814 times before
This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

pwndb

pwndb2am4tzkvold.onion

Min Onions Search | NukeShop | Kategorier | Polite NL | Meld Anoniem | FBI TIP | Andre Bookmarks

pwndb

Email

% @ nsa.gov

like = email

Password

password

@ nsa.gov

=

1
Array
(
[id] => 3707647
[luser] => 123456
[domain] => nsa.gov
[password] => P94cgD4v92B
)

2
Array
(
[id] => 32317283
[luser] => aatsamo
[domain] => nsa.gov
[password] => kiki1964
)

3
Array
(
[id] => 34612920
[luser] => abenedi
[domain] => nsa.gov
[password] => ab06131982
)

4
Array
(
[id] => 36212393
[luser] => absimm2
[domain] => nsa.gov
[password] => player

DARK WEB GRATIS PASSWORD LEAK SEARCH

adasdk@ds.dk
asd.dk@ds.dk
bbe@ds.dk
bc@ds.dk
bj@ds.dk
bk@ds.dk
bn@ds.dk
bp@ds.dk
cb@ds.dk
ccs@ds.dk
cda@ds.dk
cdsad@ds.dk
cly@ds.dk
cmv@ds.dk
crf@ds.dk
ctk@ds.dk
dfd@ds.dk
ds@ds.dk
dss.ds@ds.dk
em@ds.dk
ert@ds.dk
fda@ds.dk
fs@ds.dk
gep@ds.dk
gs@ds.dk
hd@ds.dk
hes@ds.dk
hhb@ds.dk
hhk@ds.dk
hj@ds.dk
hln@ds.dk
hpl@ds.dk
ih@ds.dk
ja@ds.dk
jak@ds.dk
jasq@ds.dk
jea@ds.dk
jeh@ds.dk
jej@ds.dk
jel@ds.dk
jfl@ds.dk
jgr@ds.dk
jjc@ds.dk
jny@ds.dk
jso@ds.dk
kat@ds.dk
kba@ds.dk
kc@ds.dk
kkc@ds.dk
kkc@ds.dk
kpe@ds.dk
ksoe@ds.dk
kt@ds.dk
lar@ds.dk
lbs@ds.dk
lhg@ds.dk
lho@ds.dk
lj@ds.dk
lk@ds.dk
lmg@ds.dk
lmh@ds.dk
ln@ds.dk
ltp@ds.dk
mads19991
ma@ds.dk
mag@ds.dk
mav@ds.dk
mba@ds.dk
mdj@ds.dk
mgc@ds.dk
mgr@ds.dk
mh@ds.dk
mtj@ds.dk
mwb@ds.dk
oc@ds.dk
os@ds.dk
pak@ds.dk
pan@ds.dk
pd@ds.dk
pen@ds.dk
pg@ds.dk
pi@ds.dk
pjn@ds.dk
pkj@ds.dk
pl@ds.dk
pn@ds.dk
pr@ds.dk
ps@ds.dk
pte@ds.dk
qa@ds.dk
rad@ds.dk
ras@ds.dk
rn@ds.dk
rsa@ds.dk
rs@ds.dk
sbe@ds.dk
scl@ds.dk
sda@ds.dk
sebastian@ds.dk
sk@ds.dk
sos@ds.dk
ssh@ds.dk
tap@ds.dk
tm@ds.dk
tok@ds.dk
tt@ds.dk
tumle@ds.dk
ujg@ds.dk
vdh@ds.dk

~ 108 unikke login navne (emails)@ds.dk

!
andrews_a_mofuckin_pimp
Bailey
bergen666
bibi1212
bivasa39
bj000917!!
bjarne
Bluefeather
Bobo2036
bpe4172
Britta
Carsten263
clb091169
cya57jhd
danielmette
dfsds
dGXAyi8Y
drtama
edda6107
em
Engbakken4
ERT497
espn3385
F91mc
frederik0101
gaara123
Heidi4040
henrik
HHPeWslj
HLNlinkedin
holmkuszon
jannekjxe6rulff
lummerkrog
mariebring
mia1emil2
miaemil
mnoj9r
mopenaka
mtjjjj
soagdsag122
sommerfis
ssyl8657
Stussi
superman
susben
sverige2
2800pan
12345qwertasdfg
060664
111213
280567
300350
654321

Fandt 225 kodeord i en søgning på @ds.dk

jebr7743
jk3041
mulamygy
MwBmFj
telefon
Troels1234
12345678m
26270514
1612851251
283730013856701

65 af koderne indeholdt tallet 1

jla2109
Jorgensen2160
josse5189
Kalle1234
kc9630
kodedef1
lakl
laklпїSder
laklPїC—P…der
lalla123
lucas1
nimbus2000
norholt1212
orkide
orkide=666
oschigosch
pejo7070
rasmus
regnskab
scl130552
sebs251199
skaGway00
tuxizuno
viborgvej
vinter10
winston
wucaresi
yowsn
zxnzxnzxn
1wazz1
1WPH29Tk
99kris90
1066hastings

4af0e222af1ff812f0d12e58f894381f
229c5be1f63c0eac40d2c8a0ee839e6c
ba77528450a32ef7aca1a3e2f8946fe6
Df0d13add5bccd54566393d44a7abf7e
Af7d5543255ee9ea8eab5122813387be
ce382dcaa74844c3b992c85d57cdaa52
E7ddedc9c10eb139b4b919a5a43d6645
6a78e4a3ec47684785a4e8b6384624a9
2bd030aece8317454b330e2b4749bca7
1f243fcf5769df9c5e6767980989c944bf9fca8b
2e67fb63fd00cd726ecdffb6dbfcb669681071c6
22f0fb8f4856c1ec0d0885f5c2bb63cc869db97b
d801f2de643d3a73dc2fbce28d102f975914cacc
9c377ca1f72db83a72c112e142e27ff9cc88a055
05ab6380fb09beb31f26dcdfd5ebe2438c859f52
ff96ec2b6a9c1882289925688b7fc1328aeb968e
2c0b37a68ef511e13d07d4b66485c25df3da5fd4
3bc15c8aae3e4124dd409035f32ea2fd6835efc9
336e074eeadb44b0f87f1f2782c36dc3414202b1
852cab59ef8256bb59c5f0286bbf726139134a36
29da73c666a166ba7bf4760280b33fa081337196
159ff5361d768ae28c0a75e0993506cd0545d086
afb4ac886e7b1d88437864708405bc640a641394
c088ac92cab5be361043383bed805e98d07001f8
d1774dcd30d7fb1201e72825548b7bae4805d19a
e1d2a8dc1507c851e0e6f1bb8b86a5b3d6b51d88
056737b17a9752bd3686cd5b81e6e55841d462f3
ed2944880803c12849ac66ae156ec65db2953d67
1m/FYNGrLQt7/8fGIYqH/pygbqMVThkoZiwx7NwViBs=

MD5 SHA-1 SHA-256 BCrypt

CRACKING AF KRYPTEREDE KODEORD...

Computerkapacitet	Tid (7 tegn)	Tid (10 tegn)	Tid (12 tegn)
Standard-desktop PC	Ca. 8 dage	208 tusinde år	2 milliarder år
Hurtig desktop PC	Ca. 2 dage	52 tusinde år	459 millioner år
GPU – PC	18 timer	21 tusinde år	184 millioner år
Hurtig GPU	9 timer	10 tusinde år	92 millioner år
Parallelle GPU'er	54 minutter	87 år	9 millioner år
Mellemstort botnet	1 sekund	6 dage	2 tusinde år

Scrypt PBKDF2 Argon2

Ref: fe-ddis.dk (2016)

CLOUD CRACKER OG BOTNETS…


WIFI WPA(2) Password Crack | O
onlinehashcrack.com/wifi-wpa-rsna-psk-crack.php
OnlineHashCrack
Professional Password Recovery
HOME
PASSWORD RECOVERY
Hash, WPA, Office, PDF, Archives,..
WIFI / WPA(2) PASSWORD RECOVER
Send us your WPA(2) dump.
If you have issues with upload contact us! Want to know what's next ?
De første 10 karakterer er gratis...
Upload your WPA(2) capture file:
Vælg fil
Der er ikke valgt nogen fil
Accepts *.cap or *.pcap or *.pcapng or *.hccapx
Max size: 100 Mb
Process all ESSID(s)
Extract PMKID(s) if available

Hvad er et godt kodeord ?

En kodeords generator

Tilbage

Adgangskode:

6jZOeAF13l7Pbi7ohnp2

Kopiér adgangskode

Adgangskodens længde:

20

Avancerede muligheder:

- (•) Tillad alle karakterer/tegn
- ( ) Gør det til at udtale
- [x] A-z [x] a-z [x] 0-9 [ ] !%@#
- 1 Minimum Numeric Characters
- [ ] Undgå karaterer med flere betydninger

Annuller | Brug Kodeord

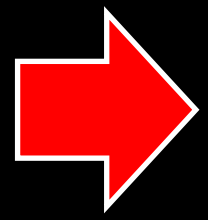
De her karakterer gør det tit svært for hackerne at benytte dem, i deres engelsk sproget programmer:

æ ø å

Æ Ø Å

her er Æ Ø Å

her er æ ø å



her er å ÿ à

her er ª ¬ Ñ

De her karakterer ødelægger tit hackernes kodeords lister:

:

:

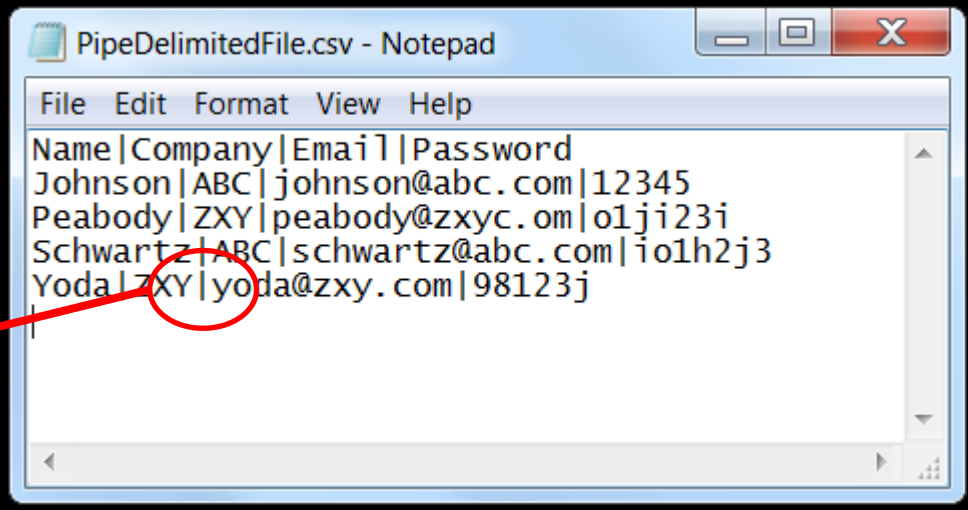
;

.

,

|

[mellemrum]



Fordi de benyttes som skilletegn mellem felter i deres lister

Et Plugin i din browser husker alle dine kodeord

KeePass

Sticky Password

dashlane

Det er dansk!

PASSWORD CRYPT
pcrypt.dk

RoboForm

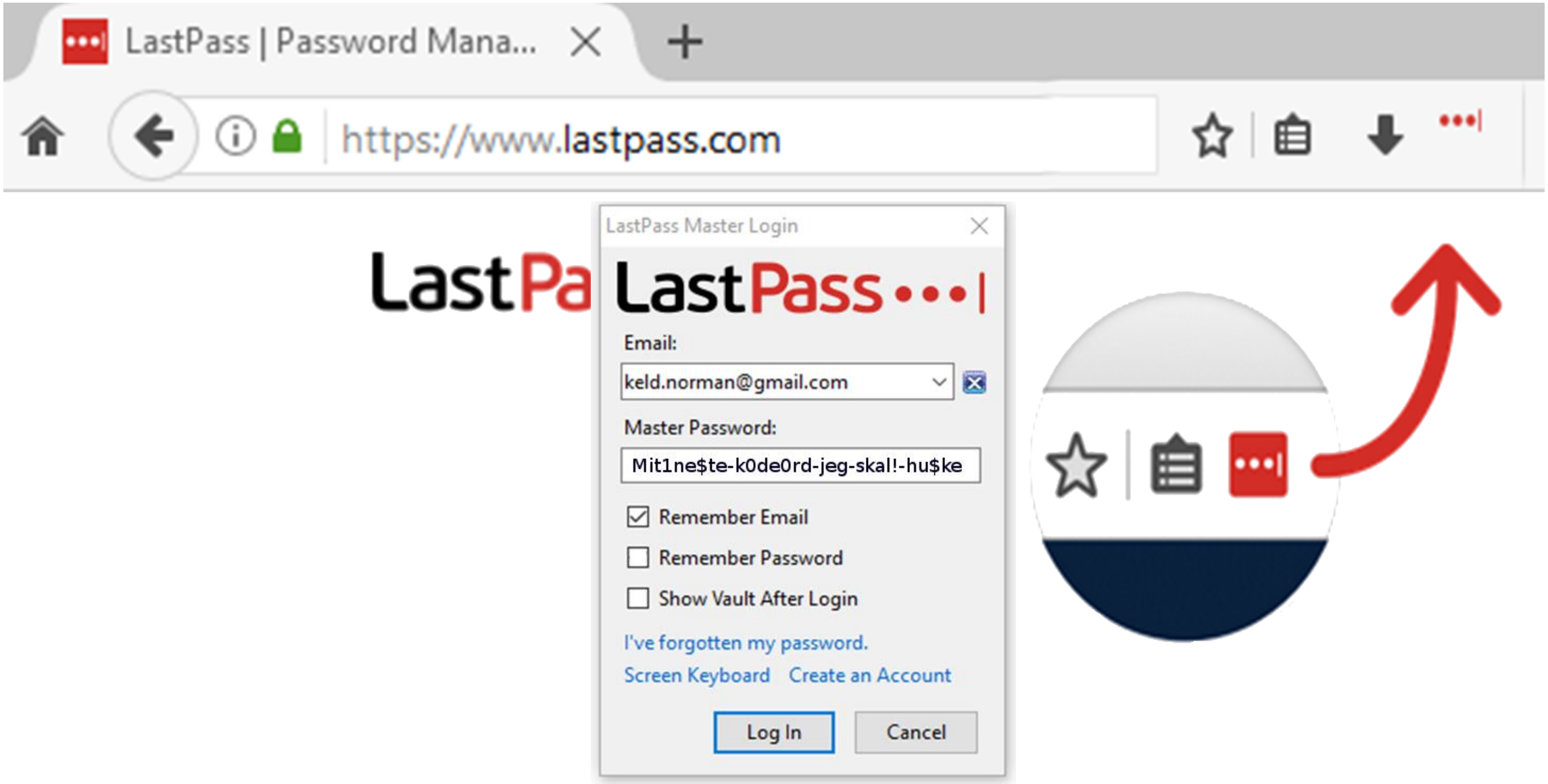
LastPass ****

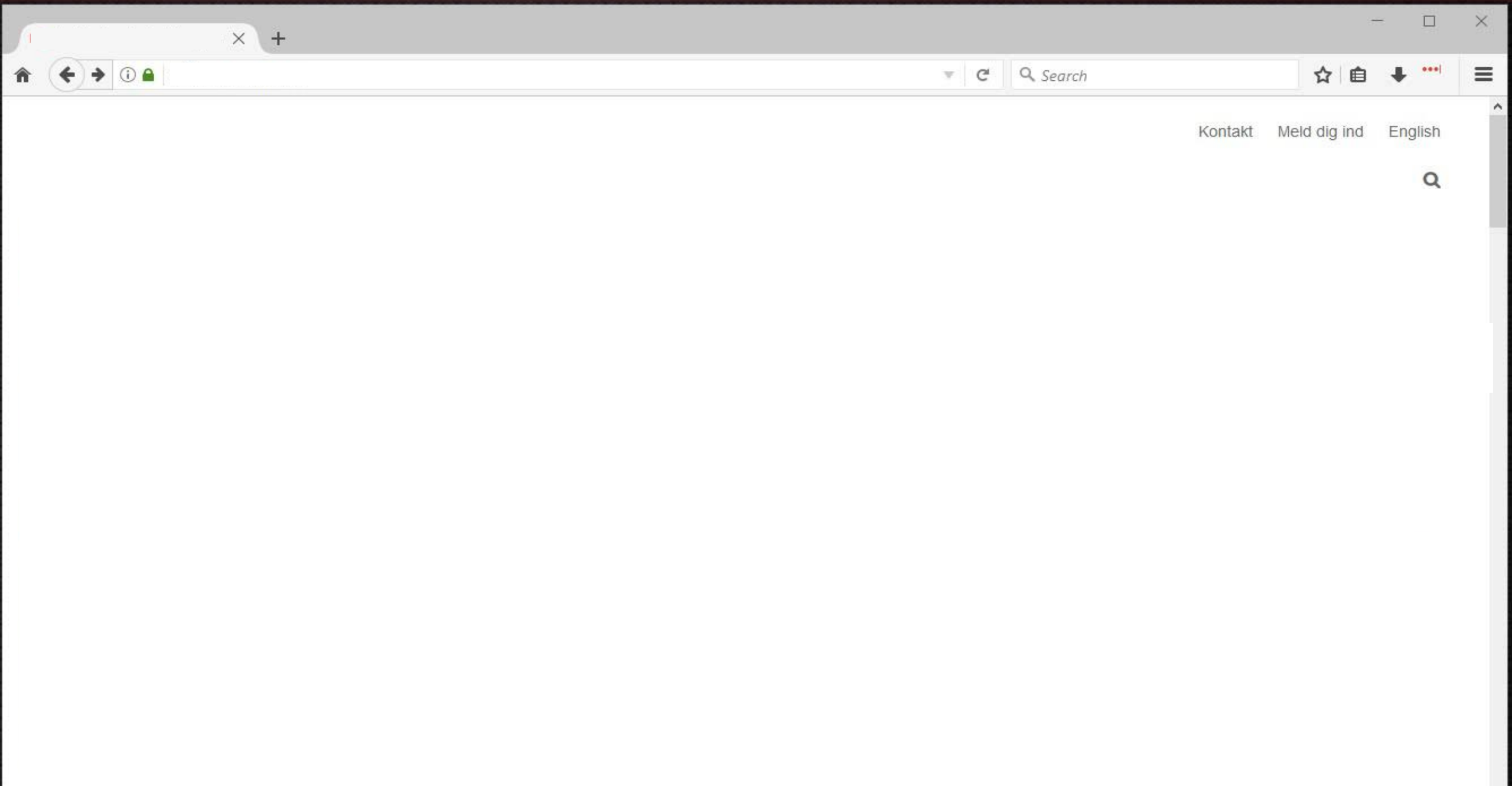
keeper

1Password

PasswordBox

Hvordan virker en password manager ?




Search
Kontakt
Meld dig ind
English

Risiko og konsekvenser...

RESEARCHER WARNS OF SECURITY HOLE IN KEEPASS PASSWORD MANAGER

by Paul Roberts — June 27, 2012 , 10:55 am

Users of the free, open source KeePass password manager got unwelcome news on Tuesday, after a private security researcher claimed to have discovered a remotely exploitable security hole that could give an attacker access to unencrypted user passwords. However, KeePass's creator calls the hole minor, and unlikely to be used in an attack.

Researcher Benjamin Kunz Mejri of Vulnerability Lab said in an e-mail to Threatpost that he had discovered the hole in a software filter and validation feature in KeePass Password Manager up to and including v1.22. If exploited, the hole would enable an attacker with access to a machine running the KeePass software to inject malicious script by passing the html/xml export feature a specially crafted file.

Hacked

lifehacker

LastPass Hacked, Change Your Master Password Now

Eric Ravenscraft — Filed to: HACKED — 6/15/15 12:30pm

Bad news first, folks. LastPass, our favorite password manager (and yours) has been hacked. It's time to change your master password. The good news is, the passwords you have saved for other sites should be safe.

Intel Buys ID Security Firm PasswordBox

By Jeffrey Burt | Posted 2014-12-01 Print

Twitter 64 LinkedIn 7 Like 17 Share 88

The deal … startup … s secu… and gives … ords … consumers … data.

Intel is bulkin… security and … capabil… with the acquisition … swordBox, a … D management startup whose … gy enables users to do such tasks as log into We… without having to memorize their passwords and pr… personal information online.

Intel officials announced the deal Dec. 1, adding that the PasswordBox business will be folded into the Safe Identity unit within Intel's Security Group. There have been more than 14 million downloads of the startup's technology, which lets users store their log-in information in a virtual lockbox. When a user wants to get into a Website or an app, he or she clicks on the site and the PasswordBox deals with the log-in process.

The software runs on both Apple iOS devices and those running Google's Android operating system.

Pa… managers hacked: …archers find 'critical' vulnerabilities

by Mike Wheatley | Jul 14, 2014 |

If you're using a popular password manager your credentials might not be entirely safe, following the discovery of several vulnerabilities that could allow attackers to gain access.

University of California Berkeley researchers have discovered a number of quickly-patched vulnerabilities in LastPass, My1Login, NeedMyPassword, PasswordBox and RoboForm. They described their work as a "wake-up call" for password manager developers.

"Our attacks are severe: in four out of the five password managers we studied, an attacker can learn a user's credentials for arbitrary websites," wrote researchers Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song wrote in their paper. "We find vulnerabilities in diverse features like one-time passwords, bookmarklets, and shared passwords.

Tænk på..
Google gmail
gemmer mange års e-mails.
Hvad står der i dem?
..hvis nu du bliver hacket?

Sendte du banken et
billede af dit pas?
Kopi af lønseddel?

Da du søgte om et lån
for 10 år siden..

Brug 2-Faktor login..

2-Faktor ved brug af en applikation

2-Faktor ved brug af papir koder

2-Faktor ved brug af et Token

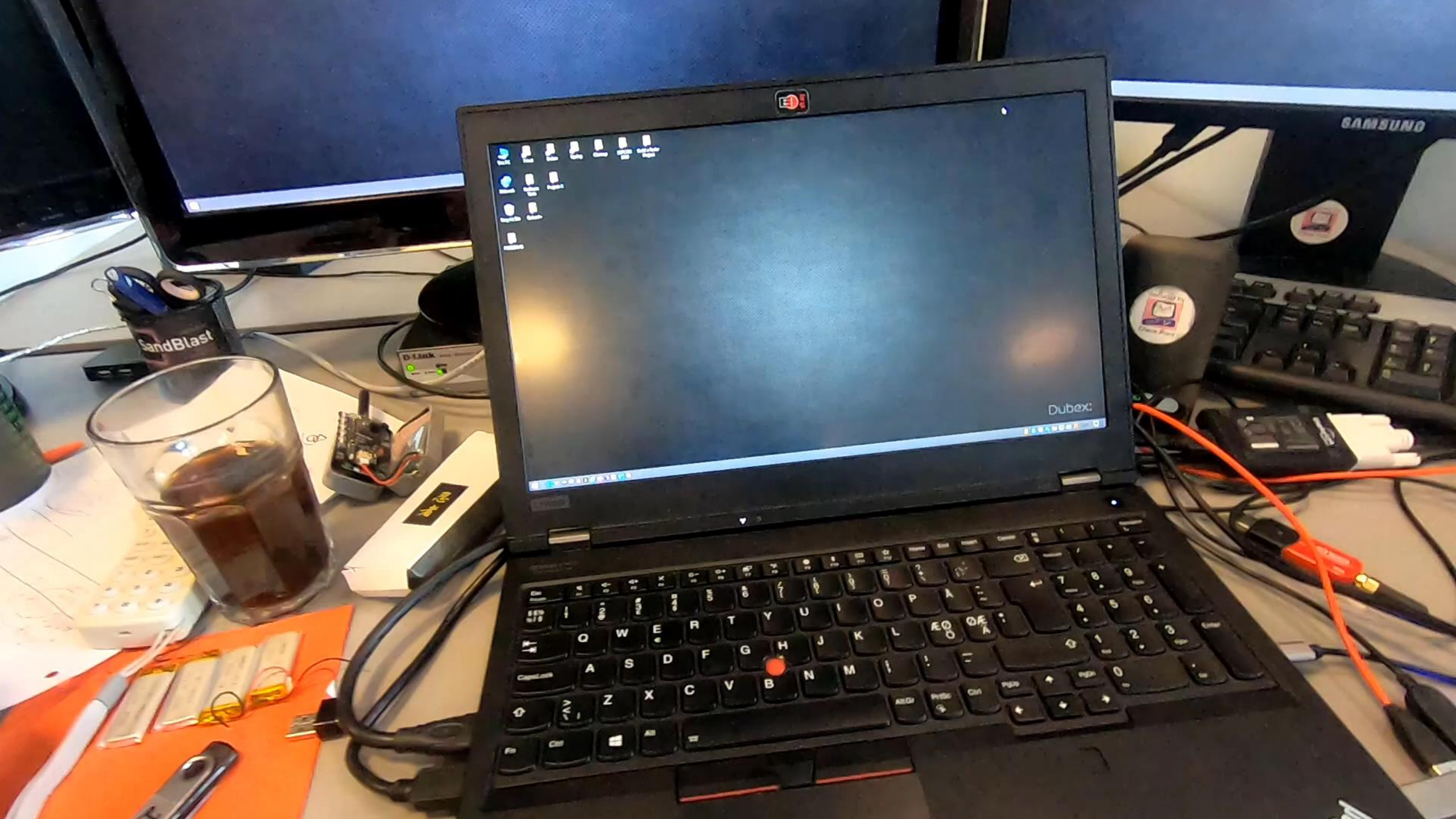
Dubex:

MANAGING RISK. ENABLING GROWTH.®

Keld Norman / kno@Dubex.dk


Supply chain attacks
No SIM
12:32 PM
192.168.4.1
51%
Payload:
Advanced
Triggers
Wifi Config
http://mg.lol/blog/omg-cable

Rubber Ducky Attack


SandBlast
D-Link
SAMSUNG
Dubex:

Har du har (stadig) sådan en ”dongle” i din computer ?

Mulig hacker afstand: 200 meter

MOUSEJACKING

GSM SIM Spy Hidden Monitor US

https://www.ebay.com/itm/GSM-SIM-Spy-Hidden-Monitor-USB-Charger-Cable-GPS-Tracker-For-iPhone-Android/332905030992?hash=item4d82afa550:m:mE...

GSM SIM Spy Hidden Monitor USB Charger Cable GPS Tracker For iPhone Android

Condition: New

Type: - Select -
- Select -
For Android
For iPhone

Quantity: 0 available / 9 sold

Price: US $7.39
Approximately DKK 48.06

Buy It Now

Add to cart

GSM AFLYTNING I LADEKABLET KOSTER 48,- DKK

Keyloggers

KEYBOARD MED INDBYGGET KEYLOGGER

- Gemmer optagelsen
- Kan ikke detekteres af software på computeren
- Laver et WiFi eller logger på et WiFi
- Optager også BIOS og harddisk krypterings kodeord

Forensic Keylogger Keyboard

Op til 16 gigabytes

The **Forensic Keylogger Keyboard** is a customized keyboard with an **integrated hardware keylogger**. The embedded hardware keylogger derives either from the **KeyGrabber Forensic** family, or from the **AirDrive Forensic** family. A **variety of keyboard models** is available to choose from when ordering your Forensic Keylogger Keyboard.

59^{99} or €50^{99}

More info

KeyGrabber Forensic Keylogger Cable / Module

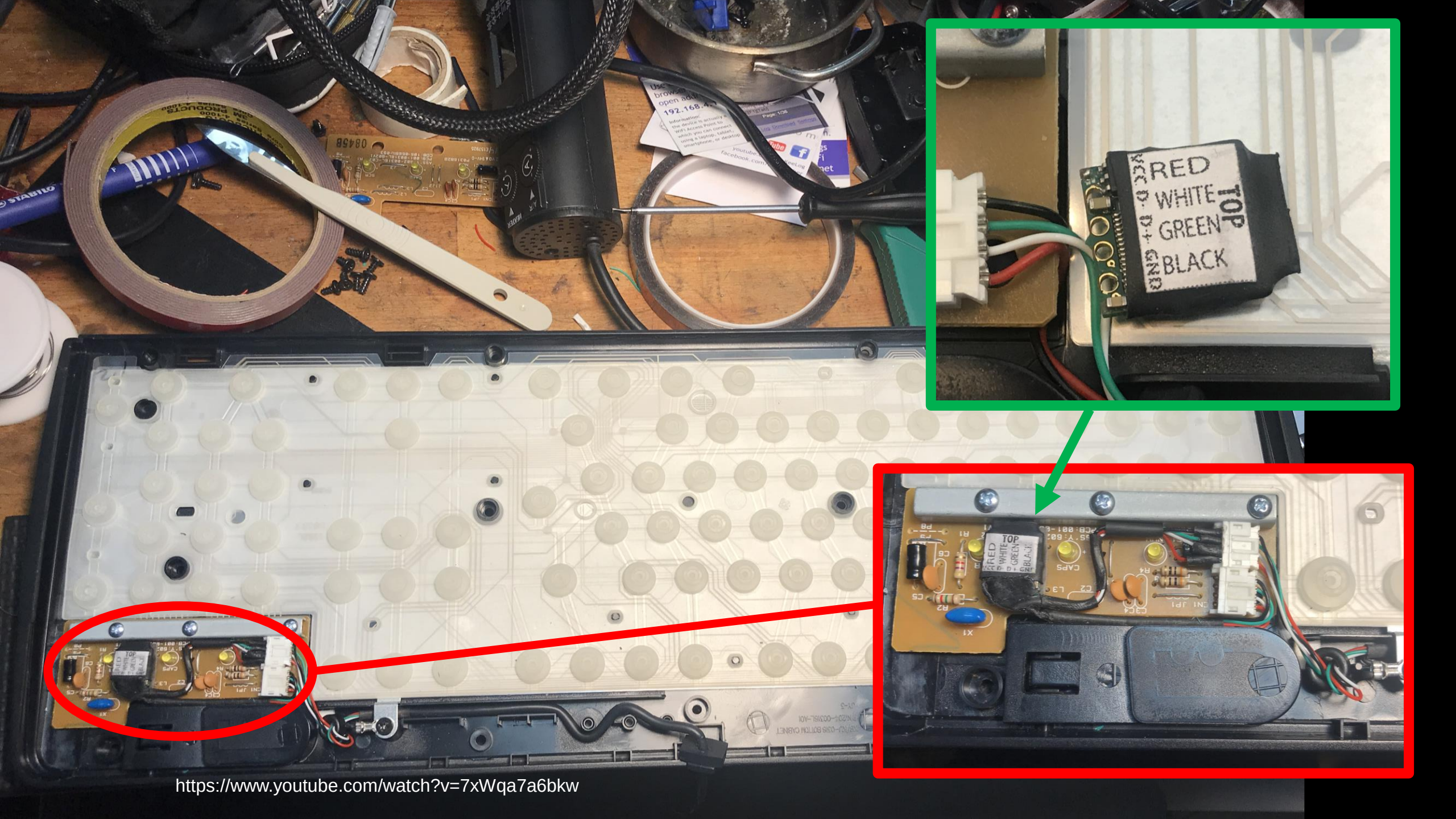
16 megabytes
(ca 8000 siders tekst)

The **KeyGrabber Forensic Keylogger** is a series of specialized hardware keyloggers with flash drive access, aiming at minimizing the risk of exposure. They diverge from the classic USB adapter shape, making them nearly impossible to locate. Available as a **USB extension cable** and **keyboard-embeddable module** only 0.5" (12 mm) in length.

29^{99} or €25^{99}

More info

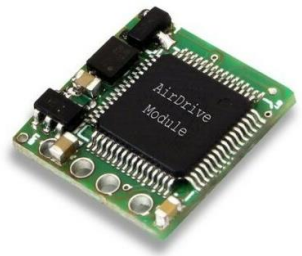
https://youtu.be/**7xWqa7a6bkw**


RED
WHITE
GREEN
BLACK
TOP
GND D+ D- +5V
https://www.youtube.com/watch?v=7xWqa7a6bkw

Keyloggers

En keylogger Sættes imellem din computer og keyboardet.

Den kan så optage og gemme det du taster som eksempel vis dit login og kodeord



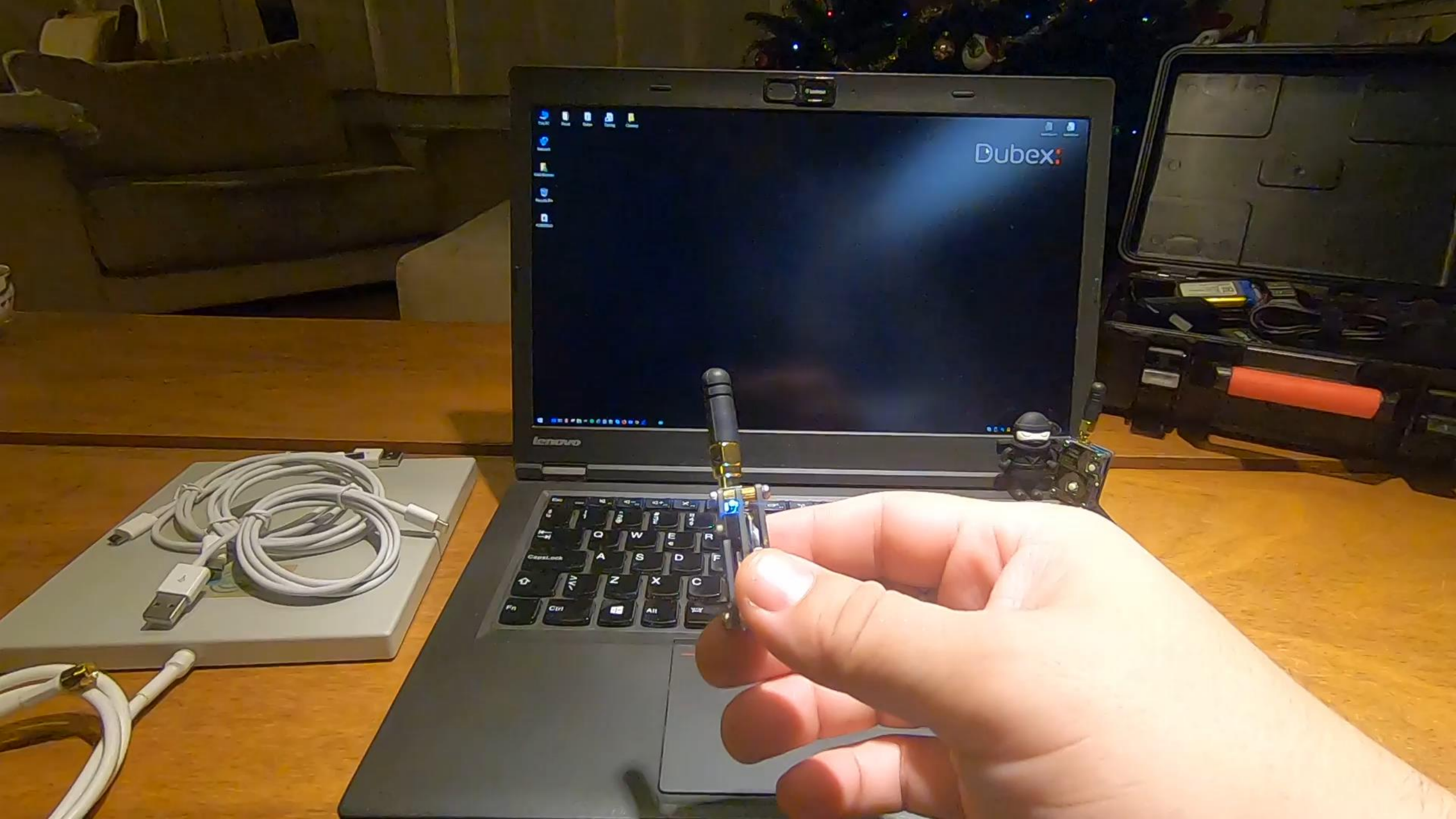
Original iPhone Lader kable

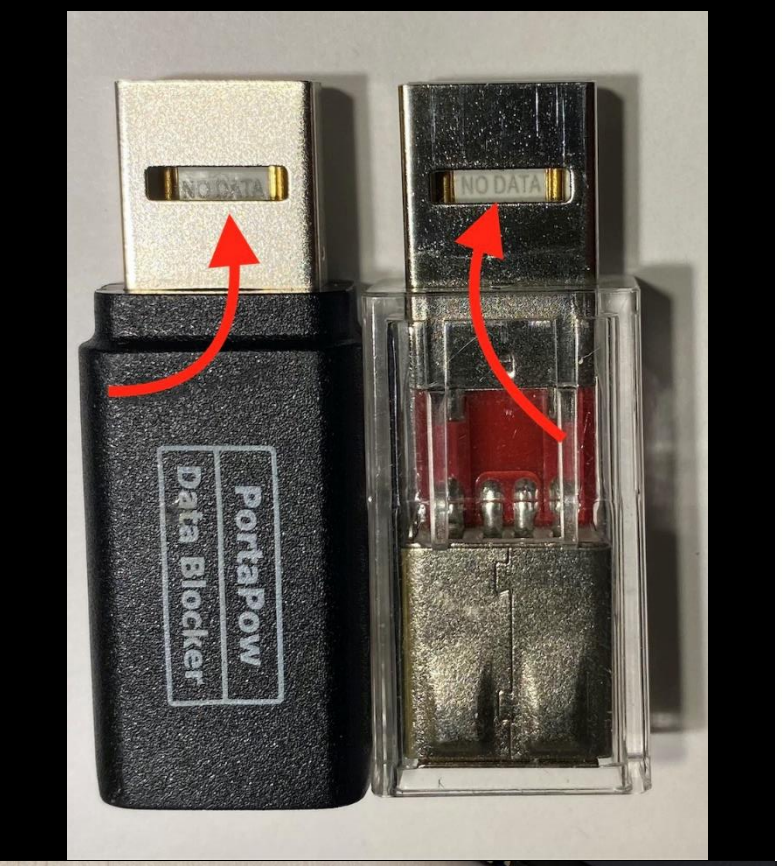
Evil USB ”Keyboard”

USB NINJA & USB KILLER

DECEMBER 2018

https://usbninja.com/shopusbninja (koster i dag mellem 1100-2800 DKK)


Dubex
lenovo

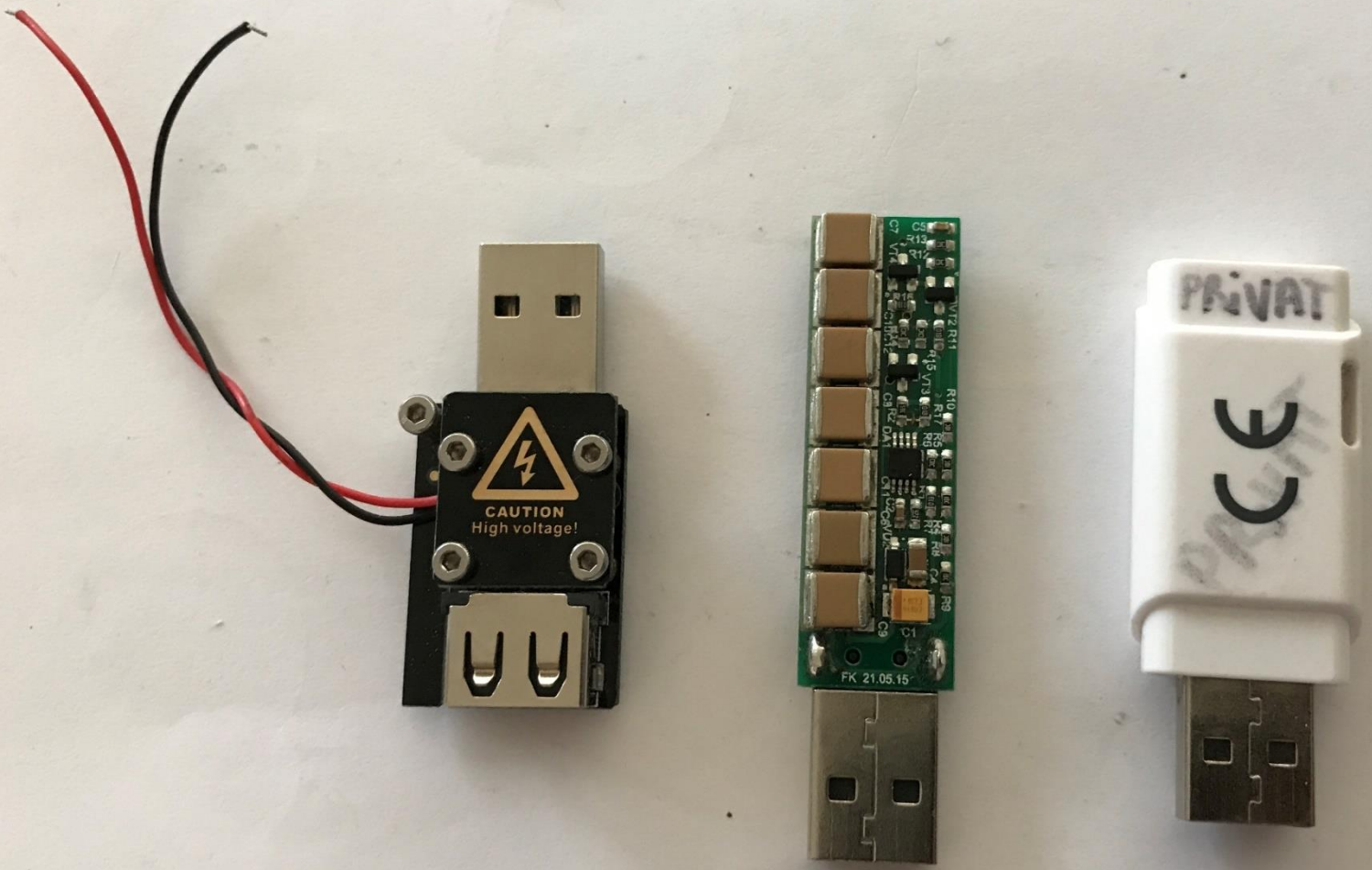


Product Image	Teardown	Name	Charge Type	Notes
		PortaPow - 3rd Gen	#3	
		EDEC - Data Blocker	#3	
		USB Defender	#3	
		PortaPow - Pure	#1	Clear case, no teardown needed!
		SyncStop	#2	
		Generic - “4th Gen”	#1	single side PCB, cost cutting design
		Generic	#1	lowest quality design. no PCB
		ET USB Defender	#1	single sided PCB, cost cutting design
		Charge Defense - Juice-Jack Defender	#2	extremely bulky design

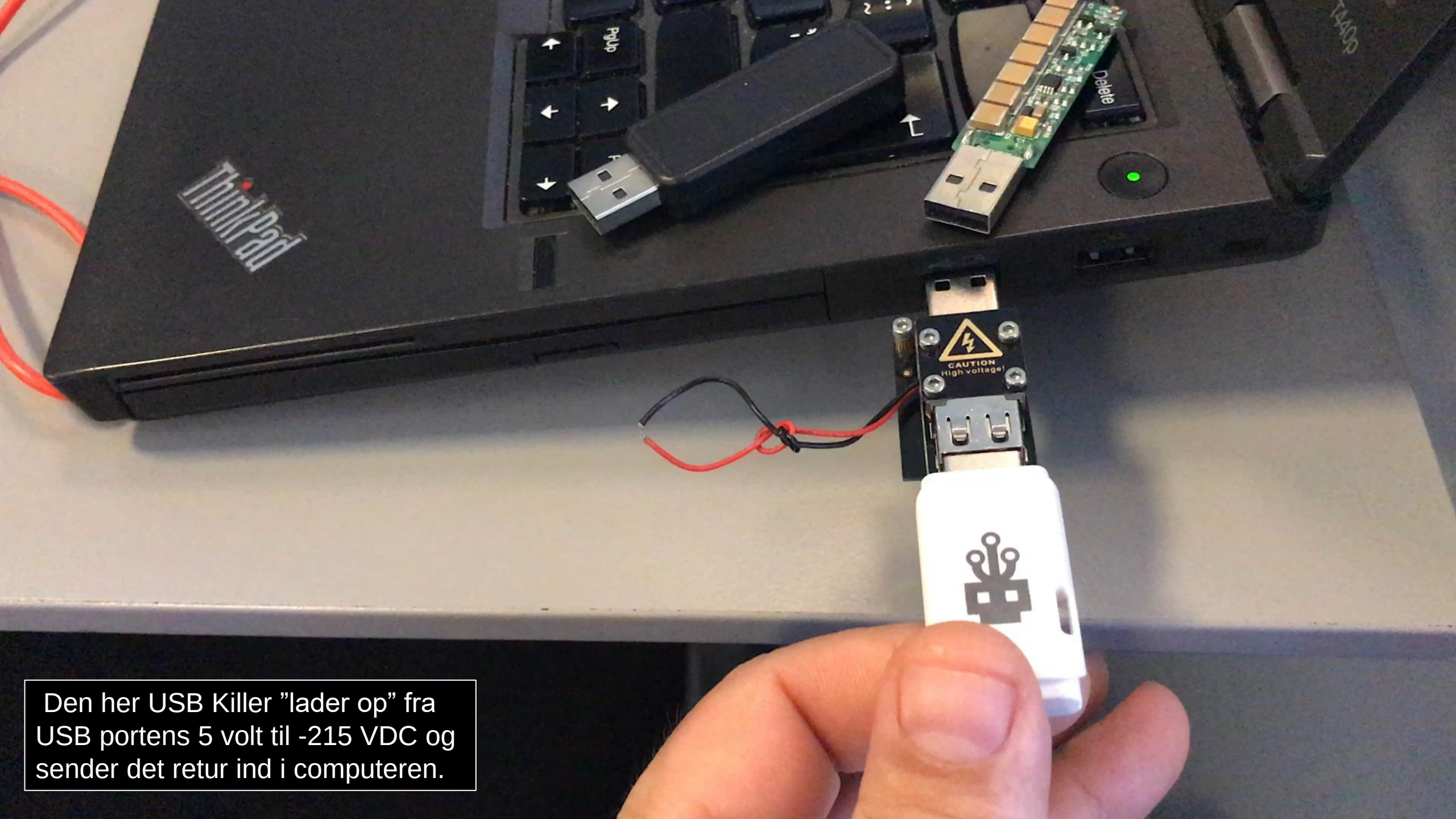
USB KONDOMER

https://mg.lol/blog/data-blocker-teardown/

USB KILLER



MARTS 2015



Den her USB Killer ”lader op” fra USB portens 5 volt til -215 VDC og sender det retur ind i computeren.

USBKill V4 Kit | USBKill

usbkill.com/products/usbkill-v4-kit?variant=32836116611154

USBKILL

USBKill | USBKill Kits | Accessories | FAQ | Contact | 0

USBKill V4.0

The new USBKill is app-controlled.|

The most powerful USBKill ever. New unstoppable attack modes. Remote controlled. The ultimate pentesting device.

needs no host power.

USBKill V4 Kit

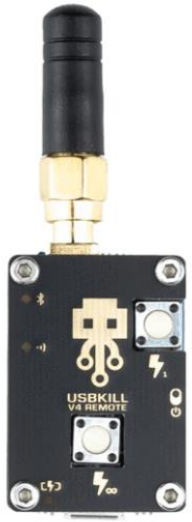
USB KILL V3

€299.95 (Svarer til ca. 2.250 DKK)

Version: Tactical

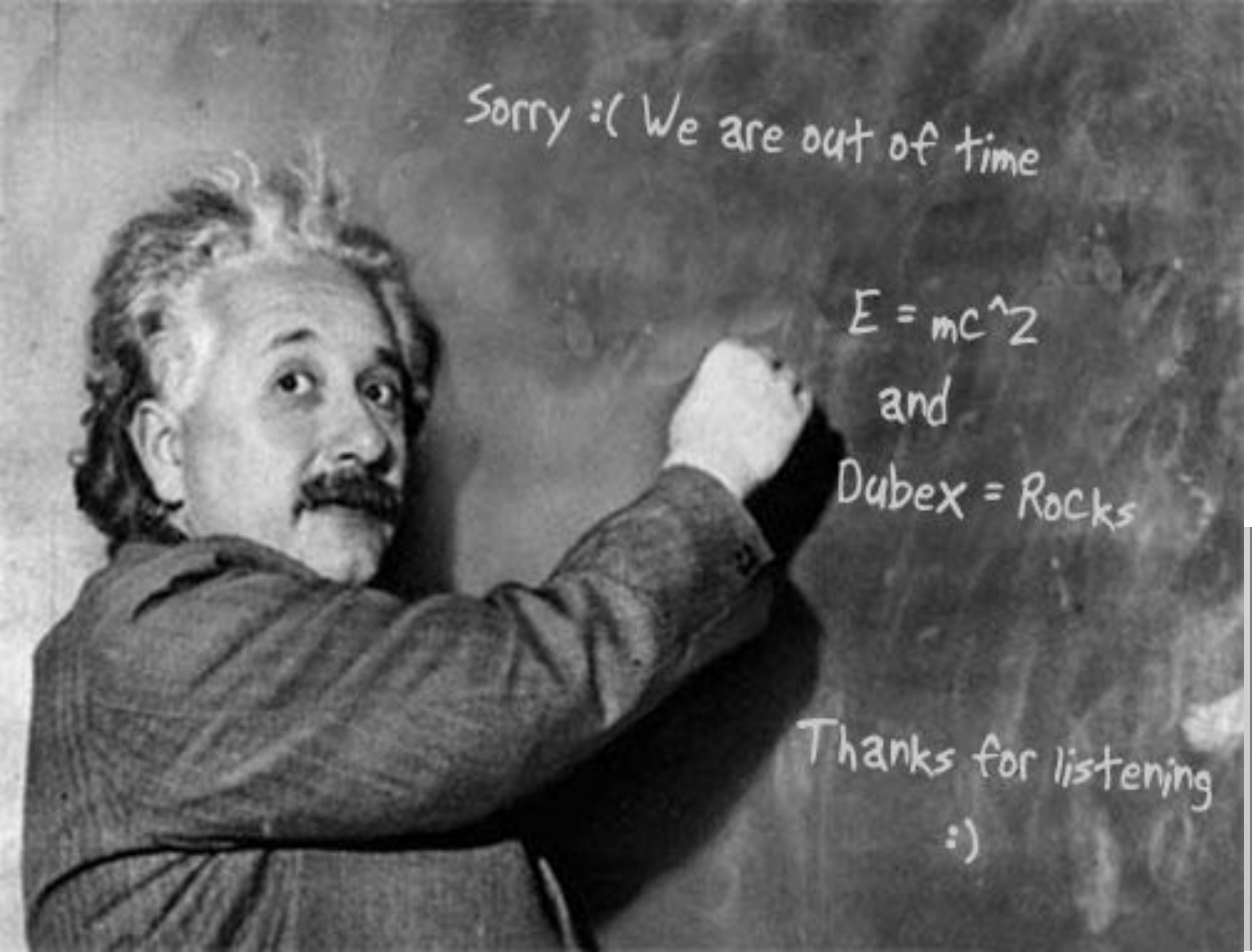
Nyhed:

Dræber nu også netværks udstyr / switche !



Den billige model koster
50 euro / 375,- DKK

Kan aktiveres via Android Application eller fjernbetjening



Dubex:

MANAGING RISK. ENABLING GROWTH.®

Keld Norman / kno@Dubex.dk

THE END