

The "Human Factor" in data and device protection.

...

Case study, hacking history and best
practices

Carlo Gubitosa - carlo@gubi.it

Case study

One innocent typo
can wipe your device

In this example which occurred to me personally, we'll examine one case in which a careless setup of a Gmail account can compromise all the mobile devices linked to that account.

Alert

An alert on a legitimate email address comes from a similar email address. Somebody is trying to pretend to be me? My address is set as “recovery address” for the same email with a “1” in the end.

Il tuo indirizzo email di recupero è stato cambiato

Inbox x



Google <no-reply@accounts.google.com>
to nome.cognome@gmail.com

24 Mar ☆



Google



Il tuo indirizzo email di recupero è stato
cambiato

Ciao Nome,
L'indirizzo email di recupero per il tuo account Google
nome.cognome1@gmail.com è stato modificato di recente.



Non riconosci questa attività?
Controlla subito i [dispositivi utilizzati di recente](#).

Cordiali saluti,
Il team di Google Account

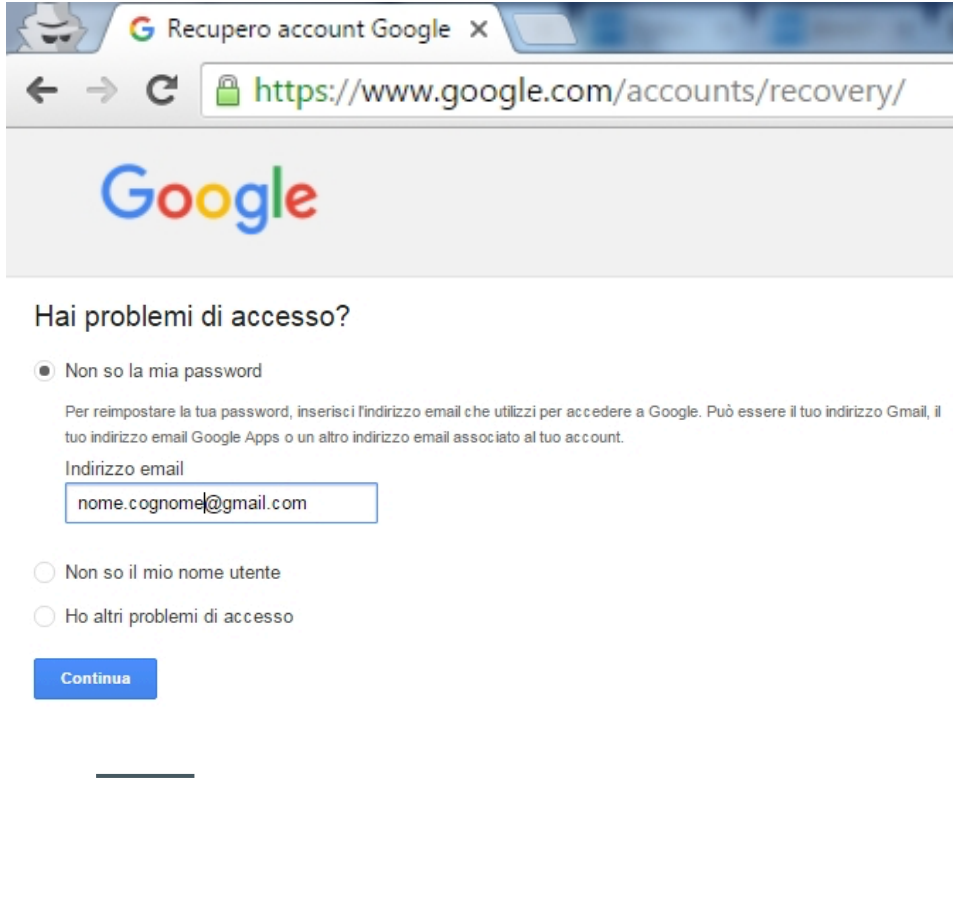
Questo indirizzo email non è abilitato alla ricezione di risposte. Per ulteriori informazioni, visita il [Centro assistenza di Google Account](#).

Ti abbiamo inviato questa email di servizio obbligatoria per informarti di importanti cambiamenti che interessano il tuo prodotto o il tuo account Google.

© 2016 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Takeover

I recover the password using the
recover address
name.surname@gmail.com and
takeover the modified account
name.surname1@gmail.com



The image shows a browser window with the title "Recupero account Google" and the URL "https://www.google.com/accounts/recovery/". The Google logo is displayed at the top. Below it, the heading "Hai problemi di accesso?" is followed by a radio button selection for "Non so la mia password". A sub-heading "Indirizzo email" is above a text input field containing "nome.cognome@gmail.com". Below this are two more radio button options: "Non so il mio nome utente" and "Ho altri problemi di accesso". A blue "Continua" button is at the bottom.

Recupero account Google X

← → ↻ <https://www.google.com/accounts/recovery/>

Google

Hai problemi di accesso?

Non so la mia password

Per reimpostare la tua password, inserisci l'indirizzo email che utilizzi per accedere a Google. Può essere il tuo indirizzo Gmail, il tuo indirizzo email Google Apps o un altro indirizzo email associato al tuo account.

Indirizzo email

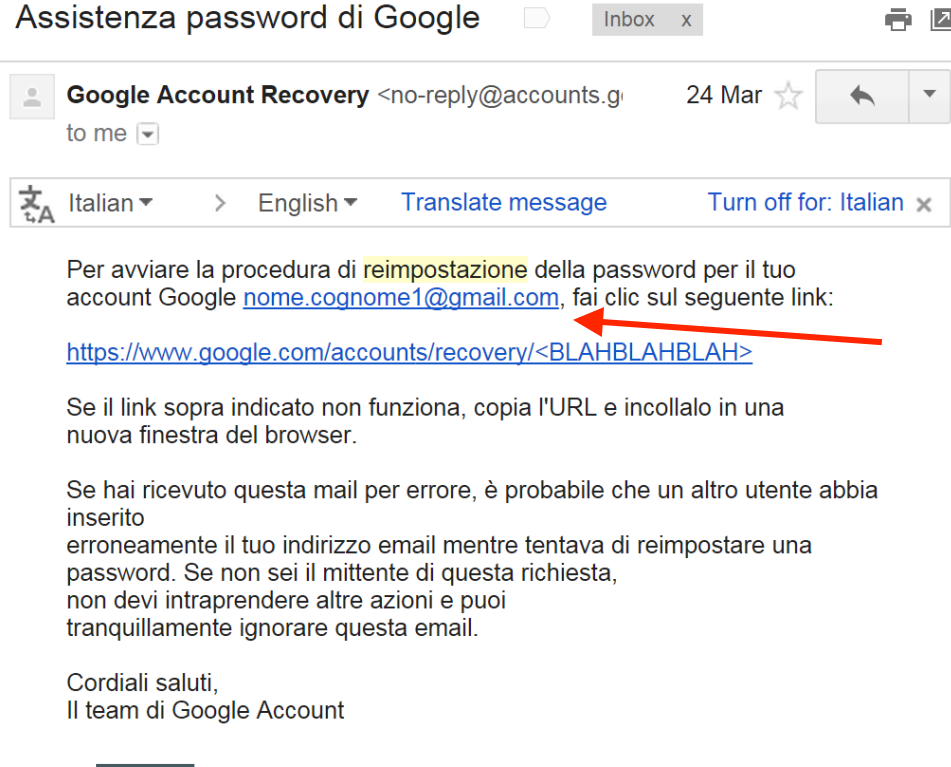
Non so il mio nome utente

Ho altri problemi di accesso

[Continua](#)

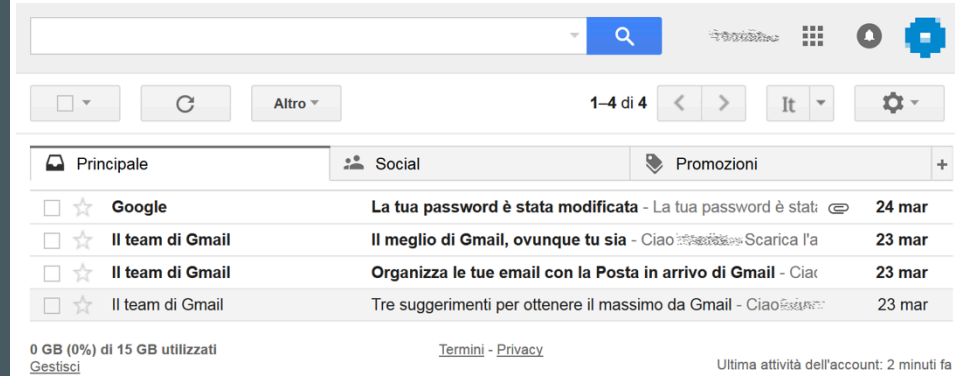
Get password

I get a recovery mail that opens
you the door of the account
name.surname1@gmail.com



Control

Checking the account it seems clean, just created, no mail sent, no suspect of fraudulent activity that may be associated to an identity theft attempt. We check the details of the connections.



The screenshot shows a Gmail inbox with the following email list:

Sender	Subject	Date
Google	La tua password è stata modificata - La tua password è stat...	24 mar
Il team di Gmail	Il meglio di Gmail, ovunque tu sia - Ciao...	23 mar
Il team di Gmail	Organizza le tue email con la Posta in arrivo di Gmail - Cia...	23 mar
Il team di Gmail	Tre suggerimenti per ottenere il massimo da Gmail - Cia...	23 mar

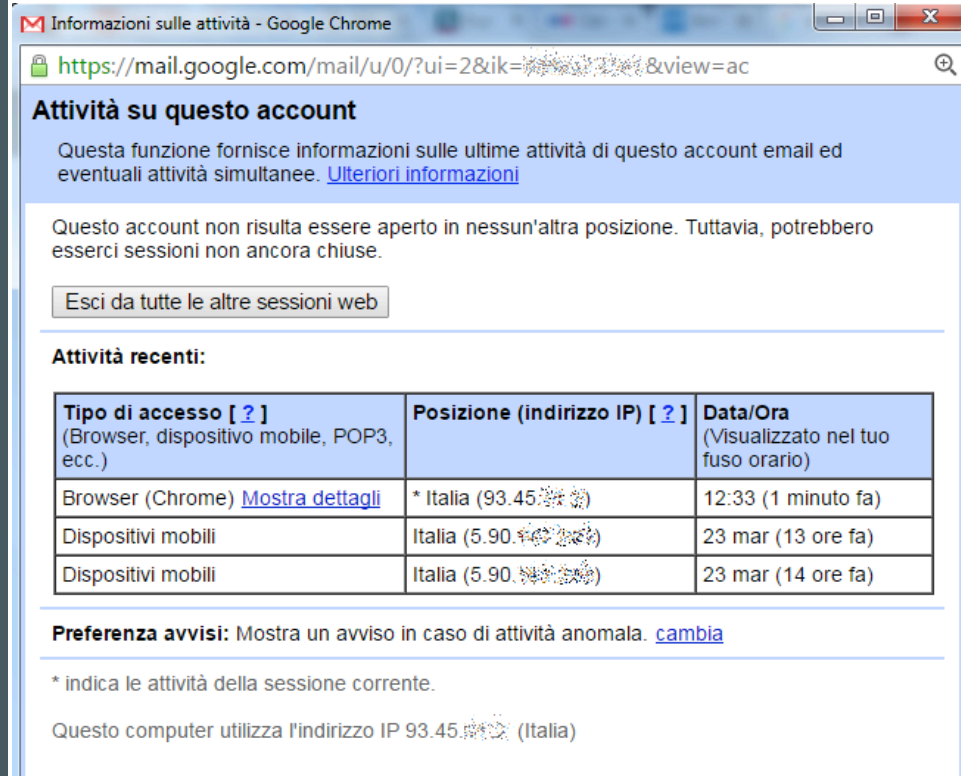
At the bottom of the page, there is a status bar with the following information:

- 0 GB (0%) di 15 GB utilizzati
- [Termini](#) - [Privacy](#)
- Ultima attività dell'account: 2 minuti fa
- [Dettagli](#)

A red arrow points to the [Dettagli](#) link.

Trace

From the details of your account you can see the history of connections to the account, with the IP and the type of device used.



Informazioni sulle attività - Google Chrome

<https://mail.google.com/mail/u/0/?ui=2&ik=...&view=ac>

Attività su questo account

Questa funzione fornisce informazioni sulle ultime attività di questo account email ed eventuali attività simultanee. [Ulteriori informazioni](#)

Questo account non risulta essere aperto in nessun'altra posizione. Tuttavia, potrebbero esserci sessioni non ancora chiuse.

[Esci da tutte le altre sessioni web](#)

Attività recenti:

Tipo di accesso [?] (Browser, dispositivo mobile, POP3, ecc.)	Posizione (indirizzo IP) [?]	Data/Ora (Visualizzato nel tuo fuso orario)
Browser (Chrome) Mostra dettagli	* Italia (93.45.40.100)	12:33 (1 minuto fa)
Dispositivi mobili	Italia (5.90.40.100)	23 mar (13 ore fa)
Dispositivi mobili	Italia (5.90.40.100)	23 mar (14 ore fa)

Preferenza avvisi: Mostra un avviso in caso di attività anomala. [cambia](#)


* indica le attività della sessione corrente.

Questo computer utilizza l'indirizzo IP 93.45.40.100 (Italia)

Locate

Using the IP address connection history you can geolocate the device who set up that account

IP Address Database Lookup



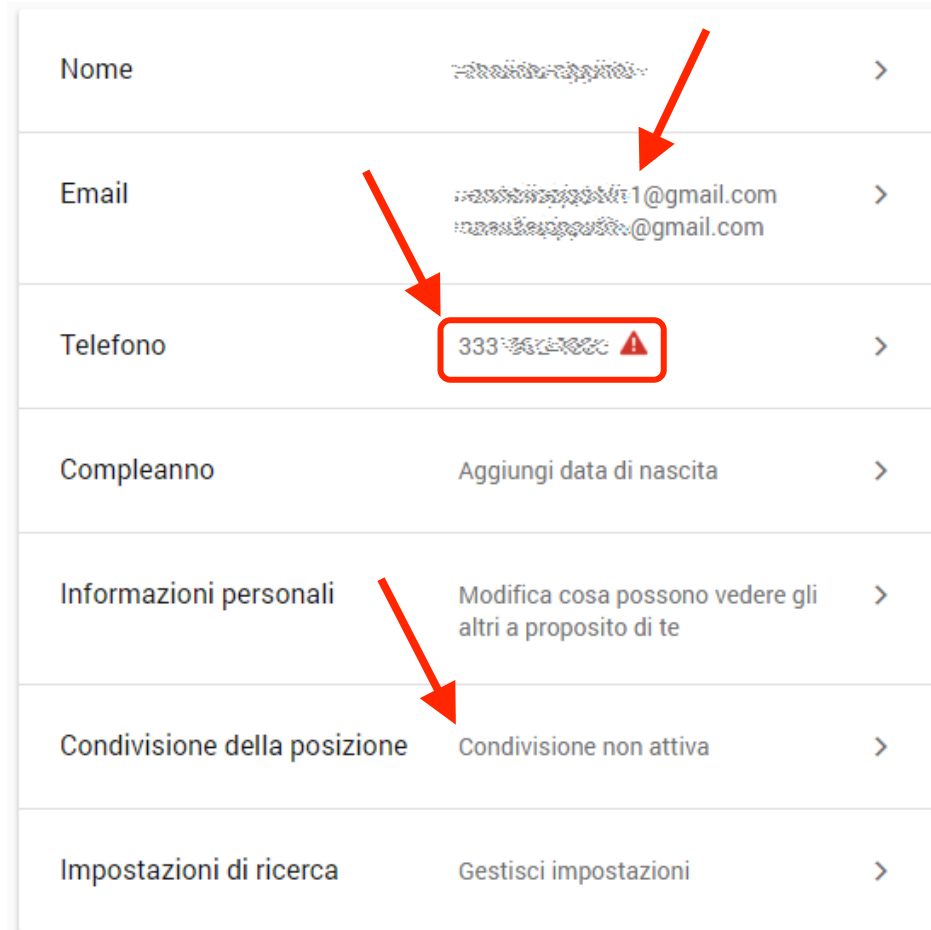
Mappa Satellite

Your IP address is 5.90.133.133
City: Ivrée
Country: Italy
Continent: Europe
Time Zone: GMT+1 [more demo?](#)

Belgio Francoforte Praga Repubblica Ceca Slovacchia
Parigi Vienna Budapest
Francia Svizzera Austria Ungheria
Milano Venezia Slovenia Zagabria
Croazia Bosnia ed Erzegovina
Monaco Firenze Italia
Andorra Sarajevo
Barcellona Podgorica
Madrid Google Dati mappa Termini e condizioni d'uso Segnala un errore nella mappa
5.90.133.133 Find
Data obtained from IPIntelligence Max [Learn more...](#)

Personal info

The profile of google account contains personal information, including geolocation. We see that the account was linked to two different e-mail addresses, which differs by only one digit.



The screenshot shows the 'Personal info' section of a Google Account. Red arrows highlight specific details: one points to the 'Nome' field, another to the first email address, a third to the phone number (which is highlighted with a red box and a warning icon), and a fourth to the 'Informazioni personali' section.

Nome	[Redacted]	>
Email	[Redacted]1@gmail.com [Redacted]@gmail.com	>
Telefono	333 [Redacted] ⚠	>
Compleanno	Aggiungi data di nascita	>
Informazioni personali	Modifica cosa possono vedere gli altri a proposito di te	>
Condivisione della posizione	Condivisione non attiva	>
Impostazioni di ricerca	Gestisci impostazioni	>

Lock out

After changing the mobile phone number associated to the account, the creator has no more means to get in. You can lock, wipe and make ring the mobile device linked to the account.



Hijack

With the “lock” feature you can even “hijack” the remote device which will display a message and the option to call just one specific phone number.

Nuova schermata di blocco

L'attuale schermata di blocco verrà sostituita con un blocco tramite password. Non utilizzare la password del tuo account Google.

Nuova password

Conferma password

Messaggio per il ripristino (opzionale)

Numero di telefono (facoltativo)

Annulla

Blocca

Remove device

You can contact the person which tried to link his email account to yours to verify its intentions explaining that s/he gave you lock and wipe control on his device.

Dispositivi utilizzati di recente

I dispositivi che sono stati attivi sul tuo account negli ultimi 28 giorni o con cui hai eseguito l'accesso di recente. [Ulteriori informazioni](#)



Hai notato qualcosa di sospetto? [Proteggi il tuo account](#)



Windows

Bologna, Italia **DISPOSITIVO IN USO**



Windows

Bologna, Italia - 4 minuti fa



IGGY

Italia - 8 ore fa



Ipap di [redacted]

Ultima sincronizzazione: ieri alle ore 20:29 ?



Accesso all'account

RIMUOVI

Modello del dispositivo

iPad

Case study:
Lessons to learn



Cyber-darwinism: the most fit species will survive

A careless typo on the recovery email address when creating your account, with no awareness of the possible consequences.



The digital identity dies

(Even if is protected by passwords, SSH encryption, two-step authentication.

Technology is nothing without knowledge)

Attention, awareness, knowledge and intention to exploit information received by mistake.



The digital identity lives

(And prevails to weaker digital identities)

We should trust our
knowledge more than
technologies

The human factor is
the weakest point of
the IT security chain

Dos and don'ts

Weak passwords which contains your name, your year of birth or other personal information.

Password written on paper bites

Smartphone without a pin

Skip software and OS updates

Click and type with no idea of what you're doing

Keys left in the main door of your house

Strong passwords, but easy to remember. (e.g. join your favourite drinks for 7UP.whisky2malt)

Password manager (Keepass or others)

Encrypted and protected smartphone

Do regular housekeeping of your devices

Be aware of what you are doing

Keep your house locked and safe.

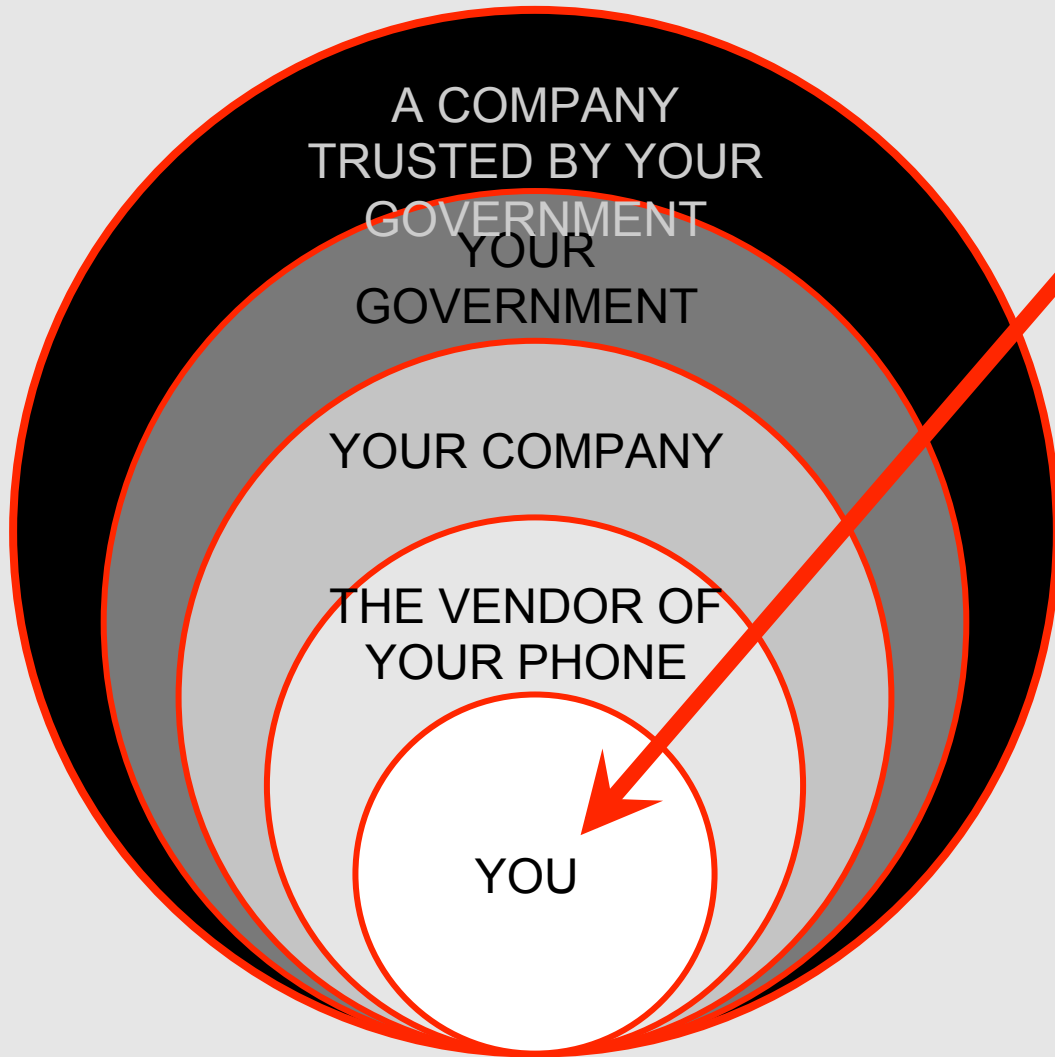
Common scam schemes lists:

[https://www.fbi.gov/scams-safety/fraud/
internet fraud/](https://www.fbi.gov/scams-safety/fraud/internet-fraud/)

[https://en.wikipedia.org/wiki/
List of confidence tricks](https://en.wikipedia.org/wiki/List_of_confidence_tricks)

Who should have
control over your
data?

Who should be able
to enter in your
home?



HOW STRONG
ARE THEIR
PROTECTION
S TO DEFEND
YOUR
PERSONAL
DATA?

IF WE OPEN
OUR DEVICES
TO 3RD
PARTIES,
THEIR

CONTENT
COULD BE
ACCESSED
BY...

POTENTIAL
LY
EVERYBO
DY

YOU

FREE TOOLS
FOR STRONG
ENCRYPTION
OF DATA AND
DEVICES



People don't care

The most popular passwords of
2015

The 25 Most Popular Passwords of 2015: We're All Such Idiots



Jamie Condliffe

1/19/16 12:01am · Filed to: PASSWORDS



It's 2016 and you may have thought we'd all be a little older and wiser than this time last year. But as you read this list of 2015's most popular passwords, you will shake your head, mumble unmentionables and reach the firm conclusion that, no, we are in fact all still complete and utter morons.

Every year, SplashData compiles a list of the millions of stolen passwords made public throughout the last twelve months, then sorts them in order of popularity. This year the results, based on a total of over 2 million leaked passwords, are not the list of random alpha-numeric characters you might hope for. Rather, they're a lesson in exactly how not to choose a password.

Yes, "123456" and "password" remain bewilderingly popular.

People don't care

The most popular passwords of
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)

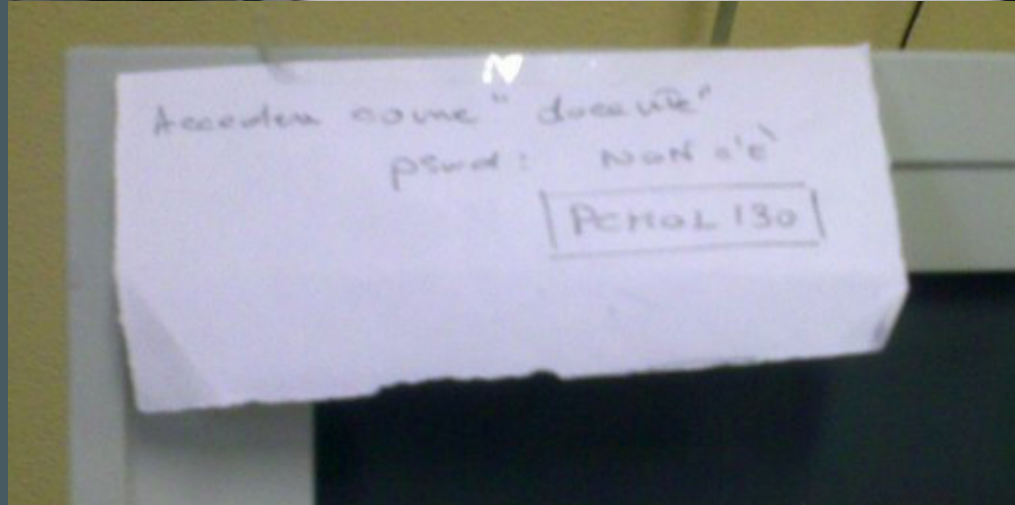
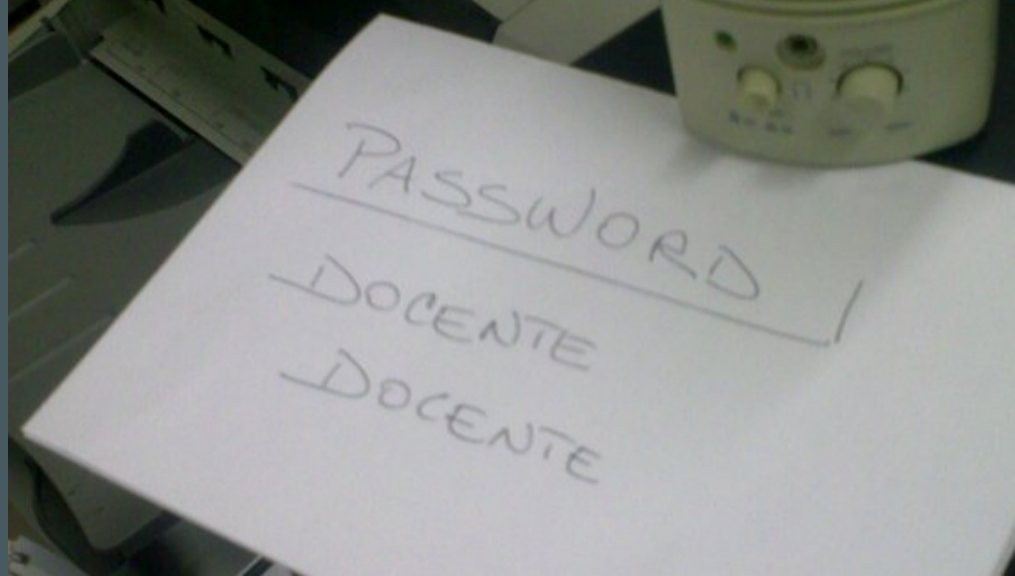
8. 1234 (Down 1)

9. 1234567 (Up 2)

10. baseball (Down 2)

People don't care

Some examples which I could
document personally



Outdated and Vulnerable WordPress, Drupal Versions Contributed To Panama Papers Breach



(wptavern.com)

155



Posted by **BeauHD** on Wednesday April 06, 2016 @08:28PM from the contributing-factors dept.

Admins don't care

“You pay as I want,
I work as you say.
You pay as you say,
I work as I want”.

CORRIERE DELLA SERA / CRONACHE



PANAMA PAPERS



3



522



25

Alla Mossack Fonseca sarebbero bastati **6 euro** per fermare gli hacker

Una somma irrisoria che avrebbe permesso di aggiornare una funzionalità della piattaforma Wordpress (sulla quale si appoggia il sito) e che nel 2014 si è scoperto essere diventata una porta di accesso per gli attacchi informatici

di Leonard Berberi

6 EUR WOULD
HAVE
STOPPED THE
BIGGEST
DATA LEAK

OF

“Così ho attaccato Hacking Team”

L'hacker sospettato di aver bucato l'azienda milanese riappare e pubblica un resoconto di come avrebbe fatto

Hackers do
care

The motivational side of
system intrusion

“This is the beauty and asymmetry of hacking: just one people, working a hundred of hours, can dismantle years of work of a multimillionaire company. Hacking gives to underprivileged people the opportunity to fight and win”.

Phineas Fisher / Hack Back

Author of the leak against the italian company “Hacking team”, accused of selling cybersurveillance technologies to authoritarian regimes like Sud Corea, Kazakistan, Arabia Saudita, Oman, Libano, Mongolia, Sudan.

Hackers do care

The motivational side of
system intrusion

“My motivation was the quest for knowledge, the intellectual challenge, the thrill and also the escape from reality. (...) [with] a lot of the companies I targeted, to get the software was simply a trophy. I'd copy the code, store it on the computer and go right on to the next without even reading the code.”

Kevin Mitnick

Notorious Hacker and IT security Expert

Hacking without a PC:

Blueboxing

Lockpicking

Shouldersurfing

Social engineering

On March 2, 2000, the U.S. Senate Committee on Governmental Affairs held a hearing on the security of federal information systems. Kevin Mitnick, who has been called the most notorious hacker of all time, spoke before the committee:

*“Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address **the weakest link in the security chain**: the people who use, administer, operate and account for computer systems that contain protected information”.*

Kevin Mitnick hearing to US Senate

*“In my experience when I would try to get into these systems, the first line of attack would be what I call **a social engineering attack**, which really means trying to **manipulate somebody** over the phone through **deception**. And I was so successful in that line of attack that I rarely had to go toward a technical attack. (...)*

*I obtained confidential information in the same way government employees did. And I did it all **without even touching a computer**.*

*Let me emphasize for the committee the fact that these breaches of information security are ongoing, even as I stand before you today, and that agency employees are being **manipulated using social engineering exploits**, despite the current policies, procedures, guidelines and standards already in place at these*

The solution:
Awareness &
Knowledge

Kevin Mitnick hearing to US Senate (2000)

*“I really have a firm belief that **there has to be extensive training and education** to educate the users and the people who administer and use these computer systems that they can be victims of manipulation over the telephone”.*

Digital Divide - ISTAT Statistical data

Among families with at least one minor:

87% of families has a PC

89% has internet access

Among families with only aged people over 65:

17,8% of families has a PC

16,3% has internet access

<http://www.istat.it/it/archivio/143073>

How do we want to protect from computer fraud that 16% of families with elder people connected to the internet?

La ricchezza che nasce dalla conoscenza

- Investire in conoscenza e formazione
- Per trasformare il sud Italia in una Silicon Valley basta il valore della conoscenza
- Scommettere sull'eccellenza italiana informatica (FLOSS, Arduino, Security)
- Sostenere iniziative orientate alla promozione dell'IT Awareness
- Valorizzare (anche economicamente) le professionalità del settore IT