ACCESS SECURITY

Personal eMail accounts – the holy grail of identity theft

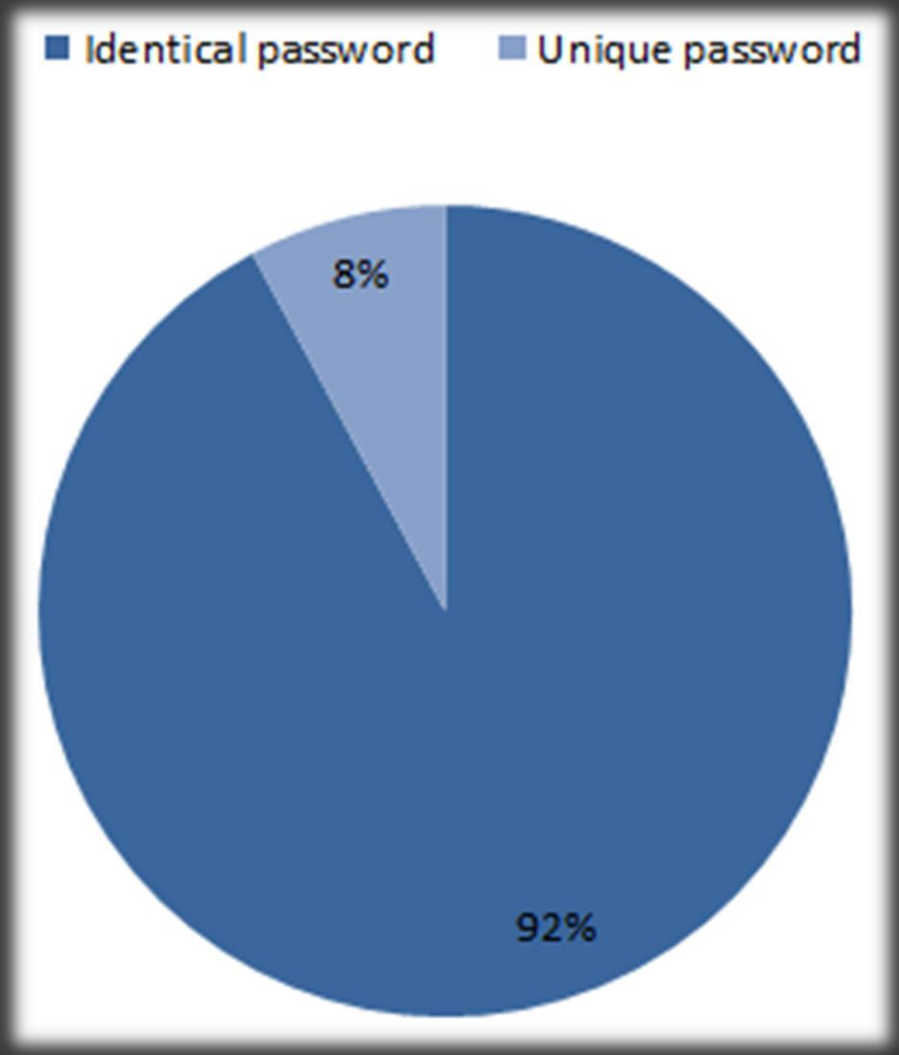
Marcus Viertel
@viertelm

The Millennial Generation

iCloud

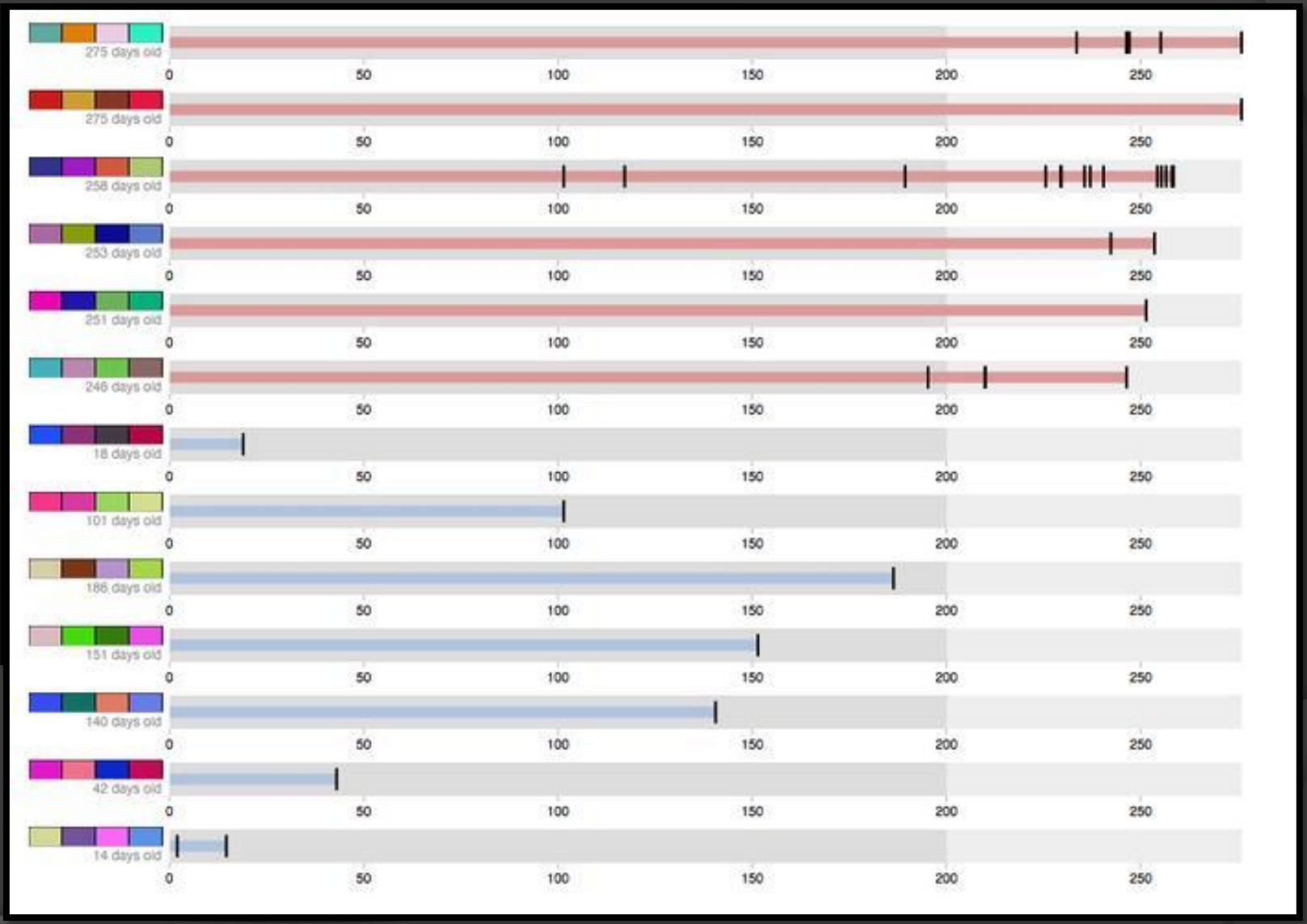
Password ‘best practice’

Password reuse



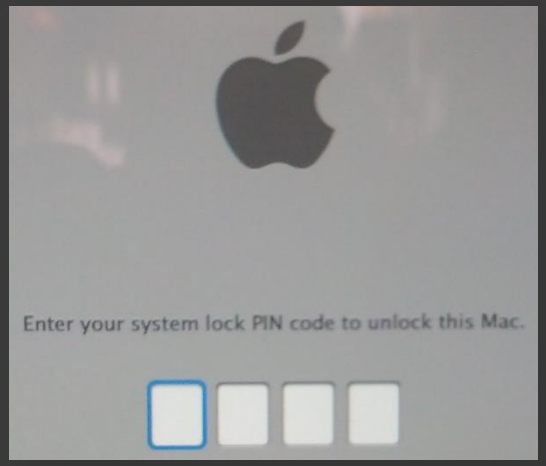
- 25:6 ratio
- Password rotation between 5 sets
- ¾ reuse banking password (Trusteer)
- ½ reuse full banking credentials (Trusteer)

Firefox Password Tools




Back
Set Up iPhone
Next
Choose to set up as a new iPhone or restore from a previous backup.
Set up as new iPhone
Restore from iCloud Backup
Restore from iTunes


No Service
11:08 AM
Back
iCloud Sign In
Next
Apple ID
Password
Required
Sign in with your iCloud Apple ID.
Forgot Apple ID or Password?


Enter your system lock PIN code to unlock this Mac.


iCal can't log in to your account because your password may be incorrect.
The password may have been entered incorrectly. Reenter the password for account on the CalDAV server
Cancel
OK


Apple ID Password
password
Cancel
OK


Sign in to Gmail with your
Google Account
Username:
Password:
Remember me on this computer.
Sign in
I cannot access my account


Sign in to Twitter
Username or email
Password
Sign in
Remember me

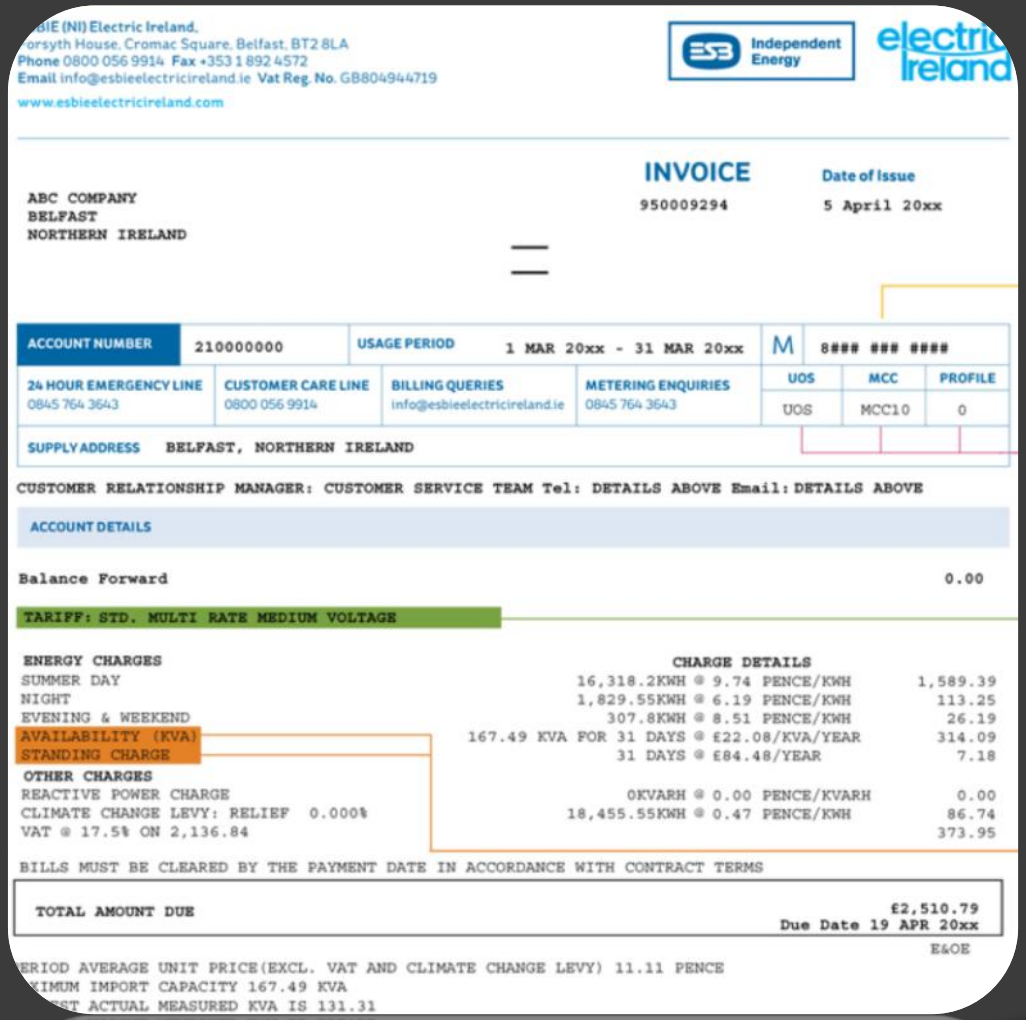
Matt Honan

- Amazon account
- iCloud account
- Gmail account
- Twitter account

The very four digits that Amazon considers unimportant enough to display in the clear on the Web are precisely the same ones that Apple considers secure enough to perform identity verification.

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

Utility bills as ID proof



BIE (NI) Electric Ireland,
orsyth House, Cromac Square, Belfast, BT2 8LA
Phone 0800 056 9914 Fax +353 1 892 4572
Email info@esbieelectricireland.ie Vat Reg. No. GB804944719
www.esbieelectricireland.com

Independent Energy

electric Ireland

INVOICE

Date of Issue
5 April 20xx

950009294

ABC COMPANY
BELFAST
NORTHERN IRELAND

ACCOUNT NUMBER	210000000	USAGE PERIOD	1 MAR 20xx - 31 MAR 20xx	M	8### ### ####

24 HOUR EMERGENCY LINE	CUSTOMER CARE LINE	BILLING QUERIES	METERING ENQUIRIES	UOS	MCC	PROFILE
0845 764 3643	0800 056 9914	info@esbieelectricireland.ie	0845 764 3643	UOS	MCC10	0

SUPPLY ADDRESS BELFAST, NORTHERN IRELAND

CUSTOMER RELATIONSHIP MANAGER: CUSTOMER SERVICE TEAM Tel: DETAILS ABOVE Email: DETAILS ABOVE

ACCOUNT DETAILS

Balance Forward 0.00

TARIFF: STD. MULTI RATE MEDIUM VOLTAGE

ENERGY CHARGES	CHARGE DETAILS	
SUMMER DAY	16,318.2KWH @ 9.74 PENCE/KWH	1,589.39
NIGHT	1,829.55KWH @ 6.19 PENCE/KWH	113.25
EVENING & WEEKEND	307.8KWH @ 8.51 PENCE/KWH	26.19
AVAILABILITY (KVA)	167.49 KVA FOR 31 DAYS @ £22.08/KVA/YEAR	314.09
STANDING CHARGE	31 DAYS @ £84.48/YEAR	7.18
OTHER CHARGES		
REACTIVE POWER CHARGE	0KVARH @ 0.00 PENCE/KVARH	0.00
CLIMATE CHANGE LEVY: RELIEF 0.000%	18,455.55KWH @ 0.47 PENCE/KWH	86.74
VAT @ 17.5% ON 2,136.84		373.95

BILLS MUST BE CLEARED BY THE PAYMENT DATE IN ACCORDANCE WITH CONTRACT TERMS

TOTAL AMOUNT DUE £2,510.79
Due Date 19 APR 20xx

E&OE

ERIOD AVERAGE UNIT PRICE(EXCL. VAT AND CLIMATE CHANGE LEVY) 11.11 PENCE
XIMUM IMPORT CAPACITY 167.49 KVA
EST ACTUAL MEASURED KVA IS 131.31

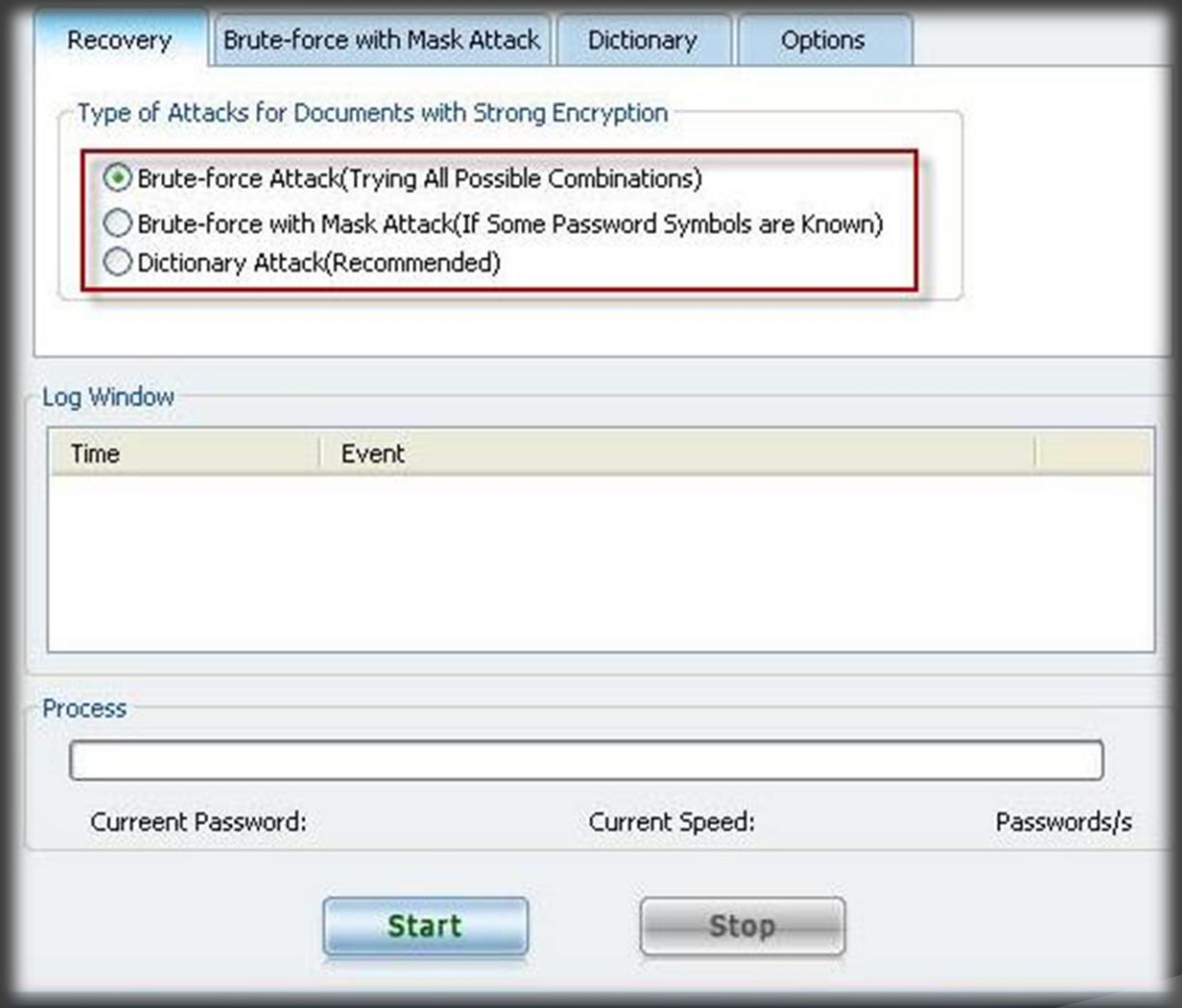
- Used in:
  - Banks
  - Mobile shops
  - Service subscriptions
  - …

Cloud backups

iCloud hacking

- Contacts
- Photos
- Videos
- Messages
- Notes
- Locations
- Events
- Etc.

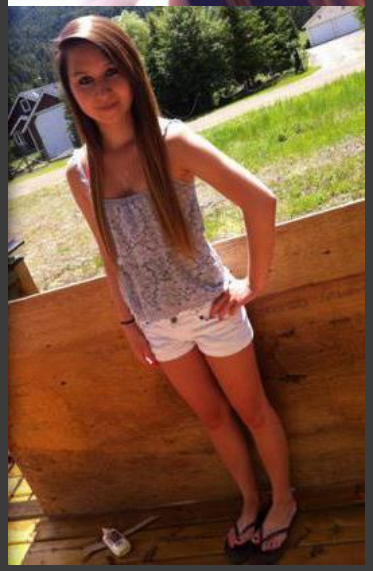
Backup encryption



- AES-128
- 256Bit key
- SHA1 signed
- Salted


BLaCK
MAiL

Victim: Amanda Todd



- Committed suicide at age 16
- Victim of online bullying & extortion

Explicit images are valuable

24-year-old girl commits **suicide** after being **blackmailed** by ex-friend ...
www.indianexpress.com/news/...girl...**suicide**...**blackmailed**.../1055032/
5 Jan 2013 - 24-year-old girl commits **suicide** after being **blackmailed** by ... her objectionable **pictures online** if she did not cancel her wedding next month.

Nude photos part of **blackmail** that drove A&M prof to **suicide** ...

houston.culturemap.com › City Life
by Tyler Rudick - in 38 Google+ circles
26 Mar 2013 - Newly-released legal documents are shedding light on the mysterious death of James Aune — the well-regarded Texas A&M professor who.

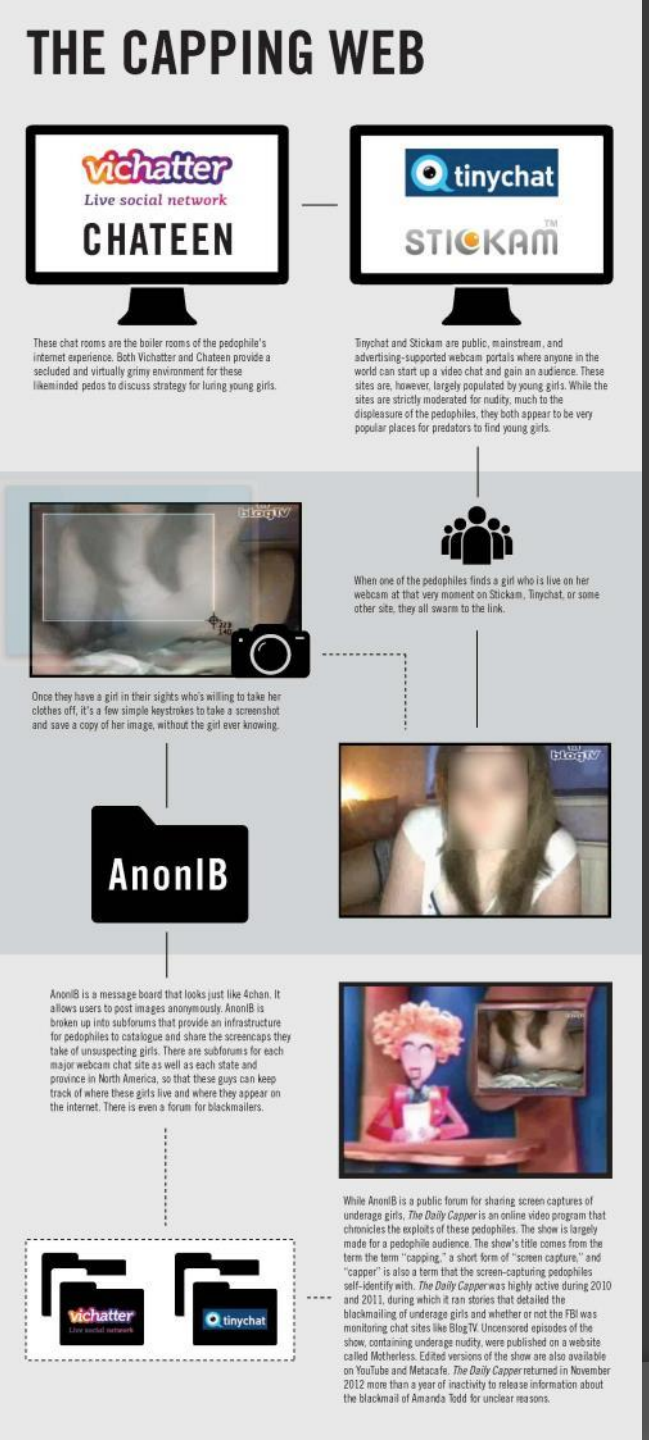
Cowards Are **Blackmailing** Young Women to Death on the **Internet** ...

www.vice.com/.../cowards-are-**blackmailing**-young-women-to-d...
by Patrick McGuire - in 127 Google+ circles
2 Jan 2013 - Five weeks before committing **suicide**, Amanda posted a video to ... at least ten fresh girls ready for **blackmail**, with Facebook, **pictures**, etc.

News for **suicide online picture blackmail**

Distraught children as young as 11 **blackmailed** into undressing on webcams by users of Russian-based website ...
Daily Mail - 2 days ago
A UK cyber-charity says they are getting 15 'desperate' calls a week from youngsters who want to kill themselves after doing a webcam strip ...

Alleged **blackmail** behind A&M professor's **suicide** - Houston Chronicle
www.chron.com › Houston & Texas › News › Houston
26 Mar 2013 - ALL OF THEM will be able to see your conversations, text, **pictures** you ... he was being **blackmailed** as the result of a sexually explicit **online** ...



Online predators

- So called Cappers collaborate online to secure ‘wins’
- Socially engineer password reset security questions
- Collaborate on password brute forcing
- Share ‘wins’ publicly

Automated image theft

Image Theft via FTP Could Be First Stage of Attack

Recommend Share +1 Tweet 51

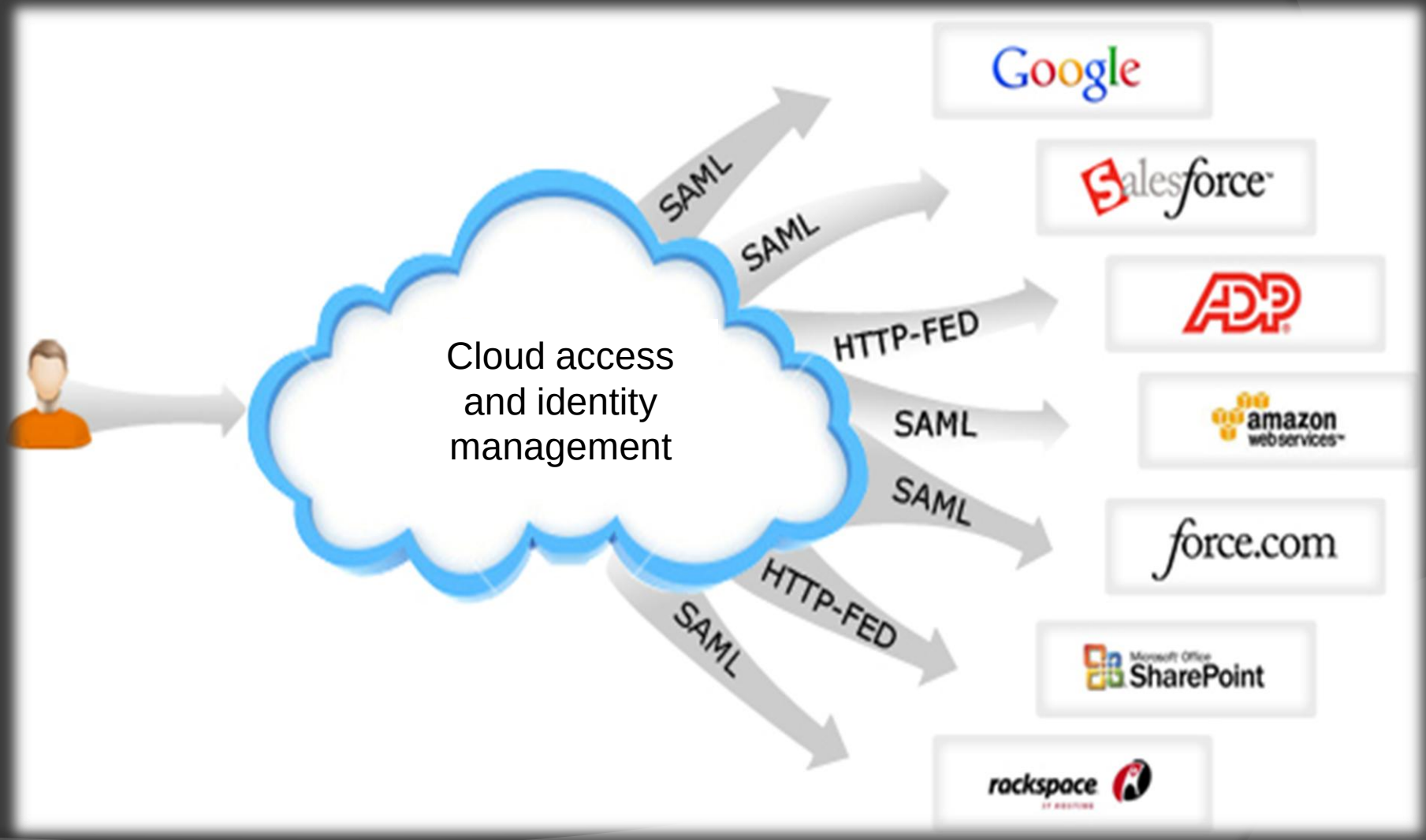
Tuesday, November 6, 2012 at 10:32am by Niranjan Jayanand

We recently came across a Trojan that steals image files of .jpg, .jpeg extensions, and Windows memory dumps (.dmp) from victims' machines and uploads them to an FTP address hardcoded in the malware.

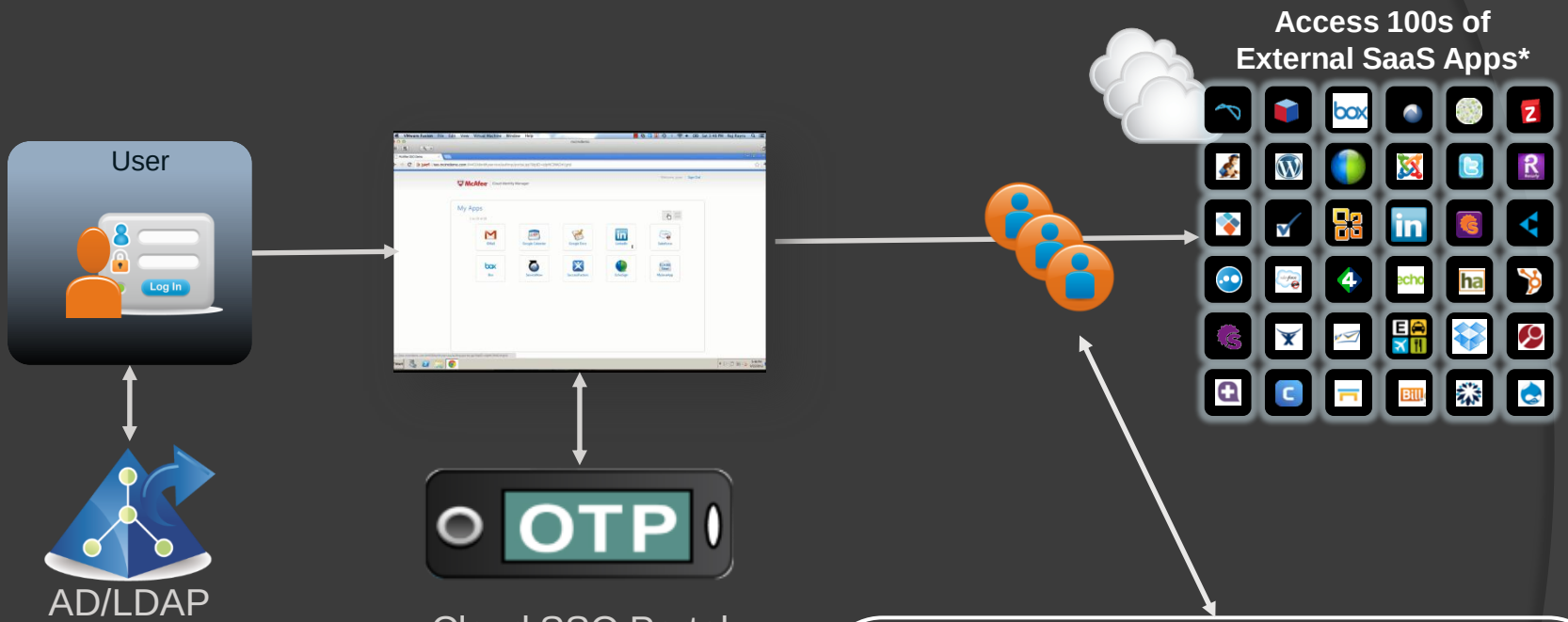
This Trojan silently opens a command line and copies those image files found on the C, D, and E drives to the C drive. These collected file are then sent to an FTP server.

Personal vs. Enterprise

Identity and Access Management



Enterprise SSO



SaaS authentication

- **SAML**: Federated SSO standard
- **HTTP POST**: User ID/password
- **Agent-based**: Java, .NET, PHP agents
- **Proprietary API**: Application-specific

Password managers

- Online or off-line
- Browser password managers

In 2008, the then-venerable Bugtraq mailing list sent out this warning: "Chrome stores passwords in CLEAR TEXT."

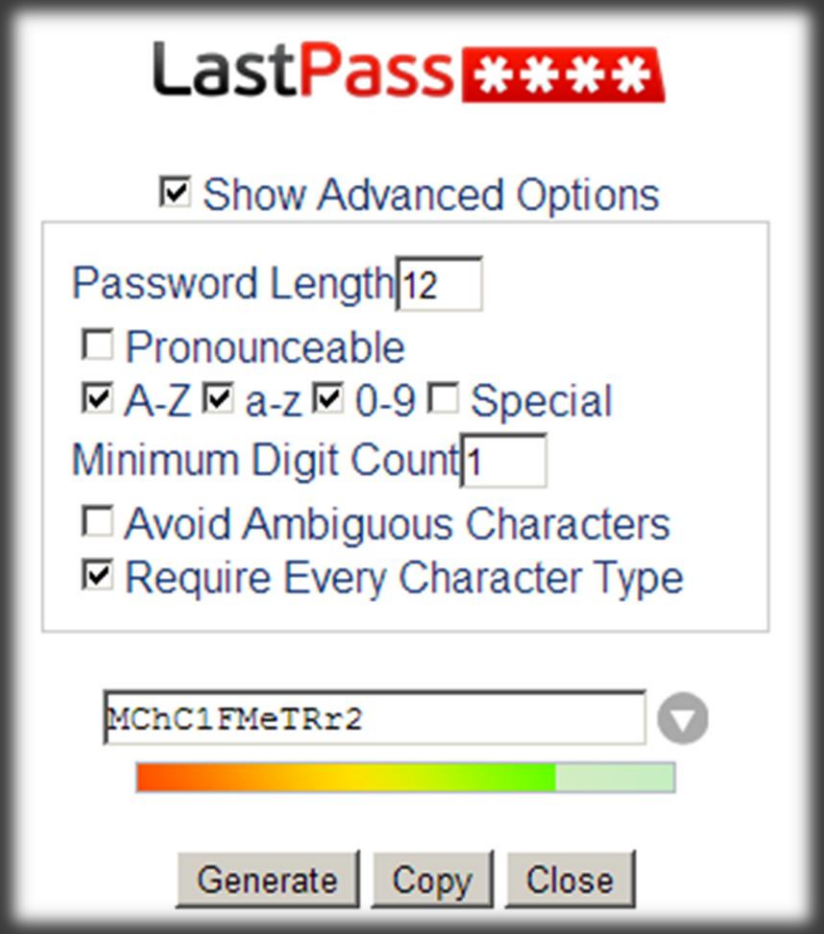
In 2011, The Windows Club blog reported: "Chrome, Firefox expose passwords in plain text."

In 2012, timmy_42 wrote in a Google Group discussion on Chrome: "Chrome devs have said many times that they won't add a master password."

In 2013, Elliott Kember "exposed" "Chrome's insane password security strategy."

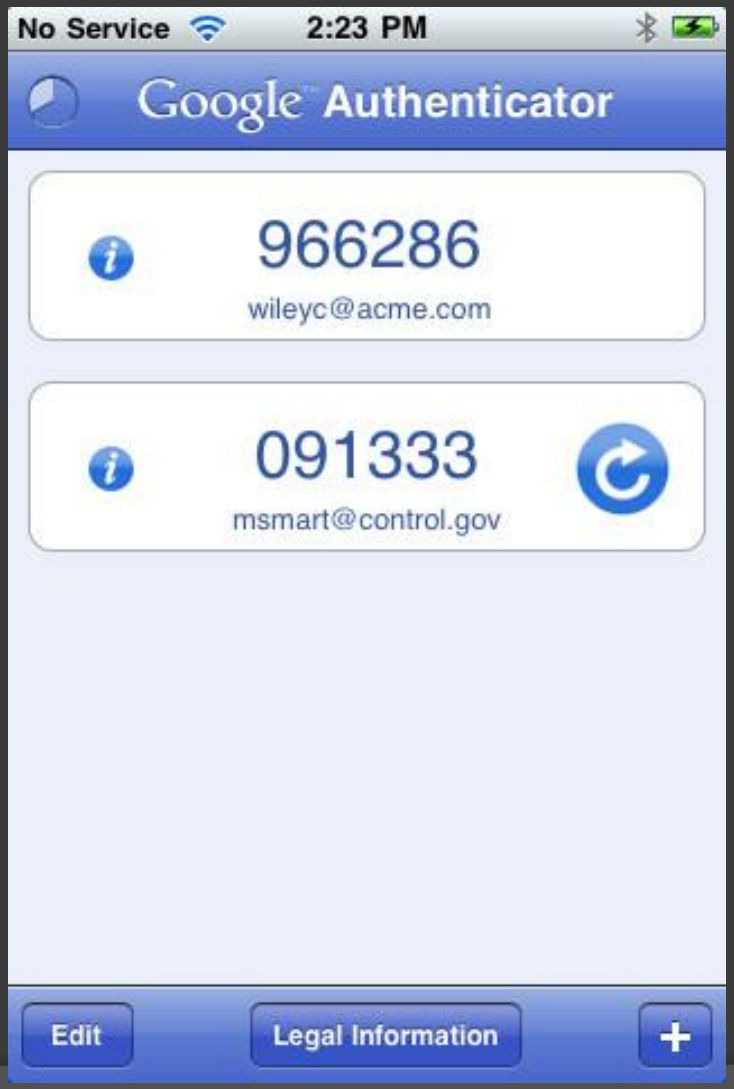
- IronKey

Password entropy



- Long, unique, complex passwords
- Automatic logins
- Broad browser and platform support
- Combine with Xmarks for bookmark syncing

Google Authenticator



Gmail by Google

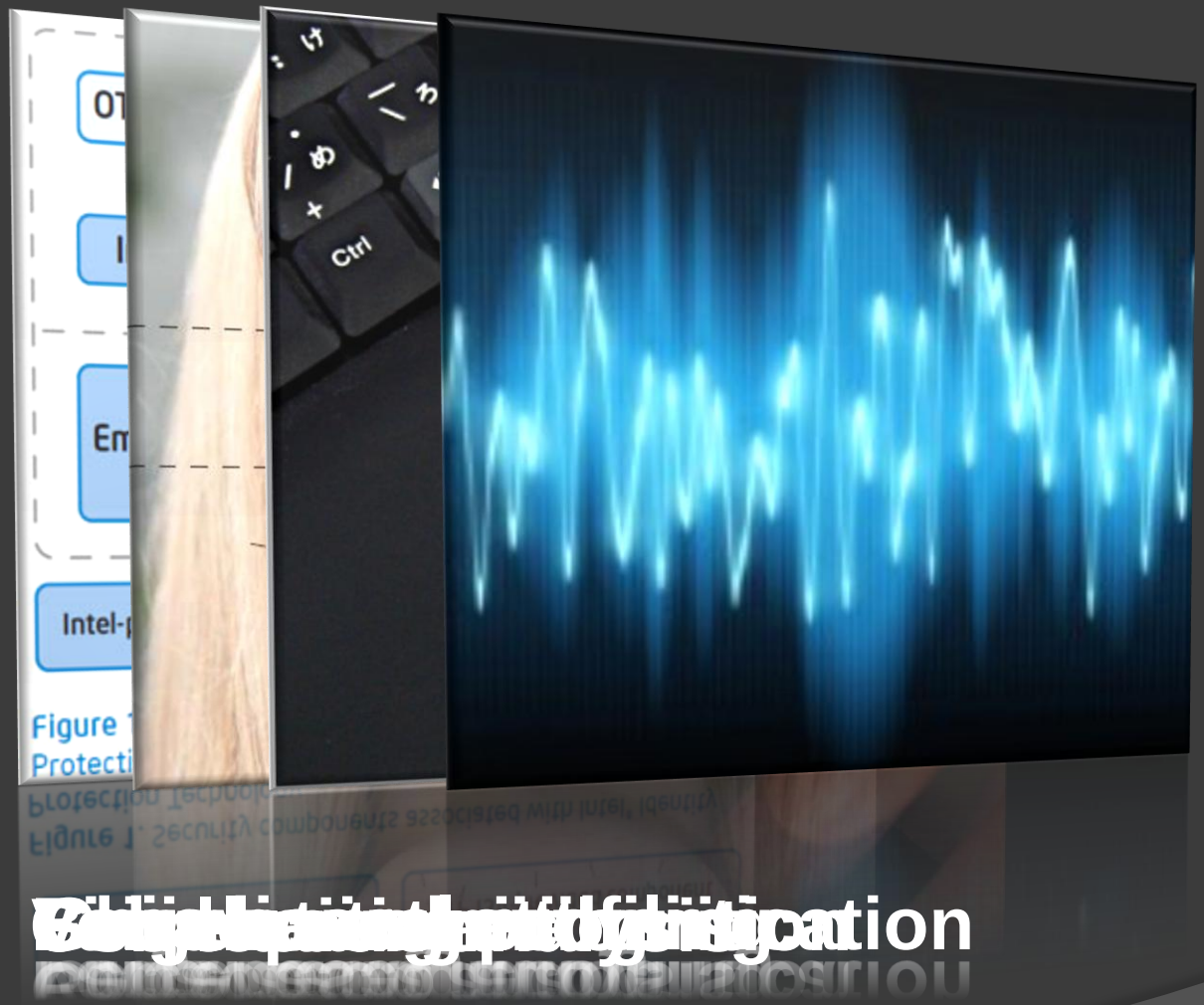
WordPress

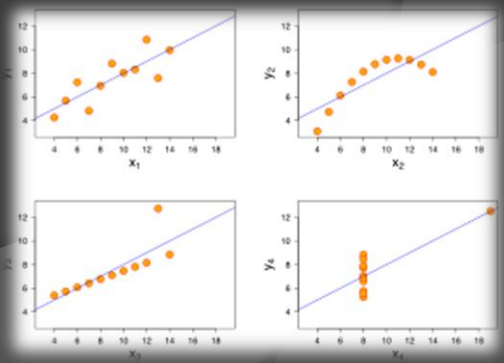
LastPass ****

Dropbox

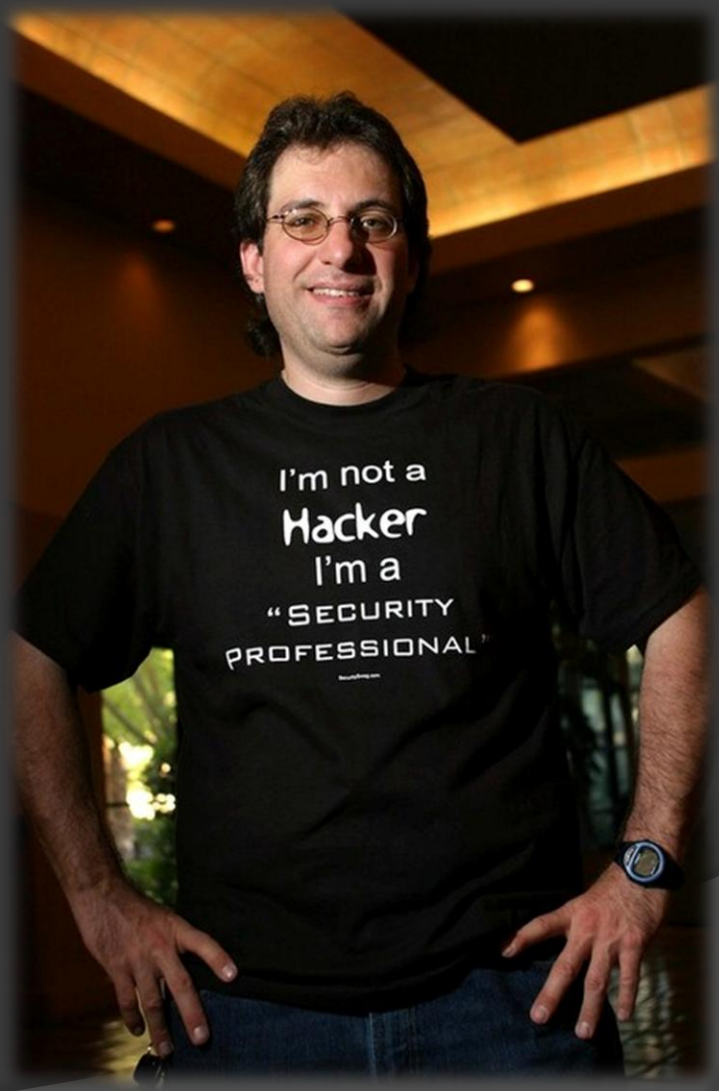
EVERNOTE

Beyond OTP





Responsibilities



Thank you

Marcus Viertel
@viertelm