Oops they did it again: il data breach nell'era del GDPR

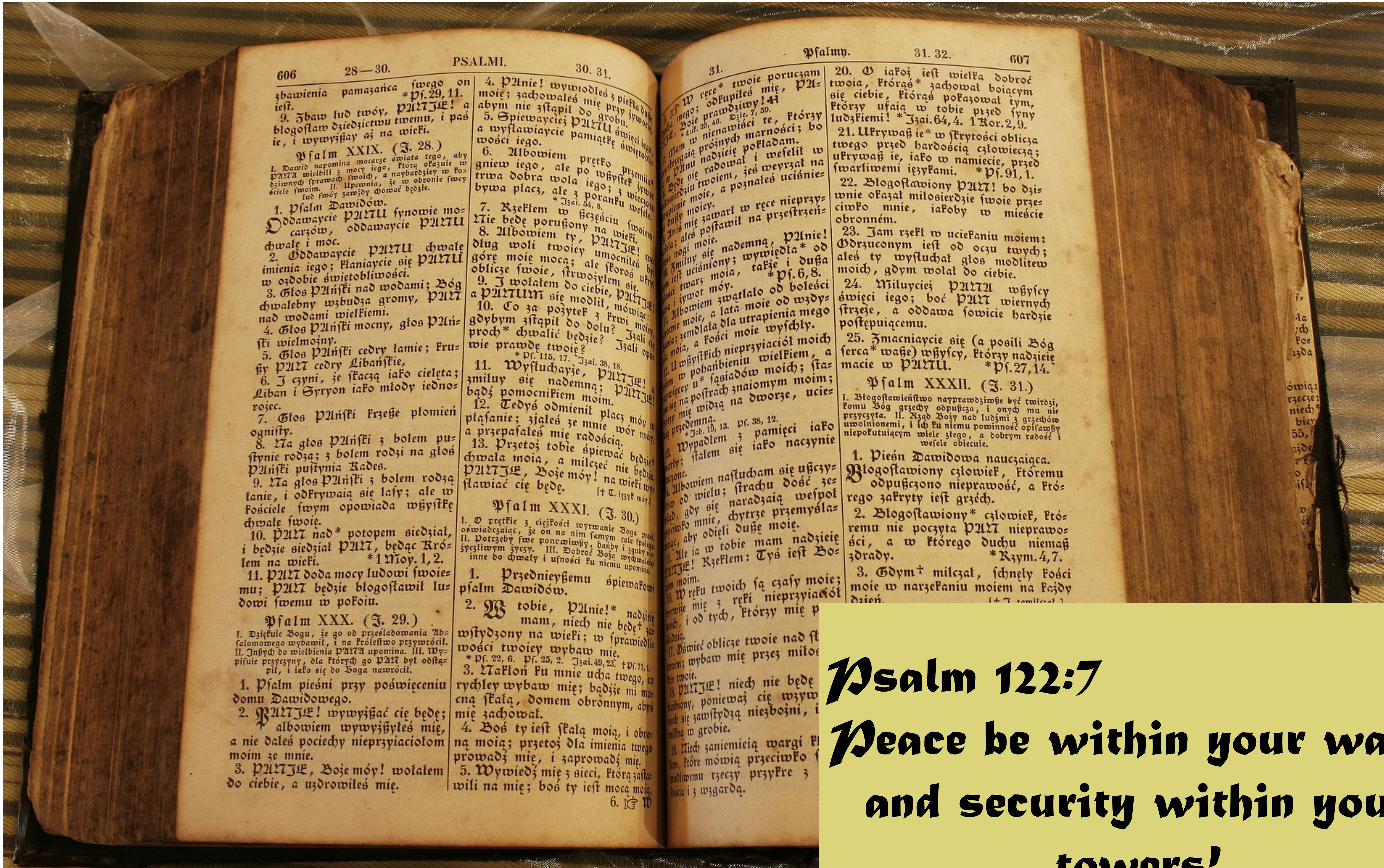
Avv. Giovanni Battista GALLUS, LL.M., Ph.D - gallus@array.eu

Hermes Center for Transparency and Digital Human Rights
Nexa Center for Internet and Society
Circolo dei Giuristi Telematici

Bologna, 8 giugno 2018

Perché parlare di data breach?

Sicurezza perimetrale 1.0



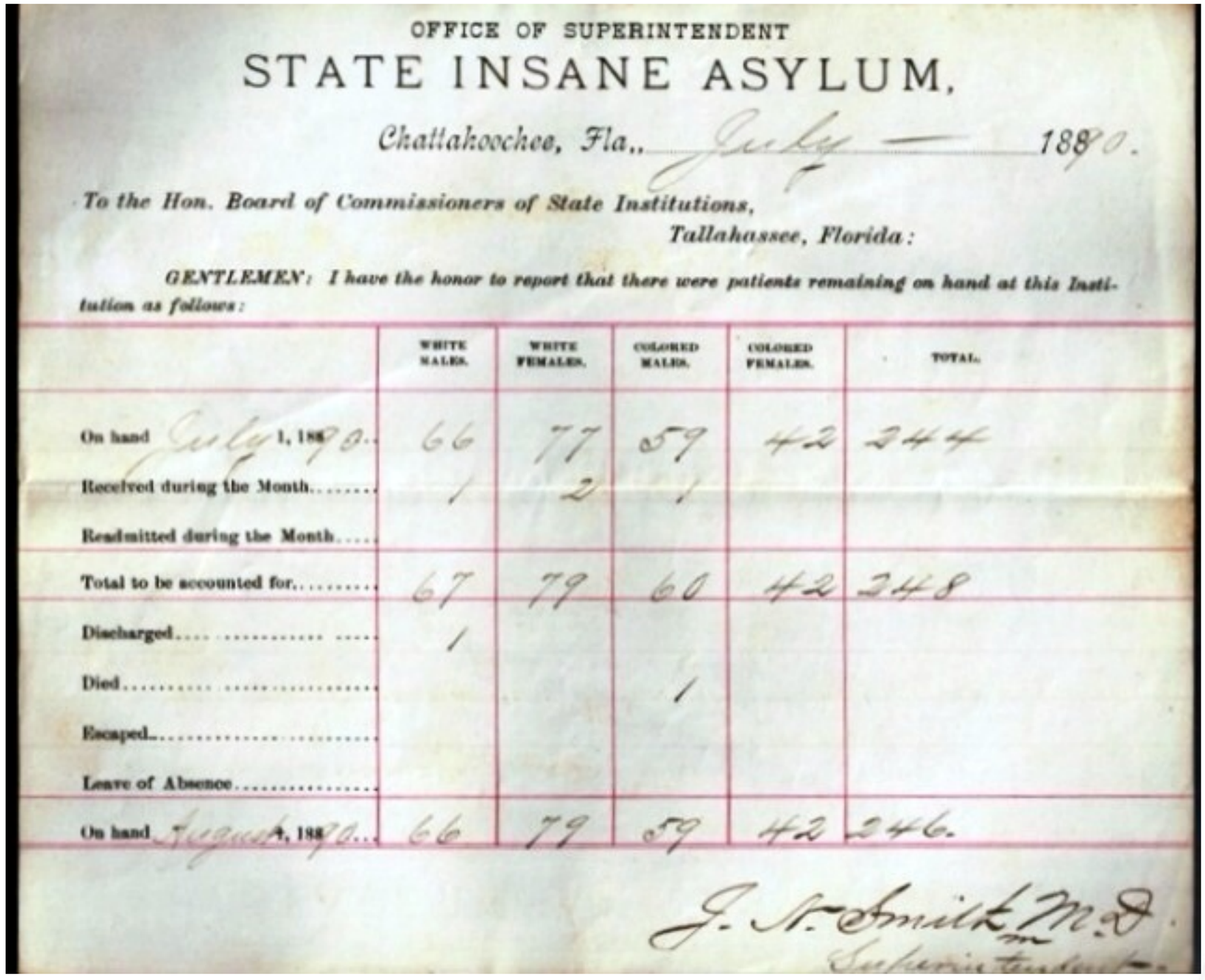
Psalm 122:7

Peace be within your walls and security within your towers!

Il primo data breach?

1903 - The dispensary records for the Southern California Hospital for the Insane went missing, and were through to be stolen (or "purloined" as the LA Times put it) by ex-Steward C.N. Whitaker and former druggist, Fred W. Howard.

https://
blog.datalossdb.org



OFFICE OF SUPERINTENDENT

STATE INSANE ASYLUM,

Chattahoochee, Fla., July — 1890.

To the Hon. Board of Commissioners of State Institutions,
Tallahassee, Florida:

GENTLEMEN: I have the honor to report that there were patients remaining on hand at this Institution as follows:

	WHITE MALES.	WHITE FEMALES.	COLORED MALES.	COLORED FEMALES.	TOTAL.
On hand July 1, 1890	66	77	59	42	244
Received during the Month	1	2	1		
Readmitted during the Month					
Total to be accounted for	67	79	60	42	248
Discharged	1				
Died			1		
Escaped					
Leave of Absence					
On hand August 1, 1890	66	79	59	42	246.

J. S. Smith M.D.
Superintendent.

CC/BY Sean . https://www.flickr.com/photos/22280677@N07/8509429865

Cyber-Safe

Every single Yahoo account was hacked - 3 billion in all

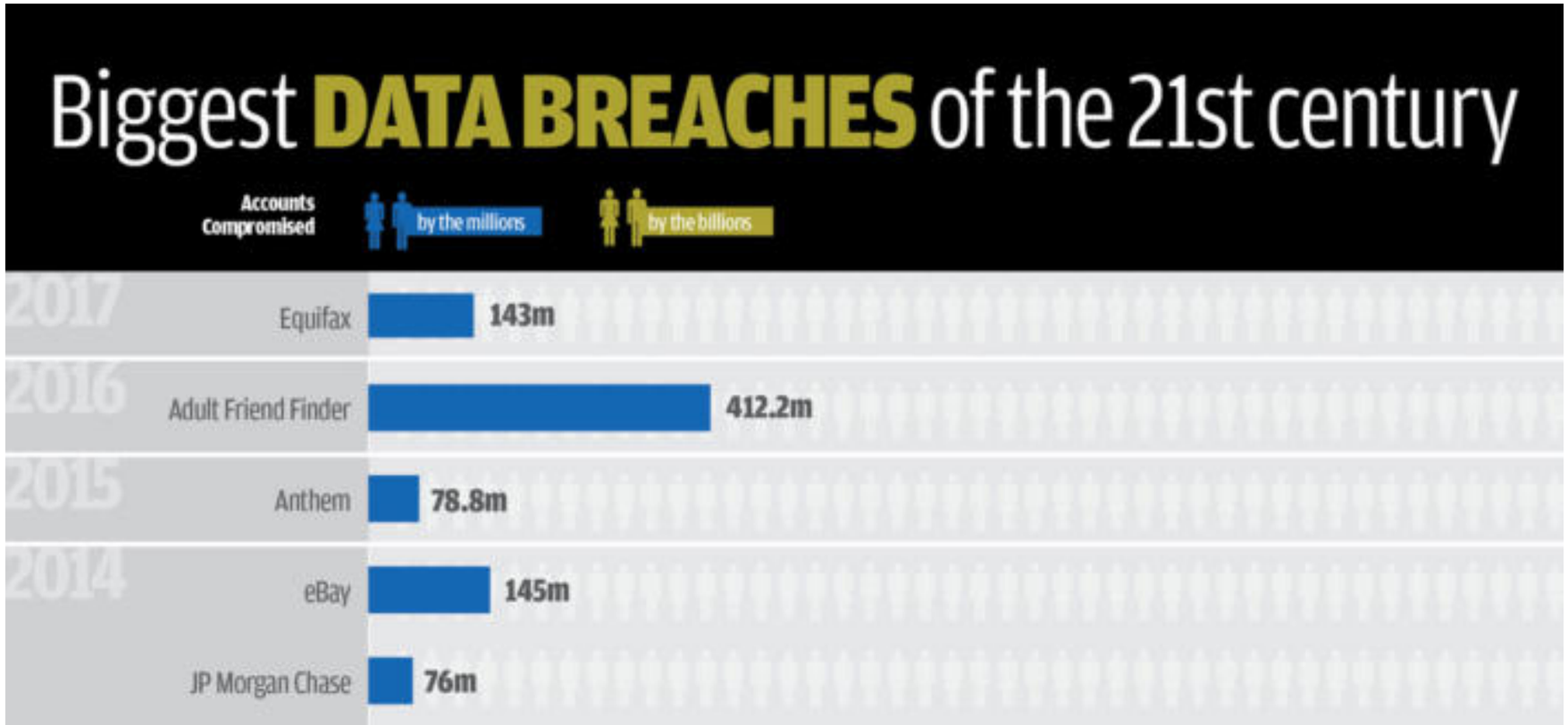
by Selena Larson @selenalarson

October 4, 2017: 6:36 AM ET

Timeline: The rise and fall of Yahoo

Sitting down? An epic and historic data breach at Yahoo in August 2013 affected every single customer account that existed at the time, Yahoo parent company Verizon said on Tuesday.

Biggest DATA BREACHES of the 21st century



Un data breach senza cappuccio
non vale
e non va notificato al Garante...

blastingnews

Cerca su Blasting News...

BLASTING NEWS - SCOPRI | OPINIONI | LAVORO GIOVANI | TERREMOTO | GUERRINA PISCAGLIA | SCUOLA | SCIOPERO GENERALE

Blasting News > Opinioni > 2017 > 08 > Ransomware, se la vittima è il commercialista per i clienti addio privacy

Ransomware, se la vittima è il commercialista per i clienti addio privacy

Studio di professionisti di Battipaglia viene colpito da un virus che prende in ostaggio tutti i dati delle denunce dei redditi di 157 clienti

We need to talk about all these absurd stock photos of hackers - mashable.com

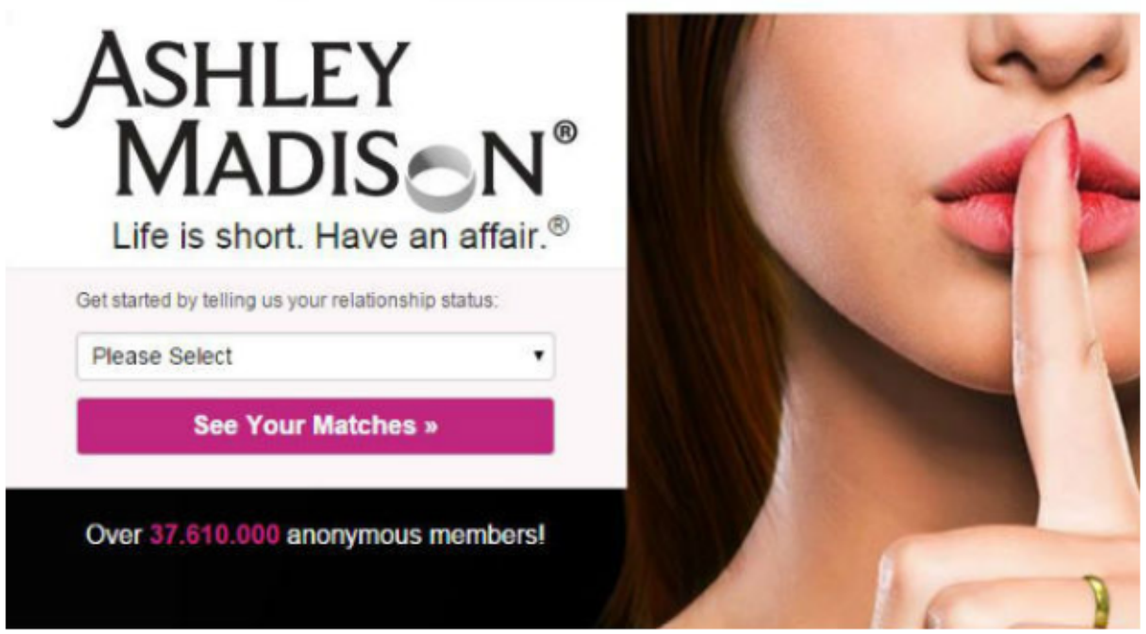
Nicola Bernardi | SEGUI
Curata da Vinicio Marchetti *Pubblicato il: 10 agosto 2017*

Dopo l'epidemia di "WannaCry", che lo scorso maggio ha imperversato per mezzo pianeta colpendo oltre 230mila computer in 150 paesi, ormai dovrebbero saperlo tutti, specialmente i professionisti, che esistono i cosiddetti "ransomware", pericolosi virus informatici che sono in grado di

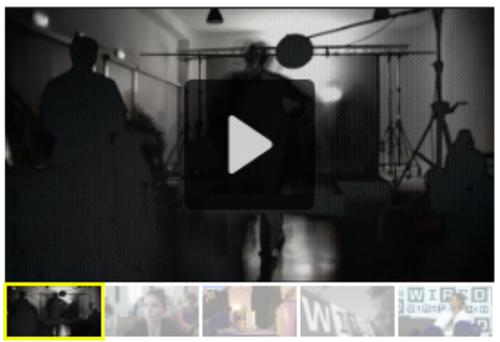
Ashley Madison, online tutti i dati dei traditori

di **Giuditta Mosca**
19 AGO, 2015

Lo scorso luglio un gruppo di hacker ha violato il famoso sito per adulteri, prelevando milioni di dati sensibili. Ora sono disponibili online



VIDEO



I dati di **milioni di fedifraghi** prelevati dal sito **Ashley Madison** lo scorso luglio sono online, nel file da **9,7 GB** si possono trovare i **nomi** degli utenti, i loro **indirizzi email**, **preferenze sessuali** e le transazioni avvenute tramite

Fonte: IBM Security – Ponemon Institute, 2017

The odds are much greater that you will experience a data breach

Experiencing a data breach?

1 in 4

(Global average 28%)

Probability that an organization in the study will experience a data breach over two-year period

Ghostery Tries to Comply With GDPR, but Ends Up Violating GDPR in the Process

By Catalin Cimpanu

May 28, 2018 08:58 AM 1

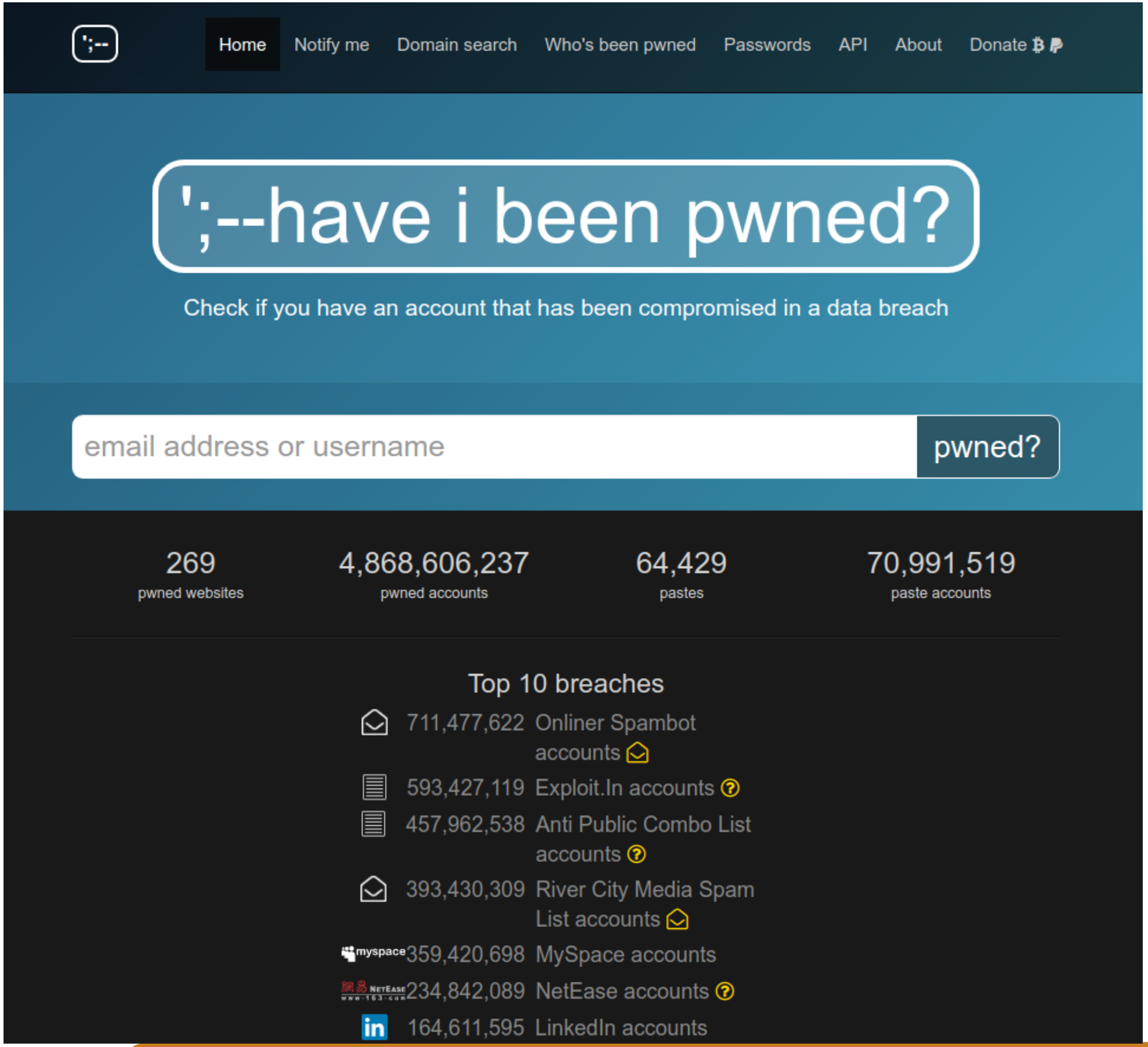
The company behind Ghostery, a privacy-focused browser and an ad-blocking browser extension, has apologized for a technical error that occurred last Friday when its staff was sending out GDPR-themed notification emails.

Violato l'archivio di MyHeritage, la piattaforma degli alberi genealogici

92 milioni di credenziali trovate online da un ricercatore. Ma i dati genetici sono al sicuro, dice l'azienda

di **CAROLA FREDIANI** | 07 giugno 2018,08:36

MY HERITAGE HACKER


';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
269
pwned websites
4,868,606,237
pwned accounts
64,429
pastes
70,991,519
paste accounts
Top 10 breaches
711,477,622 Onliner Spambot accounts
593,427,119 Exploit.In accounts
457,962,538 Anti Public Combo List accounts
393,430,309 River City Media Spam List accounts
359,420,698 MySpace accounts
234,842,089 NetEase accounts
164,611,595 LinkedIn accounts

È una figura del tutto nuova?

Violazioni di dati personali *(data breach)*

Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedime
amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a s
informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamit
perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmes
La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014
[doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015
[doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015
[doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

i pubblicati sul sito: www.garanteprivacy.it

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VEDI ANCHE provvedimento del 26 luglio 2017

[doc. web n. 6376175]

Trattamento di dati personali riguardanti l'intestazione di utenze telefoniche - 6 aprile 2017

IL GARANTE PER LA P

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 6431926]

Violazione di dati personali nel settore dei servizi telefonici - 11 maggio 2017

Registro dei provvedimenti
n. 226 dell'11 maggio 2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

VEDI ANCHE Provvedimento del 6 aprile 2017

[doc. web n. 6821640]

Trattamento di dati personali riguardanti l'intestazione di utenze telefoniche - 26 luglio 2017

Registro dei provvedimenti
n. 344 del 26 luglio 2017

Arriviamo al GDPR

Ricordiamo brevemente:

Art. 5, comma 1, lett F.
1. I dati personali sono:
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Art. 24 - Responsabilità del titolare del trattamento

Art. 32 - Sicurezza del trattamento

Art. 35 – Data Protection Impact Assessment

Dalla gestione del rischio ex ante alla gestione ex post

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

"The focus of any breach response plan should be on protecting individuals and their personal data"

Redditi on line: illegittima la diffusione dei dati sul sito Internet dell'Agenzia delle entrate - 6 maggio 2008 [1512255]

G.U. n. 107 dell'8 maggio 2008

SCHEDA

Doc-Web:
1512255

Data:
06/05/08

Argomenti:
Fisco , Agenzia delle Entrate , Diffusione dati fiscali , Comunicazione a terzi , Dichiarazioni dei redditi

Tipologia:
Divieto del trattamento

[doc. web n. 1512255]
[doc. web n. **1519208**]
[v. Comunicati stampa: **30 aprile**, **2** e **6** maggio 2008]
[v. provv. **1510761**]

Redditi on line: illegittima la diffusione dei dati sul sito Internet dell'Agenzia delle entrate - 6 maggio 2008
G.U. n. 107 dell'8 maggio 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

ANSA.it Economia

Fai la ricerca | Il mondo in Immagini

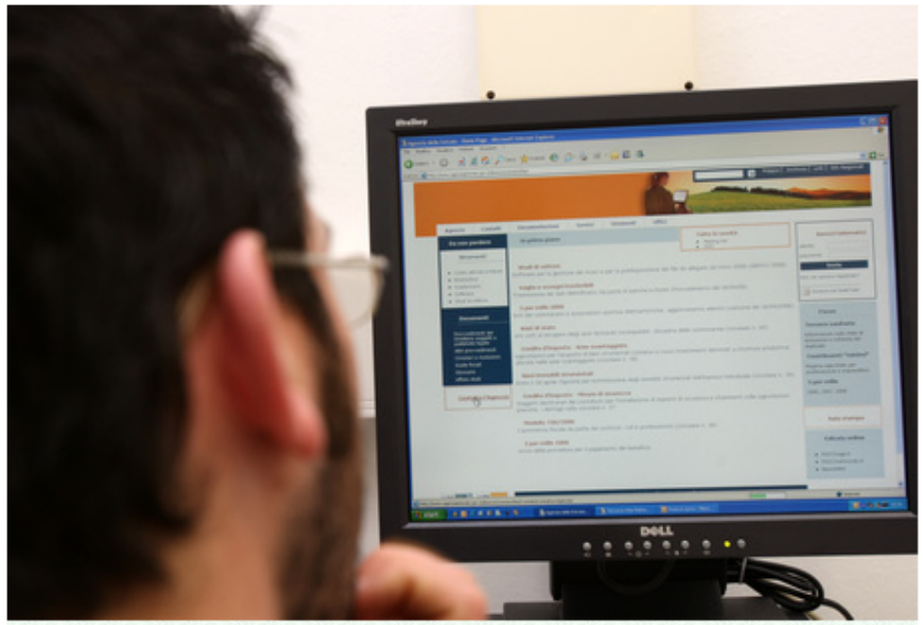
Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia | Sp

PRIMOPIANO • BORSA • INDUSTRY 4.0 • FINANZA PERSONALE • PROFESSIONI • REAL ESTATE • PMI •

ANSA.it › Economia › Spesometro, dati altrui non più visualizzabili

Spesometro, dati altrui non più visualizzabili

Governo valuta misure, faro Garante Privacy Commercialisti chiedono altra



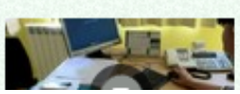
© ANSA

CLICCA PER INGRANDIRE

Dopo il blocco dello Spesometro online e il ripristino (non del tutto completo) avvenuto ieri mattina, Sogei ha comunicato che "nessun utente può più visualizzare dati di altri soggetti per i quali non è stato espressamente delegato dal sistema". Lo ha precisato il direttore dell'Agenzia delle Entrate, Ernesto Maria Ruffini, in audizione alla Commissione Anagrafe tributaria.

Scrivi alla redazione

Notizie Correlate



CORRIERE DELLA SERA / POLITICA

1

2873

FISCO E PRIVACY

Buco nel sistema: fatture elettroniche online. Indagano Garante e Vigilanza

Con un semplice codice fiscale si potevano vedere e scaricare le fatture telematiche trasmesse all'Agenzia delle Entrate. L'Ad Ruffini «nero», chiede una relazione alla Sogei. Il presidente della Vigilanza parlamentare «furibondo». Il Garante chiede lumi.

di **Mario Sensini**

Sanzioni e responsabilità civile

Art. 83 GDPR

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli **obblighi del titolare** del trattamento **e del responsabile del trattamento** a norma degli articoli 8, 11, **da 25 a 39**, 42 e 43;

Art. 83 GDPR

- Omessa notificazione o comunicazione
- Inidonea notificazione o comunicazione
- Ritardo
- Omessa documentazione
- …

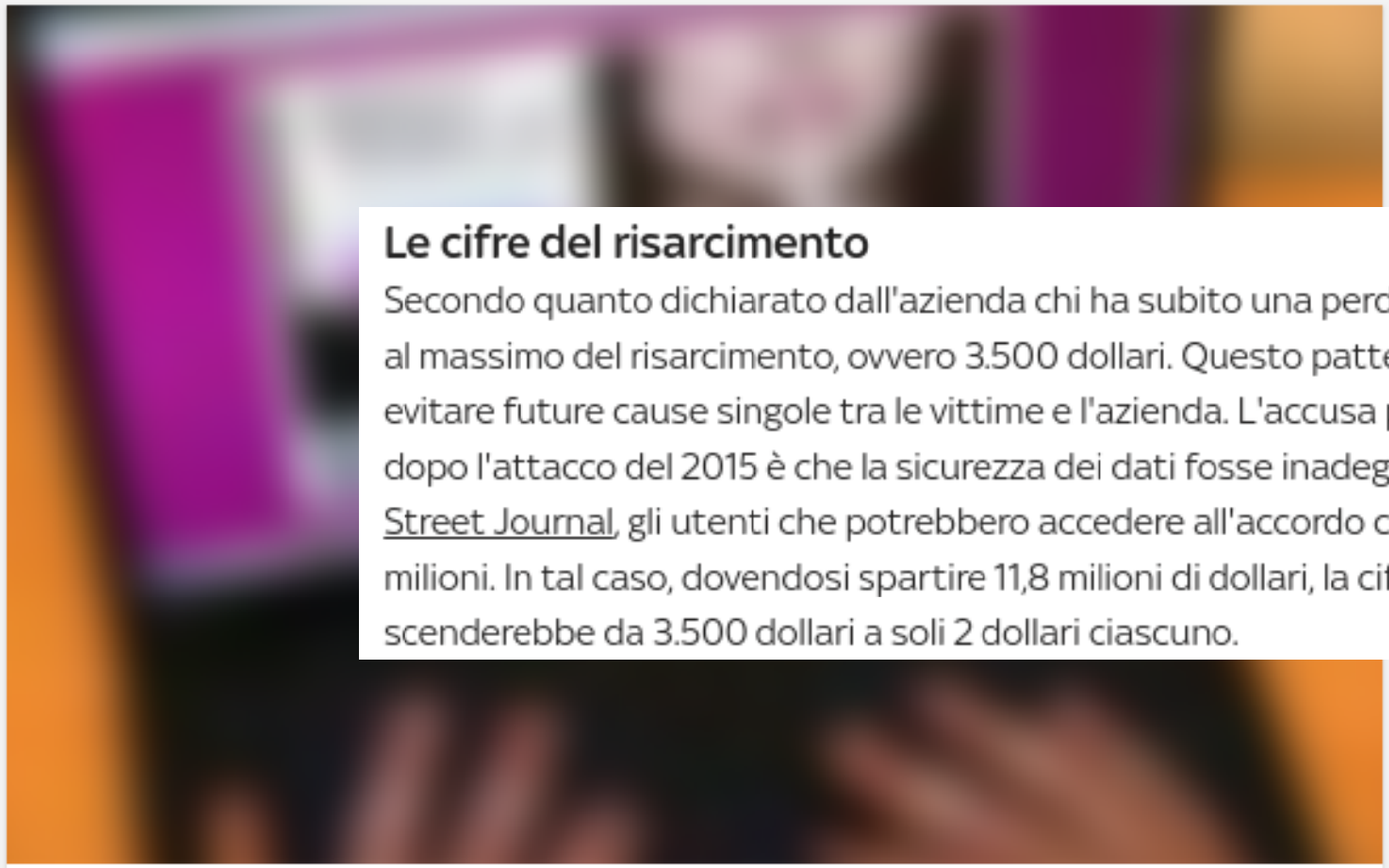
Tra i criteri per l'irrogazione della sanzioni vi è:

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

TECNOLOGIA

18 luglio 2017

Ashley Madison pagherà 12 milioni di dollari a vittime cyber attacco



Le cifre del risarcimento

Secondo quanto dichiarato dall'azienda chi ha subito una perdita consistente potrà aspirare al massimo del risarcimento, ovvero 3.500 dollari. Questo patteggiamento è stato deciso per evitare future cause singole tra le vittime e l'azienda. L'accusa principale mossa all'azienda dopo l'attacco del 2015 è che la sicurezza dei dati fosse inadeguata. Secondo le stime del Wall Street Journal, gli utenti che potrebbero accedere all'accordo con la Ruby Life Inc. sono 6 milioni. In tal caso, dovendosi spartire 11,8 milioni di dollari, la cifra che spetterebbe loro scenderebbe da 3.500 dollari a soli 2 dollari ciascuno.

Il sito dedicato alle relazioni extraconiugali Ashley Madison ha annunciato che risarcirà le vittime del cyber-attacco del 2015 (foto di archivio-Getty Images)

La compagnia Ruby Life Inc risarcirà gli utenti americani del sito dedicato alle relazioni extraconiugali. L'accordo è stato raggiunto dopo la class action

- Il danno non patrimoniale risarcibile ai sensi dell'art. 15 del d.lgs. 30 giugno 2003, n. 196 (c.d. codice della privacy) non si sottrae alla verifica di "gravità della lesione" (concernente il diritto fondamentale alla protezione dei dati personali, quale intimamente legato ai diritti ed alle libertà indicate dall'art. 2 del codice, convergenti tutti funzionalmente alla tutela piena della persona umana e della sua dignità) e di "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), che, in linea generale, si richiede in applicazione dell'art. 2059 cod. civ. nelle ipotesi di pregiudizio inferto ai diritti inviolabili previsti in Costituzione

- ove l'offesa non superi la soglia di minima tollerabilità o il danno sia futile, si può escludere la possibilità di somministrare il risarcimento del danno

Cass., Sez. 3, sent. 16133/2014

Violazione di dati personali e responsabilità civile

Civile Ord. Sez. 1 Num. 14242 Anno 2018
Presidente: CAMPANILE PIETRO
Relatore: CIRESE MARINA
Data pubblicazione: 04/06/2018

La fattispecie delineata dai due commi dell'art. 15 del d.lgs. n. 196 del 2003 pone quindi ***due presunzioni****:*

- ***Il danno è da addebitare a chi ha trattato i dati personali*** *o a chi si è avvalso di un altrui trattamento a meno che egli non dimostri di avere adottato tutte le misure idonee per evitarlo ai sensi dell'art. 2050 c.c. e* ***quella secondo la quale le conseguenze non patrimoniali di tale danno*** *— sia esso di natura contrattuale che extracontrattuale —* ***sono da considerare in re ipsa a meno che il danneggiante non dimostri che esse non vi sono state*** *ovvero che si tratta di un danno irrilevante o bagatellare ovvero ancora che il danneggiato abbia tratto vantaggio dalla pubblicazione dei dati.*

Grazie

per l'attenzione