ORDINE DEI DOTTORI
COMMERCIALISTI
E DEGLI ESPERTI CONTABILI
DI FERRARA

Associazione
Nazionale
Commercialisti
FERRARA

opera
professioni

Partner
24ORE

COMPLIANCE NEGLI STUDI PROFESSIONALI
NOVITÀ ANTIRICICLAGGIO E PRIVACY

PROFESSIONISTI

6 marzo 2023

opera professioni

INSIEME, SI CRESCE!

Tutto ciò che facciamo è finalizzato al costante **miglioramento**!

Perché crediamo fortemente che la crescita e il **successo** passino attraverso una continua **formazione**, **condivisione**, **innovazione** e evoluzione di sé.

avv. Antonio Valentini
a.valentini@operaprofessioni.it
+39 3481134952

Partner 24ORE

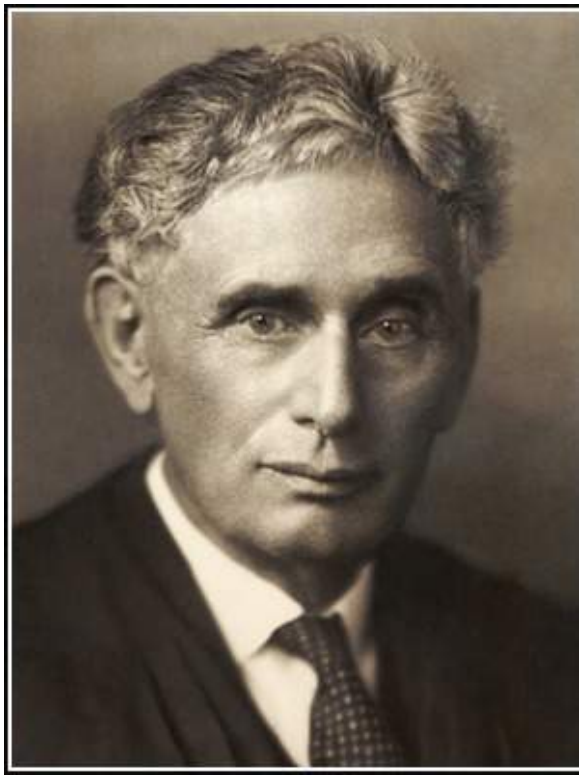
AGENDA

- QUADRO NORMATIVO ATTUALE
- AMBITO DI APPLICAZIONE
- DEFINIZIONI E PRINCIPI
- BASI GIURIDICHE
- NUOVI RUOLI DEI SOGGETTI COINVOLTI NEL TRATTAMENTO
- DIRITTI DELL'INTERESSATO
- DATA BREACH
- MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI
- OBBLIGHI IN CONCRETO

AGENDA

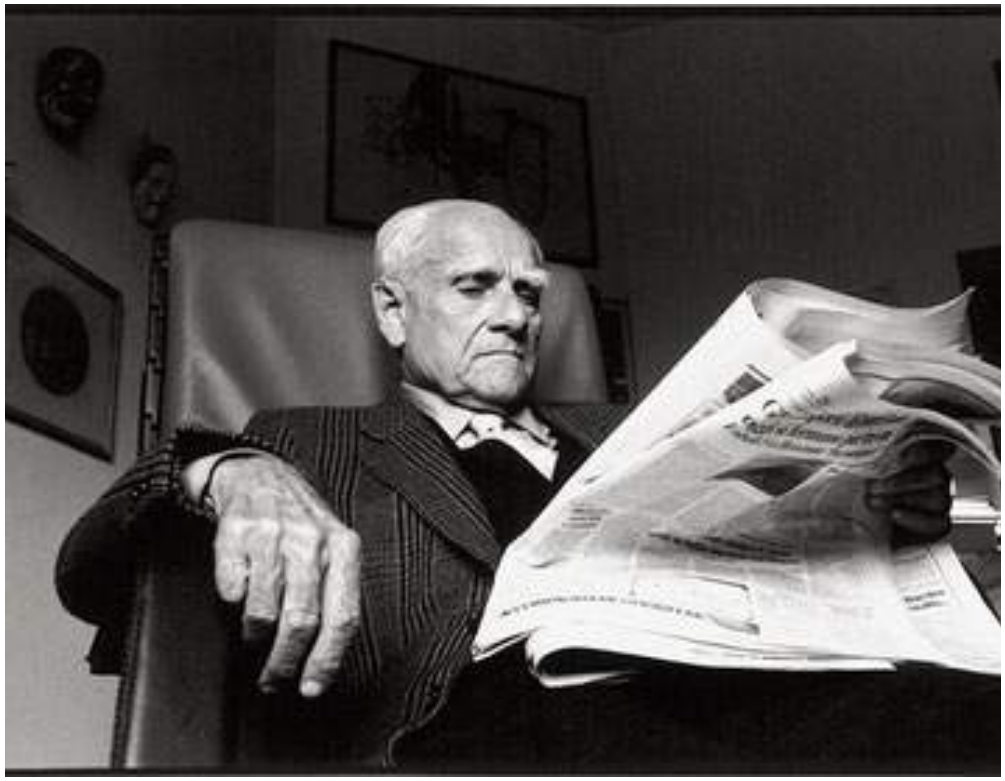
- QUADRO NORMATIVO ATTUALE
- AMBITO DI APPLICAZIONE
- DEFINIZIONI E PRINCIPI
- BASI GIURIDICHE
- NUOVI RUOLI DEI SOGGETTI COINVOLTI NEL TRATTAMENTO
- DIRITTI DELL'INTERESSATO
- DATA BREACH
- MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI
- OBBLIGHI IN CONCRETO

QUADRO NORMATIVO ATTUALE



" The makers of our Constitution)fourth amendment ,(conferred ,as against the government ,the right to be let alone—the most comprehensive of rights and the right most valued by civilized men"

Louis D. Brandeis



«La tecnologia non è la scienza. Al contrario della ricerca scientifica, che stimola l'iniziativa individuale, la tecnologia tende piuttosto a creare gli strumenti per un sempre maggiore controllo di tutti su tutti»

(Corriere della Sera,17 luglio 1969)

Alberto Moravia

«società confessionale che promuove la pubblica esposizione di sé al rango di prova eminente e più accessibile, oltre che verosimilmente più efficace, di esistenza sociale»

Zygmunt Bauman

• «*È paradossale che qualcuno debba lottare per la difesa della privatezza in una società di esibizionisti*»
(Bustina di Minerva, 13 giugno 2014 – La Perdita della privatezza)

• ***«****Chi difende la privacy difende qualcosa che la gente non vuole più; la gente ormai vuole andare in tv a dire che è cornuta, usa in modo spasmodico il telefonino, che è la negazione della privacy; va su Internet, si fa assalire dalle offerte pubblicitarie, paga ed è contenta****»***

(Convegno sull'Europa organizzato dall'Aspen Institute, Cernobbio 1998)

UN DIRITTO FONDAMENTALE

«Di fronte all'emergere di sempre più incisivi poteri "privati", il diritto all'autodeterminazione informativa costituisce uno dei più importanti presidi a tutela non solo dell'identità, dell'eguaglianza, della dignità ma anche un presupposto della tenuta delle stesse garanzie democratiche.»

Pasquale Stanzione

Presidente del Garante per la protezione dei dati personali

L'ATTUALE QUADRO NORMATIVO

- REGOLAMENTO UE 2016/679
- D. LGS 10 AGOSTO 2018 N. 101
- D. LGS 30 GIUGNO 2003 N. 196


REGOLAMENTO (UE)
N. 2016/679

G.D.P.R.
GENERAL DATA PROTECTION REGULATION

- È un Regolamento, non una Direttiva: non richiede una legge nazionale di recepimento, è immediatamente esecutivo
- È stato approvato il 24 maggio 2016: non richiede, quindi, ulteriori approvazioni
- La sua piena applicabilità decorre dal 25 maggio 2018
- Le sanzioni previste sono molto rilevanti e non possono essere ignorate, come pure il rischio di essere chiamati a rispondere di danni a terzi

LE PRINCIPALI NOVITÀ

- Uniformità in ambito UE
- Più attenzione a nuove tecnologie
- Responsabilizzazione per i titolari di trattamento (*accountability*)
- Approccio basato sulla "Privacy by design" e "Privacy by default"
- Adozione di misure tecniche ed organizzative adeguate
- Valutazione d'impatto sulla protezione dei dati
- Registro delle attività di trattamento

LE PRINCIPALI NOVITÀ

- Diritto all'oblio
- *Data Protection Officer* (DPO)
- Eliminazione notifica dei trattamenti
- Notifica e comunicazione degli eventi di "*data breach*"
- Responsabilità civile solidale tra titolare, contitolare e responsabile del trattamento
- Sportello unico ("one stop shop") per multinazionali
- Board europeo con poteri di indirizzo delle autorità garanti (erede dell'attuale gruppo ex art. 29)
- Nuovo sistema sanzionatorio

AGENDA

- QUADRO NORMATIVO ATTUALE
- AMBITO DI APPLICAZIONE
- DEFINIZIONI E PRINCIPI
- BASI GIURIDICHE
- NUOVI RUOLI DEI SOGGETTI COINVOLTI NEL TRATTAMENTO
- DIRITTI DELL'INTERESSATO
- DATA BREACH
- MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI
- OBBLIGHI IN CONCRETO

AMBITO DI APPLICAZIONE

AMBITO DI APPLICAZIONE

AMBITO DI APPLICAZIONE MATERIALE (ART. 2)

Il presente regolamento **si applica** al trattamento:

interamente o parzialmente automatizzato di dati personali

non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi

AMBITO DI APPLICAZIONE MATERIALE (ART. 2)

effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico

Il presente regolamento **non si applica** ai trattamenti:

effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (=> DIRETTIVA (UE) 2016/680).

AMBITO DI APPLICAZIONE TERRITORIALE (ART. 3)

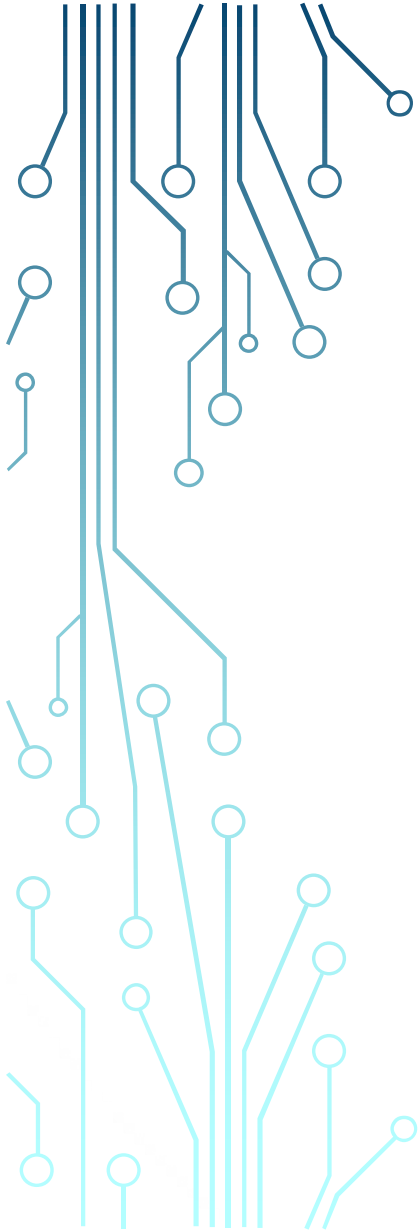
1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento **nell'Unione**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

AMBITO DI APPLICAZIONE TERRITORIALE (ART. 3)

2. Il presente regolamento si applica al trattamento dei dati personali di **interessati che si trovano nell'Unione**, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.



DEFINIZIONI


IS SHOE SIZE PERSONAL INFORMATION?
... IN CERTAIN CASES, YES...
MICHAŁ NAROJEK

DEFINIZIONI

"DATO PERSONALE" (Art. 4)

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera **identificabile** la persona fisica che può essere identificata, **direttamente** o **indirettamente**, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

DEFINIZIONI

"TRATTAMENTO" (Art. 4)

Qualsiasi **operazione** o **insieme di operazioni**, compiute con o senza l'ausilio di processi automatizzati e **applicate a dati personali o insiemi di dati personali**, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

PRINCIPI APPLICABILI (ART. 5)

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; […] («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

PRINCIPI APPLICABILI (ART. 5)

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; [...] («**limitazione della conservazione**»);

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**»).

ACCOUNTABILITY DI TITOLARI E RESPONSABILI

Il regolamento pone con forza l'accento sulla **"responsabilizzazione" (*accountability* nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Si tratta di una **grande novità** per la protezione dei dati in quanto viene **affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali** – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

ACCOUNTABILITY DI TITOLARI E RESPONSABILI

"*data protection **by default** and **by design***"

(art. 25 GDPR)

necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

ACCOUNTABILITY DI TITOLARI E RESPONSABILI

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del GDPR) e richiede, pertanto, **un'analisi preventiva** e un **impegno applicativo** da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

BASI GIURIDICHE

LICEITÀ DEL TRATTAMENTO
DATI COMUNI (ART. 6)

consenso dell'interessato al trattamento dei propri dati personali per una o più specifiche finalità

LICEITÀ:
se ricorre almeno una delle seguenti condizioni

trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento

trattamento necessario all'**esecuzione di un contratto o di misure precontrattuali** di cui l'interessato è parte

LICEITÀ DEL TRATTAMENTO
DATI COMUNI (ART. 6)

trattamento necessario per **salvaguardia di interessi vitali** dell'interessato o di un'altra persona fisica

LICEITÀ:
se ricorre almeno una delle seguenti condizioni

trattamento necessario per perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato

trattamento necessario per **esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

LICEITÀ DEL TRATTAMENTO
CATEGORIE PARTICOLARI DI DATI PERSONALI (ART. 9)

È vietato *trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a. ***l'interessato ha prestato il proprio consenso esplicito*** *al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;*

LICEITÀ DEL TRATTAMENTO
CATEGORIE PARTICOLARI DI DATI PERSONALI (ART. 9)

b. *il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato […];*

e. ***il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato*** *[…];*

h. *il trattamento è necessario per finalità di* ***medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale*** *ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità,* ***fatte salve le condizioni e le garanzie di cui al paragrafo 3*** *[…]*

ESECUZIONE DI UN CONTRATTO

Qualora il trattamento dei dati sia necessario per la conclusione di un contratto, lo stesso risulta lecito e non è necessario richiedere il consenso dell'interessato

CONSENSO

L'interessato deve aver rilasciato il proprio **consenso** per il trattamento dei propri dati con riferimento a una specifica finalità. Tale consenso deve essere:

- Libero: fornito in assenza di condizionamenti
- Specifico: deve riferirsi esclusivamente ad un singolo trattamento
- Informato: l'interessato deve conoscere le implicazioni e le caratteristiche del trattamento
- Inequivocabile: non devono sussistere dubbi circa le intenzioni dell'Interessato

LEGITTIMO INTERESSE

Il **legittimo interesse** del titolare deve prevalere sugli interessi dell'interessato. Deve essere effettuata una valutazione e un bilanciamento dei diversi interessi e deve evidentemente risultare prevalente quello del titolare.

ESEMPIO

Nel caso di acquisto di un prodotto, i dati forniti dal cliente per il pagamento e l'invio/attivazione del prodotto si fondano appunto sulla conclusione del contratto e sono funzionali alla conclusione dello stesso, quindi:

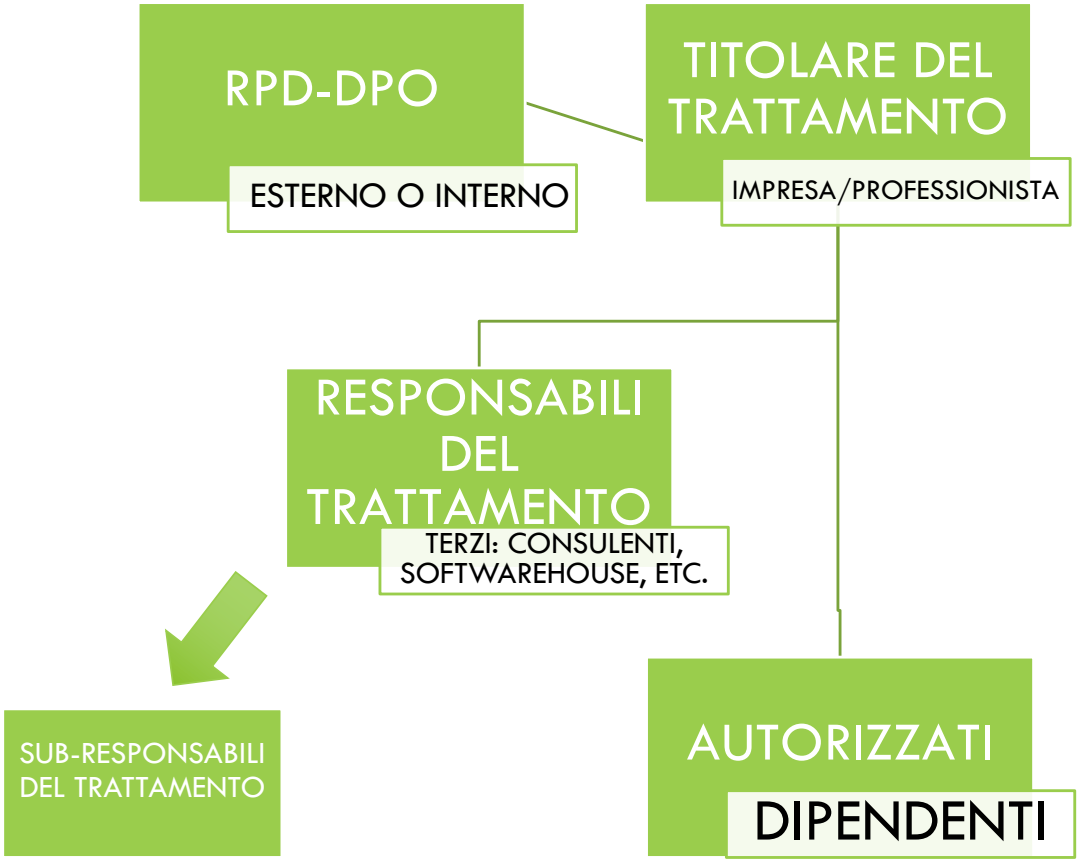
- tutti i dati potranno sempre essere utilizzati dal titolare del trattamento per quelle specifiche finalità;
- un indirizzo di consegna potrà essere sempre utilizzato per la consegna del prodotto;

ESEMPIO

- un indirizzo di consegna non potrà mai essere utilizzato per invio di materiale pubblicitario senza il consenso dell'interessato;
- un indirizzo email non potrà mai essere utilizzato per l'invio di newsletter senza il consenso dell'interessato.

NUOVI RUOLI DEI SOGGETTI COINVOLTI NEL TRATTAMENTO

ORGANIGRAMMA PRIVACY



I SOGGETTI COINVOLTI

- L'INTERESSATO
- IL TITOLARE DEL TRATTAMENTO
- IL CONTITOLARE
- IL RESPONSABILE DEL TRATTAMENTO
- IL SOGGETTO AUTORIZZATO
- IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

L'INTERESSATO

L'interessato è la persona fisica **indentificata** o **identificabile**.

- Non c'è una definizione nel Regolamento, ma la si desume da quella di dato personale: ovvero qualsiasi informazione riguardante una persona fisica.
- La qualità d'interessato cessa con la sua morte, ossia con il venir meno della persona fisica.
- La morte del soggetto non fa venir meno il legittimo interessi di altri, ad esempio agli eredi, ad aver accesso a informazioni del deceduto e dunque a far valere disposizioni regolamentari relative a dati riferibili a quest'ultimo.

IL TITOLARE DEL TRATTAMENTO

ART. 4 «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

IL TITOLARE DEL TRATTAMENTO

Finalità: perché del trattamento?

Obiettivo al servizio del quale viene effettuato il trattamento (es: il trattamento per finalità di marketing, è funzionale allo svolgimento dell'attività di promozione)

Mezzi: come avviene il trattamento?

Non si riferisci solo ai mezzi tecnici (es. hardware, software), ma anche quali sono i dati, come e quando raccoglierli, quali terzi avranno accesso ai dati, ecc. (profilo organizzativo)

È una figura apicale nella gerarchia della privacy.

TITOLARE DEL TRATTAMENTO - Poteri

Individua all'interno della propria struttura ruoli subordinati (personale dipendente o collaboratori) a cui affidare operazioni di trattamento, istruendoli adeguatamente.

Esternalizza attività di trattamento nominando responsabili di trattamento e istruendoli adeguatamente.

Autorizza i responsabili a designare altri responsabili.

TITOLARE DEL TRATTAMENTO - Obblighi

- Stabilire, programmare e attuare e aggiornare misure di sicurezza adeguate
- Adottare tecniche di privacy by design e by default
- Procedere alla valutazione d'impatto e alla consultazione preventiva
- Facoltativamente, dotarsi di policy interne, adottare codici di condotta e munirsi di certificazioni
- Attenersi ai doveri di correttezza per l'intera durata del trattamento

TITOLARE DEL TRATTAMENTO - Obblighi

- Conformarsi ai principi di trasparenza e responsabilizzazione
- Scegliere e formare i soggetti che ricoprono i ruoli subalterni
- Designare il DPO nei casi previsti dalla legge
- Applicare contromisure effettive e tempestive e procedere alla notificazione al Garante e alla comunicazione all'interessato

TITOLARE DEL TRATTAMENTO - Obblighi

❖**Nei confronti dell'interessato:**

A seconda che la raccolta dei dati sia diretta presso l'interessato o indiretta o per finalità ulteriori, il titolare fornisce a quest'ultimo la relativa informativa. Successivamente si dota di idonea organizzazione per riscontrare tempestivamente le istanze dell'interessato e per permettere l'esercizio dei diritti riconosciuti.

❖**Nei confronti dei soggetti preposti al controllo:**

- coopera con l'Autorità garante
- coopera con gli organismi indipendenti di certificazione
- coopera con DPO fornendolo dei mezzi, delle informazioni e degli accessi necessari a realizzare la sua attività, pur senza interferire con istruzioni nello svolgimento dei suoi compiti.

IL RESPONSABILE DEL TRATTAMENTO

ART. 4 «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento** […]

IL RESPONSABILE DEL TRATTAMENTO

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento **che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

IL RESPONSABILE DEL TRATTAMENTO

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto, o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che **vincoli** il responsabile del trattamento al titolare del trattamento e che **definisca:**

- la materia disciplinata
- la durata del trattamento
- la natura e la finalità del trattamento
- il tipo di dati personali e le categorie di interessati
- gli obblighi e i diritti del titolare del trattamento.

IL RESPONSABILE DEL TRATTAMENTO

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

- tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste ai sensi dell'articolo 32 (es. cifratura, pseudonimizzazione, recupero da back up);
- rispetti le condizioni previste per ricorrere a un altro responsabile del trattamento (sub-responsabile)

IL RESPONSABILE DEL TRATTAMENTO

- tenendo conto della natura del trattamento, **assiste il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato**; su scelta del titolare del trattamento;

- **cancella o restituisce al Titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancella le copie esistenti**, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

- **mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi** e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato […].

IL (SUB)RESPONSABILE DEL TRATTAMENTO

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento**, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.

IL (SUB)RESPONSABILE DEL TRATTAMENTO

Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, **il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile**.

IL (SUB)RESPONSABILE DEL TRATTAMENTO

- Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
- Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

IL SOGGETTO AUTORIZZATO

Pur non prevedendo espressamente la figura dell'«incaricato» del trattamento, il regolamento non ne esclude la presenza in quanto fa riferimento a «*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*» (cfr. artt. 4, n. 10), e 29).

Il soggetto autorizzato (ex "*incaricato*") è una figura di primissima rilevanza nell'organigramma di privacy di qualsiasi struttura poiché è colui il quale, sotto la diretta autorità del titolare e del responsabile (se nominato), dietro apposita autorizzazione, effettua materialmente le operazioni di trattamento sui dati personali.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

costituisce un punto di riferimento interno alle aziende e degli enti, in quanto è coinvolto in tutte le questioni attinenti alla privacy

è un punto di contatto per gli interessati, le divisioni operative interne di aziende o enti, le autorità di controllo

l'identità e i dati di contatto del DPO devono essere riportati nell'informativa privacy, nel registro dei trattamenti e devono essere pubblicati sul sito internet dell'ente

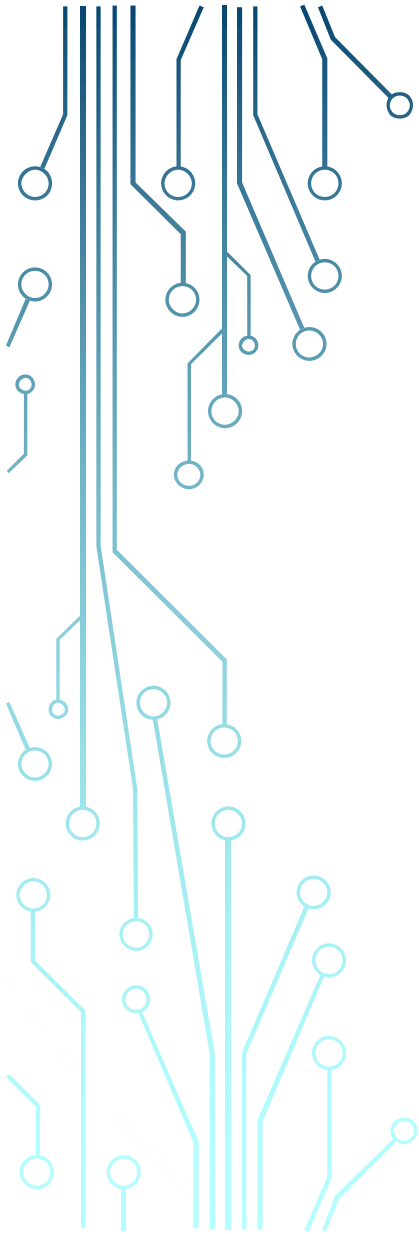
IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie

Soggetti tenuti a designare un DPO

tutti i soggetti la cui **attività principale** consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**

tutti i soggetti la cui attività principale consiste nel trattamento, su **larga scala**, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici



DATA BREACH

DATA BREACH

Violazione di sicurezza che comporta accidentalmente o in modo illecito:

la **distruzione**	la **perdita**	la **modifica**	la **divulgazione non autorizzata**	l'**accesso**

ai dati personali trasmessi, conservati o comunque trattati

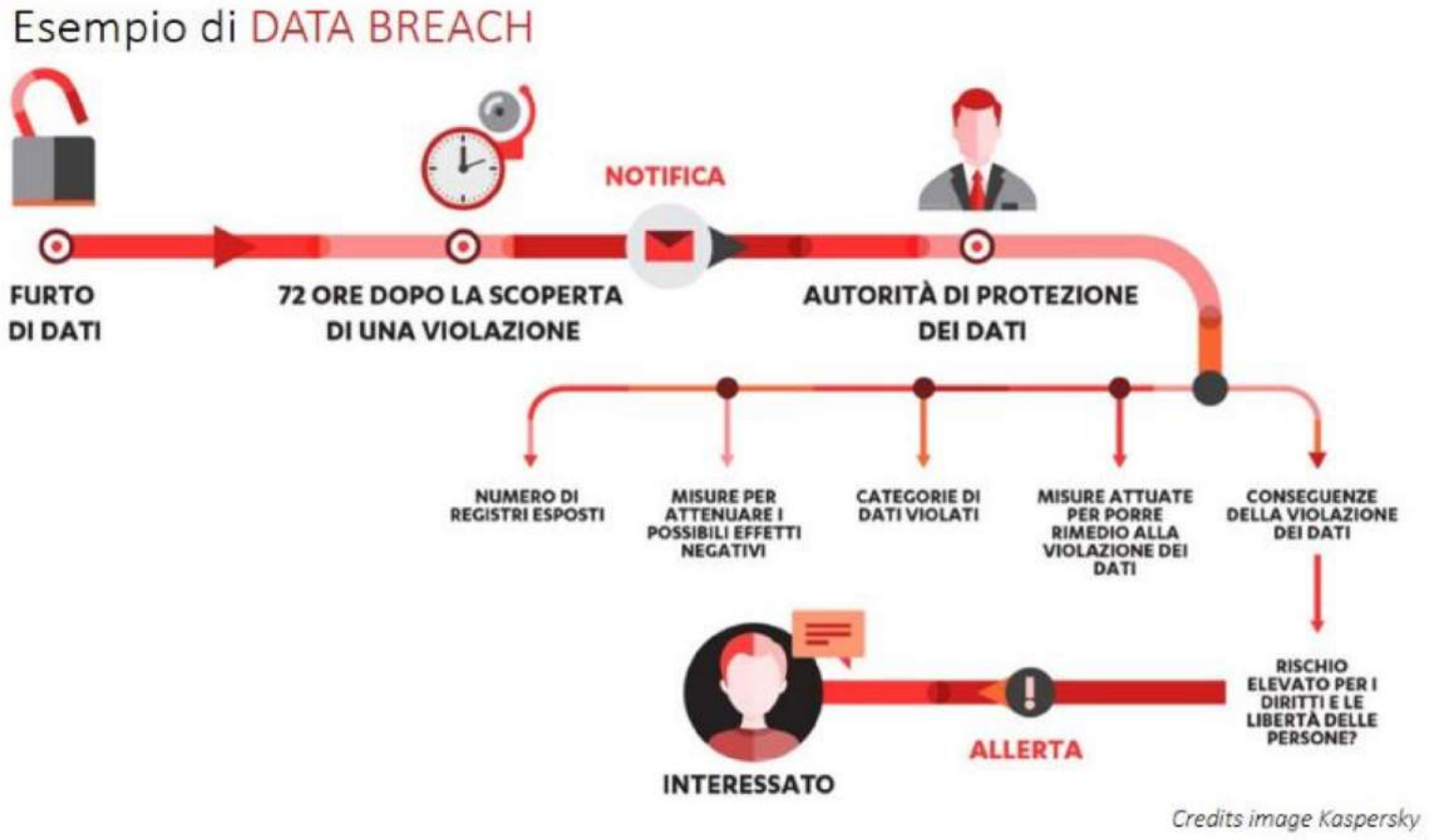
DATA BREACH

Il GDPR disciplina il "Data Breach" prevedendo un obbligo di notifica e comunicazione in capo al Titolare, in presenza di **violazioni di dati personali** che possono compromettere le libertà e i diritti dei soggetti interessati.

Esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

PROCEDURA


Esempio di DATA BREACH
NOTIFICA
FURTO DI DATI
72 ORE DOPO LA SCOPERTA DI UNA VIOLAZIONE
AUTORITÀ DI PROTEZIONE DEI DATI
NUMERO DI REGISTRI ESPOSTI
MISURE PER ATTENUARE I POSSIBILI EFFETTI NEGATIVI
CATEGORIE DI DATI VIOLATI
MISURE ATTUATE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI
CONSEGUENZE DELLA VIOLAZIONE DEI DATI
RISCHIO ELEVATO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE?
ALLERTA
INTERESSATO
Credits image Kaspersky

OBBLIGHI IN CONCRETO

ATTIVITÀ IN CONCRETO

- verifica preliminare delle attività e della legittimità dei trattamenti
- redazione documenti informativi ex artt. 13-14 GDPR
- raccolta dei consensi (ove necessario)
- aggiornamento della modulistica interna
- disciplina dei rapporti con i soggetti coinvolti nel trattamento (interni ed esterni)

ATTIVITÀ IN CONCRETO

- adozione di *privacy policy*
- adozione di una procedura in caso di *data breach*
- compilazione del registro delle attività di trattamento
- istruzioni e formazione del personale
- individuazione e adozione delle misure di sicurezza adeguate

SICUREZZA E PROTEZIONE DEI DATI NEGLI STUDI

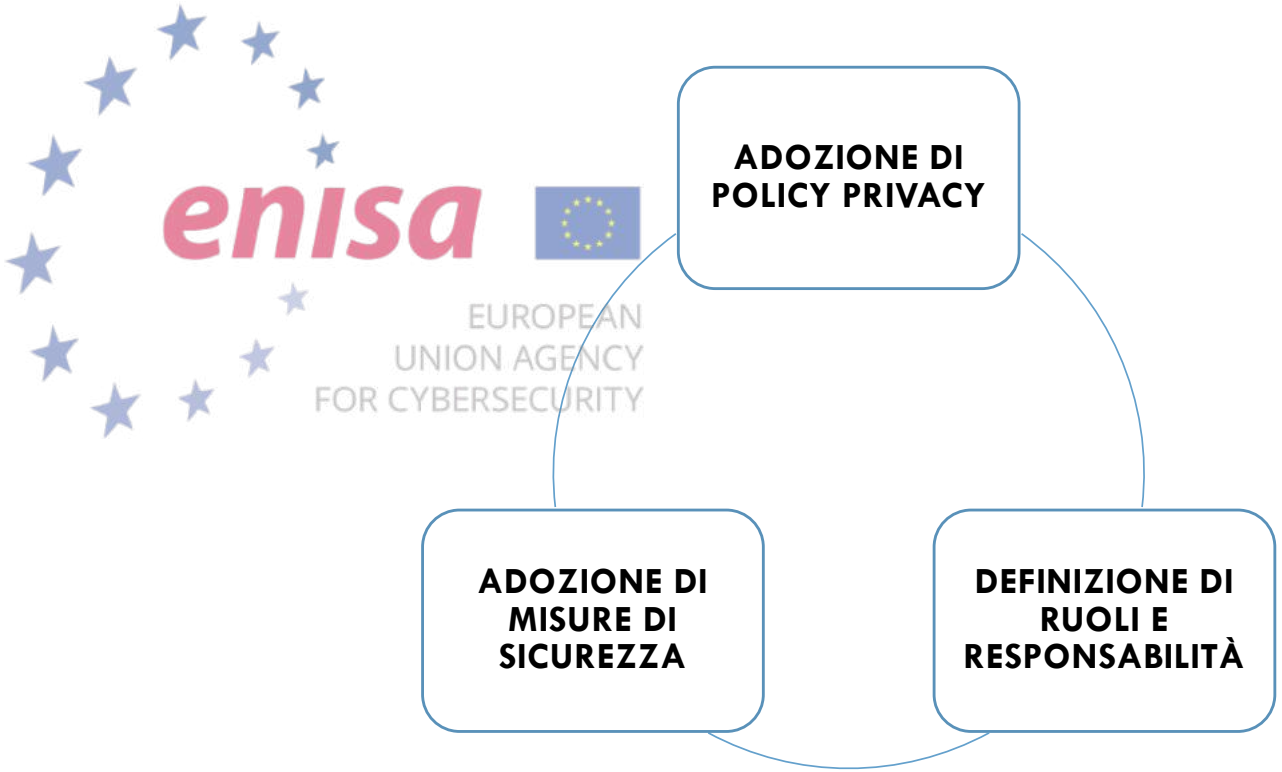
SICUREZZA E PROTEZIONE DEI DATI NEGLI STUDI

Ai sensi del Regolamento EU 2016/679, uno degli obblighi fondamentali per tutte le imprese, compresi i Professionisti, che agiscono in qualità di Titolari o di Responsabili del trattamento, è quello della sicurezza nel trattamento dei dati personali.

SICUREZZA E PROTEZIONE DEI DATI NEGLI STUDI

La sicurezza è una tematica che include la riservatezza, integrità e disponibilità dei dati e deve essere considerata seguendo un approccio basato sul rischio: più alto è il rischio e più rigorose devono essere le misure per gestirlo.

LE MISURE DI SICUREZZA



SICUREZZA E PROTEZIONE DEI DATI

VERIFICA PRELIMINARE DELLE ATTIVITÀ

1) ADOZIONE DI PRIVACY POLICY

2) DEFINIZIONE DI RUOLI E RESPONSABILITÀ

3) MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
FOCUS: LE PROCEDURE DI SICUREZZA INFORMATICA

VERIFICA PRELIMINARE DELLE ATTIVITÀ

IL RUOLO DEL PROFESSIONISTA

- **Titolare del trattamento:** persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

- **Responsabile del trattamento:** persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

IL RUOLO DEL PROFESSIONISTA

- Titolare del trattamento
- Responsabile esterno

Per entrambi i ruoli, quali **compiti** e quali **responsabilità**?

IL RUOLO DEL COMMERCIALISTA

IL COMMERCIALISTA	
TITOLARE	**RESPONSABILE**
Tratta i dati dei propri clienti (persone fisiche) o dei propri dipendenti nella sua qualità di professionista	Tratta dati per conto del Cliente (es. i dati relativi alla contabilità)

IL RUOLO DEL COMMERCIALISTA

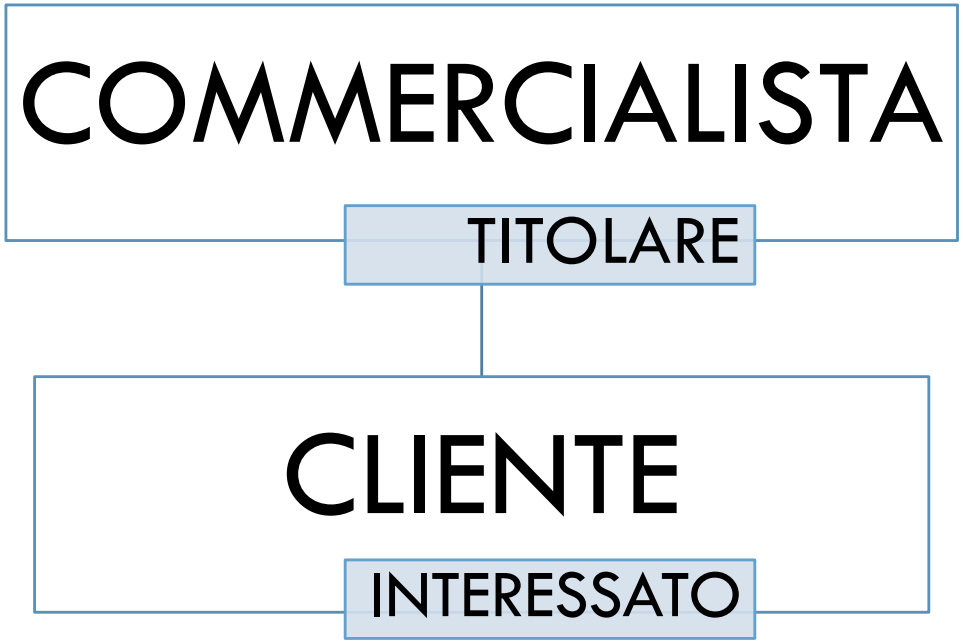
Nel primo caso agisce in piena autonomia e indipendenza per il perseguimento di scopi attinenti alla gestione della propria attività.

Per tali ragioni, egli ricopre il ruolo di **titolare del trattamento**: non effettua un'attività meramente esecutiva di trattamento, "per conto" del cliente, bensì esercita un potere decisionale del tutto autonomo sulle finalità e i mezzi del trattamento.

IL RUOLO DEL COMMERCIALISTA

Il commercialista è Titolare per tutte quelle attività svolte direttamente a favore della persona che richiede la prestazione, fornendo servizi come ad esempio la predisposizione dichiarazioni fiscali ed altri adempimenti alla persona fisica (elaborazione ed invio telematico 730, addebito F24/F23; elaborazione ed invio telematico modello IMU; elaborazione modello ISEE; richiesta rateazione di avvisi bonari e cartelle Agenzia della Riscossione; registrazione contratti d'affitto, etc).

IL RUOLO DEL COMMERCIALISTA



IL RUOLO DEL COMMERCIALISTA

COMMERCIALISTA
TITOLARE

- Fornire la cd. *Informativa* agli interessati ex art. 13 GDPR
- Nominare soggetti autorizzati
- Nominare responsabili ex art. 28 GDPR

IL RUOLO DEL COMMERCIALISTA

Nel secondo caso il Commercialista svolge attività delegate dal titolare.

Si pensi ad un audit specifico, attività di data entry o elaborazione dati e controllo contabile che non richiedono delle decisioni del professionista (es. operazioni di tenuta della contabilità oppure l'elaborazione dei cedolini paga dei dipendenti del cliente).

IL RUOLO DEL COMMERCIALISTA

Per tale ragioni, nella seconda ipotesi, il Commercialista ricopre il ruolo di **responsabile del trattamento**: viene delimitato l'ambito delle rispettive attribuzioni e gli sono fornite specifiche istruzioni sui trattamenti da effettuare.

IL RUOLO DEL COMMERCIALISTA

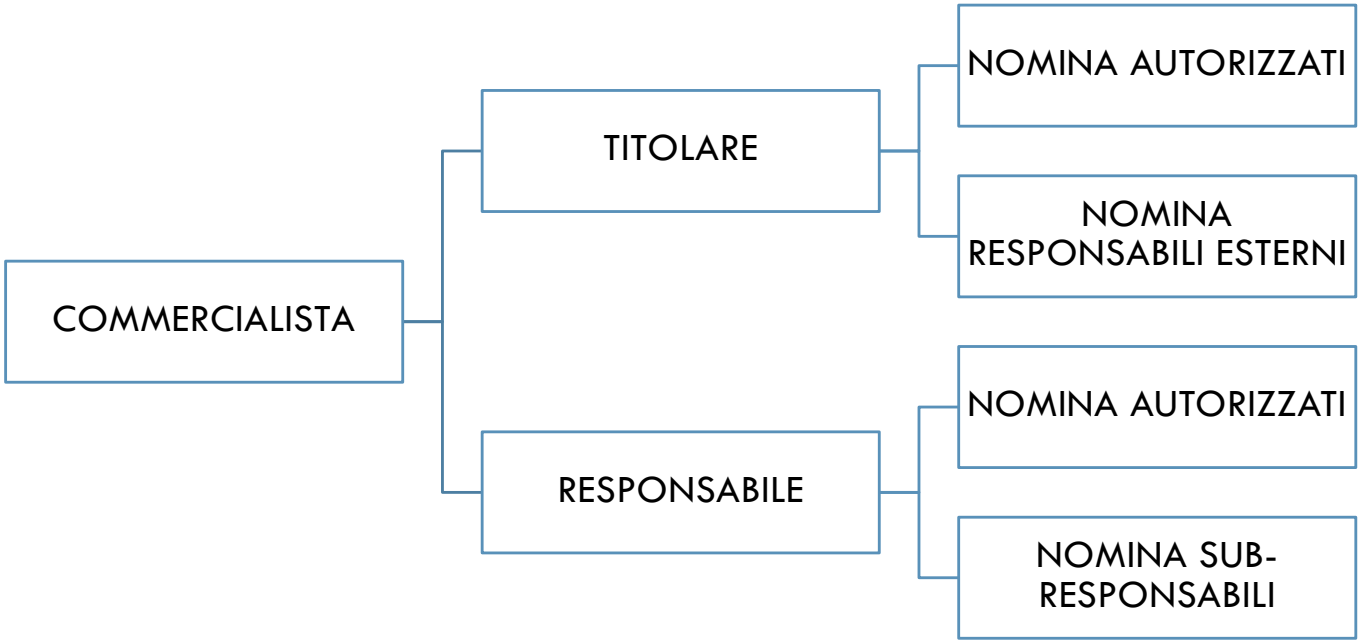
IL RUOLO DEL COMMERCIALISTA

RESPONSABILE

- Aderire alle istruzioni impartite dal Cliente/Titolare
- Nominare soggetti autorizzati
- Nominare sub-responsabili ex art. 28 GDPR

DEFINIRE I RUOLI E LE RESPONSABILITÀ

I SOGGETTI COINVOLTI NEL TRATTAMENTO



I SOGGETTI COINVOLTI NEL TRATTAMENTO

Articolo 28 GDPR - Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

I SOGGETTI COINVOLTI NEL TRATTAMENTO

Articolo 28 GDPR - Responsabile del trattamento

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

I SOGGETTI COINVOLTI NEL TRATTAMENTO

I collaboratori esterni (non dipendenti) potranno assumere in concreto il ruolo di sub-responsabili, qualora sia demandata "l'esecuzione di specifiche attività di trattamento per conto del titolare" (art. 28, par. 4 del Regolamento).

I SOGGETTI COINVOLTI NEL TRATTAMENTO

Articolo 29 GDPR - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

I SOGGETTI COINVOLTI NEL TRATTAMENTO

Qualora il professionista si avvalga normalmente di collaboratori di propria fiducia questi, in base alle concrete operazioni di trattamento affidate, potranno operare sotto la sua diretta autorità e in base alle istruzioni impartite, configurando il rapporto preso in considerazione dall'art. 29 del Regolamento.

ADOZIONE DI PRIVACY E DATA BREACH POLICY

ADOZIONE DI PRIVACY POLICY

Articolo 25 GDPR - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

Il titolare del trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate.

ADOZIONE DI PRIVACY POLICY

Tali misure devono essere mirate a:

- attuare in modo efficace i principi di protezione dei dati;
- integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.

ADOZIONE DI PRIVACY POLICY

ATTENZIONE!

L'articolo 25 non richiede l'attuazione di misure tecniche e organizzative *specifiche* e *univoche* per tutti, bensì connesse all'attuazione dei principi di protezione dei dati nello specifico trattamento.

ADOZIONE DI PRIVACY POLICY

Il titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR.

ADOZIONE DI PRIVACY POLICY

Dimostrare la conformità …come?

Al fine di poter dimostrare la conformità con il Regolamento, il titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita *(cfr. considerando 74 e 78 del GDPR)*.

ADOZIONE DI PRIVACY POLICY

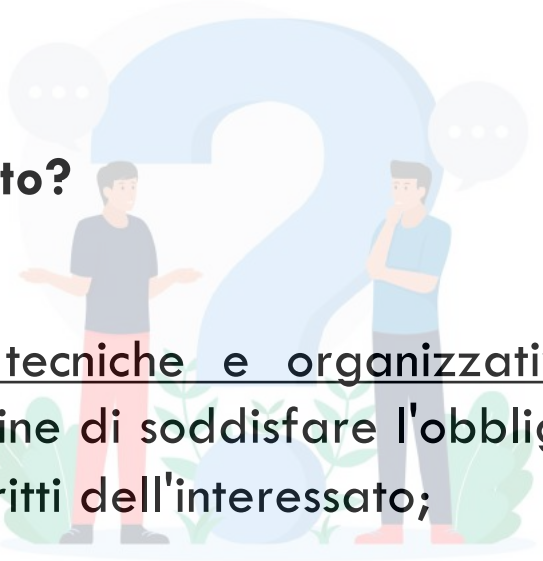
I principi della protezione dei dati by design e by default

- Garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
- Attuare misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

ADOZIONE DI PRIVACY POLICY

Per quanto riguarda il Responsabile del trattamento?

Articolo 28 GDPR - Responsabile del trattamento



- Assiste il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- Assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

LE MISURE DI SICUREZZA

Articolo 32 GDPR - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, *tra le altre*, *se del caso*:

LE MISURE DI SICUREZZA

Articolo 32 GDPR - Sicurezza del trattamento

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

LE MISURE DI SICUREZZA

Articolo 32 GDPR - Sicurezza del trattamento

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

LE MISURE DI SICUREZZA

Alcune osservazioni:

- le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, par. 1 GDPR).
- la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Non possono sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza!

LE MISURE DI SICUREZZA

Il titolare del trattamento e il responsabile del trattamento devono adottare misure tecniche e organizzative tenendo conto:

- dello stato dell'arte e dei costi di attuazione;
- della natura, dell'oggetto, del contesto e delle finalità del trattamento;
- del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

LE MISURE DI SICUREZZA

Tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.

LE MISURE DI SICUREZZA

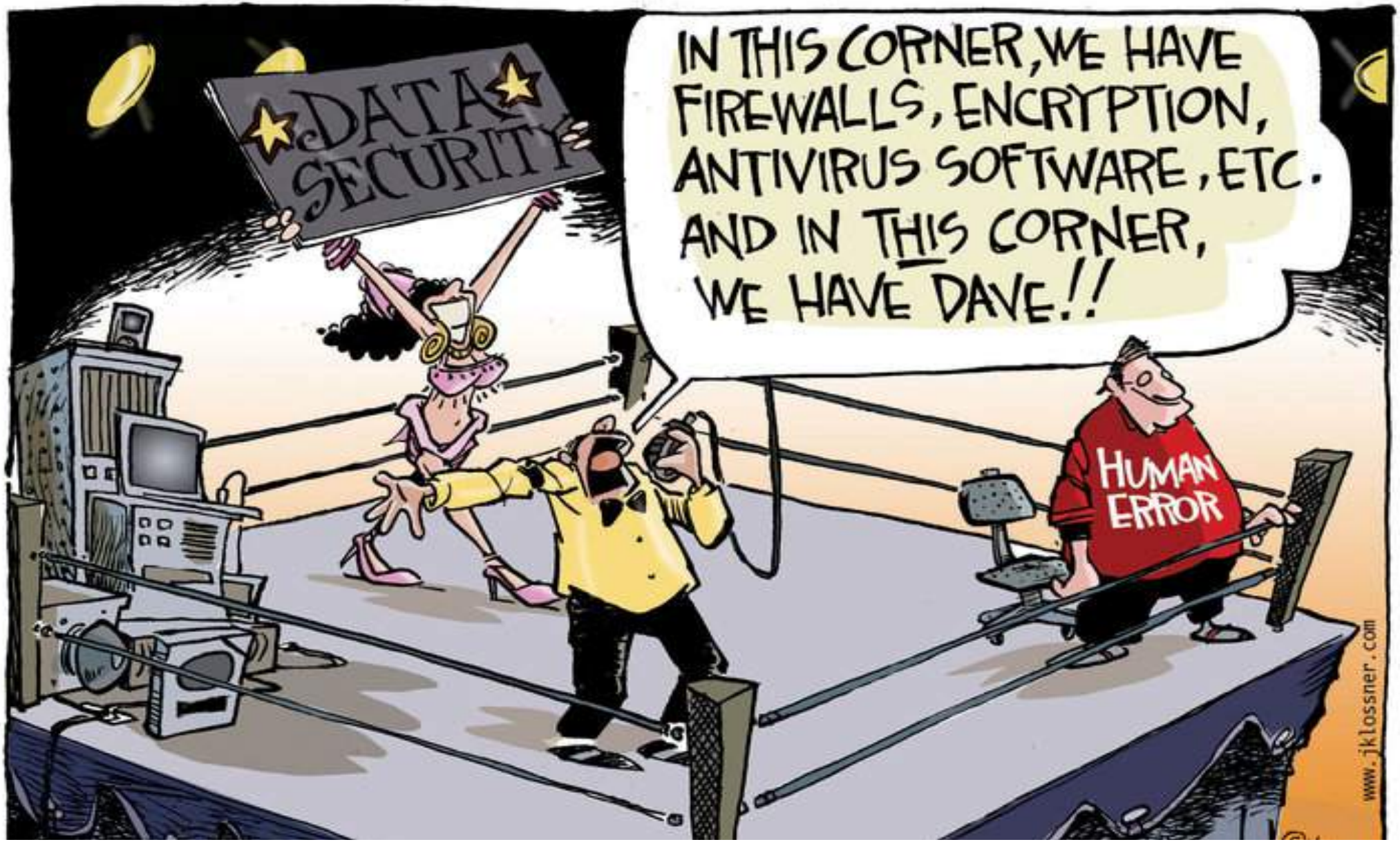
…e per il Responsabile?

Il regolamento attribuisce direttamente al responsabile del trattamento compiti specifici in ordine alla individuazione e predisposizione delle idonee misure di sicurezza adeguate al rischio, attraverso misure tecniche ed organizzative (v. art. 32 del Regolamento).

LE MISURE DI SICUREZZA

Al Professionista che operi (anche) in qualità di responsabile del trattamento è dunque attribuito un apprezzabile margine di autonomia (e correlativa responsabilità) nella individuazione dei sistemi e delle misure idonee a garantire la sicurezza dei dati gestiti nei propri archivi.

FOCUS:
LE MINACCE INFORMATICHE



2022 Cyberthreat Defense Report

CYBEREDGE GROUP

SURVEY DEMOGRAPHICS

17 Countries represented around the world

19 Industries represented

1,200 Qualified IT security decision makers & practitioners

UNRELENTING PRESSURE ON SECURITY TEAMS

A near-record 85% of organizations experienced at least one successful cyberattack in the past year, and an unprecedented 41% suffered six or more attacks.

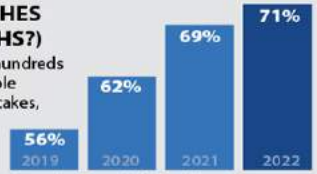
COMPROMISED ORGANIZATIONS BY COUNTRY

The percentage of organizations that were victimized by at least one successful attack.

Colombia	93.9%
Turkey	93.7%
Spain	91.8%
Mexico	90.6%
Canada	89.8%
France	89.3%
Brazil	88.2%
Saudia Arabia	87.8%
Japan	87.2%
USA	86.8%
China	86.0%
Italy	85.7%
South Africa	84.0%
Singapore	82.0%
UK	81.4%
Germany	72.6%
Australia	62.5%

RANSOMWARE REACHES NEW HEIGHTS (DEPTHS?)

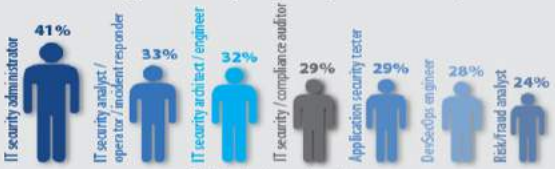
High-visibility cases affected hundreds of thousands of people, "double extortion" attacks raised the stakes, and the percentage of organizations affected by ransomware reached a new peak.



Organizations victimized by ransomware

SECURITY SKILLS IN DEMAND

Eighty-four percent of organizations are experiencing a shortfall of skilled IT security personnel. Openings are spread across many roles.



Skills shortage, by role

SECURITY BUDGETS KEEP GROWING

Survey respondents expect their organization's IT security budget to grow 4.6% in 2022, consistent with previous years. Security accounts for 12.7% of total IT budgets.

Mean annual increase in IT security budgets

MSSPs ARE IN STYLE

Ninety-three percent of organizations rely on a managed security service provider (MSSP) to monitor or manage at least one security function.

Organizations working with an MSSP

Organizations using an MSSP to monitor/manage

SIEM platforms	41%
Detection and response	41%
Web application firewalls	39%
Intrusion detection systems	38%

TOP STRESSORS

The cyberthreats causing the greatest concern:

1. Malware
2. Account takeover / credential abuse attacks
3. Ransomware
4. Phishing / spear-phishing attacks

SECURITY'S BIGGEST OBSTACLES

These obstacles prevent IT from stopping attacks:

1. Lack of skilled personnel
2. Low security awareness among employees
3. Poor integration between security solutions
4. Lack of management support/awareness

PROTECTING WORK FROM HOME

Technologies used most often to enable employees to work from home securely:

1. Endpoint security software
2. Virtual private networks (VPNs)
3. SD-WANs
4. Network access control (NAC)

HOTTEST SECURITY TECH FOR 2022

The security solutions with the highest "plan for acquisition" rating in each of our five technology categories:

CATEGORY	#1 SOLUTION
Network security	Next-generation firewall (NGFW)
Endpoint security	Deception technology/honeypot
Application & data security	Bot management
Security managment & operations	Advanced security analytics
Identity & access management	Biometrics

MISURE DI SICUREZZA
LE PRINCIPALI MINACCE

- **RANSOMWARE**
- **PHISHING**

LE MISURE DI SICUREZZA

Il **RANSOMWARE** è un programma informatico dannoso ("malevolo") che può “infettare” un PC, tablet, smartphone, smart TV, ecc., bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, “*ransom*”) da pagare per “liberarli”.

LE MISURE DI SICUREZZA

Ci sono due tipi principali di ransomware:

- i **cryptor** (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);
- i **blocker** (che bloccano l'accesso al dispositivo infettato).

Lo scopo è (quasi) sempre il profitto: si richiede un riscatto per riavere i propri dati

LE MISURE DI SICUREZZA

La prima e più importante forma di difesa è la prudenza. Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune accortezze:

- non aprire mai allegati con estensioni "strane" (ad esempio, allegati con estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);

LE MISURE DI SICUREZZA

- scaricare preferibilmente app e programmi da market ufficiali, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;
- se si usa un pc, si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).

ATTENZIONE AL RANSOMWARE

Il programma che prende «in ostaggio» PC e smartphone

1. COS'E' IL RANSOMWARE?

Il **ransomware** è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone, smart TV), **bloccando l'accesso ai contenuti** (foto, video, file) e **chiedendo un riscatto** *(in inglese, ransom)* per «liberarli». La **richiesta di pagamento** con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato. L'utente ha pochi giorni per pagare: **poi il blocco diventa definitivo**. Ci sono **due tipi principali di ransomware**: i **cryptor** (che criptano i file contenuti nel dispositivo rendendoli illeggibili) e i **blocker** (che bloccano l'accesso al dispositivo infettato).

2. COME SI DIFFONDE?

Il ransomware si diffonde soprattutto attraverso **messaggi** - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da **soggetti conosciuti e sicuri** come corrieri espressi, gestori di servizi *(acqua, luce, gas)*, operatori telefonici, soggetti istituzionali, ecc.. Chi li riceve è indotto ingannevolmente ad **aprire allegati** o a **cliccare link o banner** collegati a software dannosi. Il dispositivo infettato può poi «contagiarne» altri, perché il ransomware, impossessandosi della **rubrica dei contatti,** può utilizzarla per **spedire automaticamente messaggi contenenti file dannosi**.

3. COME DIFENDERSI?

La prima difesa è **evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti** *(ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.)* e **non cliccare su collegamenti a siti sospetti**.
E' utile installare un **antivirus** con estensioni per malware sui propri dispositivi e **mantenere aggiornato il sistema operativo**.
E' fondamentale effettuare **backup periodici dei contenuti:** così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, **i dati in esso contenuti non verranno persi**.

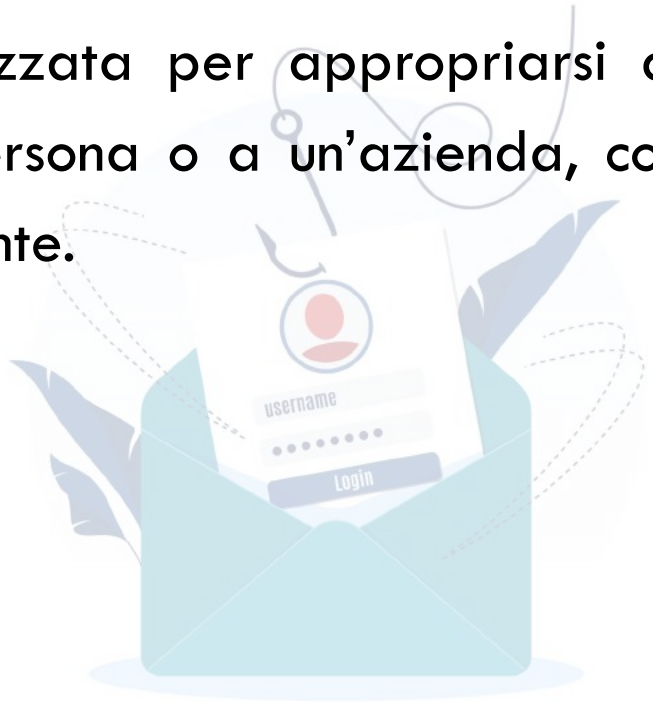
4. COME LIBERARSI DAL RANSOMWARE?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di **non ricevere i codici di sblocco**, o addirittura di finire in **liste di «pagatori»** potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di **rivolgersi a tecnici specializzati** capaci di sbloccare il dispositivo. Oppure si può **formattare il dispositivo**, ma con il rischio di perdere tutti i dati in esso contenuti se **non è disponibile un backup**.
E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia postale, anche per aiutare a prevenire ulteriori truffe.

La scheda ha mere finalità divulgative

LE MISURE DI SICUREZZA

Il **PHISHING** è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda, con l'intento di compiere operazioni fraudolente.



LE MISURE DI SICUREZZA

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media.

Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici

LE MISURE DI SICUREZZA

Come proteggersi? Il buonsenso prima di tutto!

- Dati, codici di accesso e password personali non dovrebbero mai essere comunicati.
- Banche, enti pubblici e aziende non richiedono informazioni personali attraverso e- mail, sms, social media o chat.

LE MISURE DI SICUREZZA

- I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti.
- Capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.
- E' utile anche prestare attenzione al mittente o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).

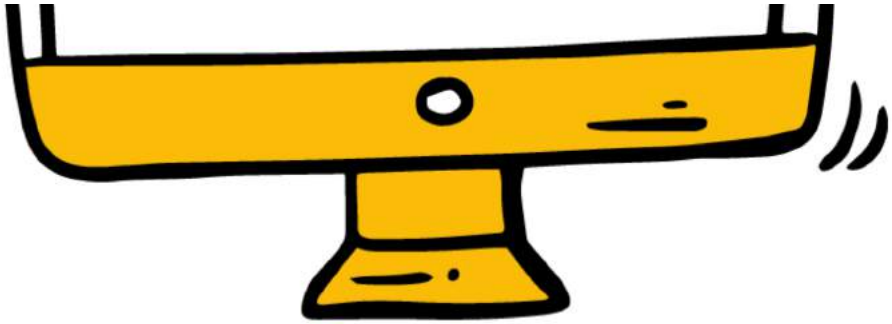
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

IL PHISHING: Attenzione ai «pescatori» di dati personali

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

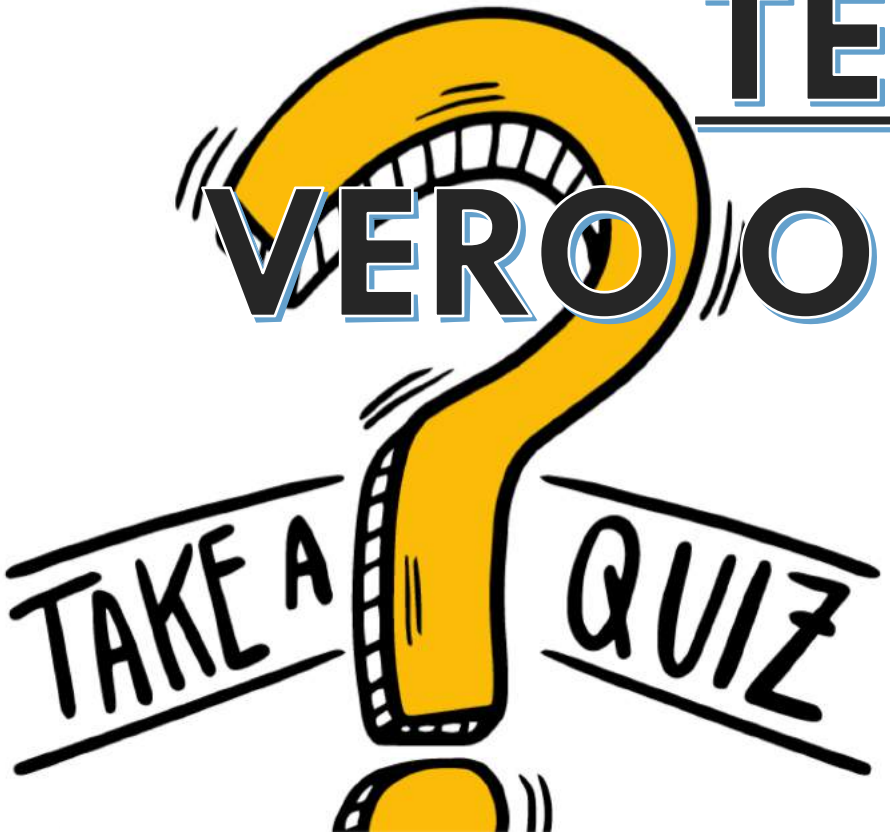
La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

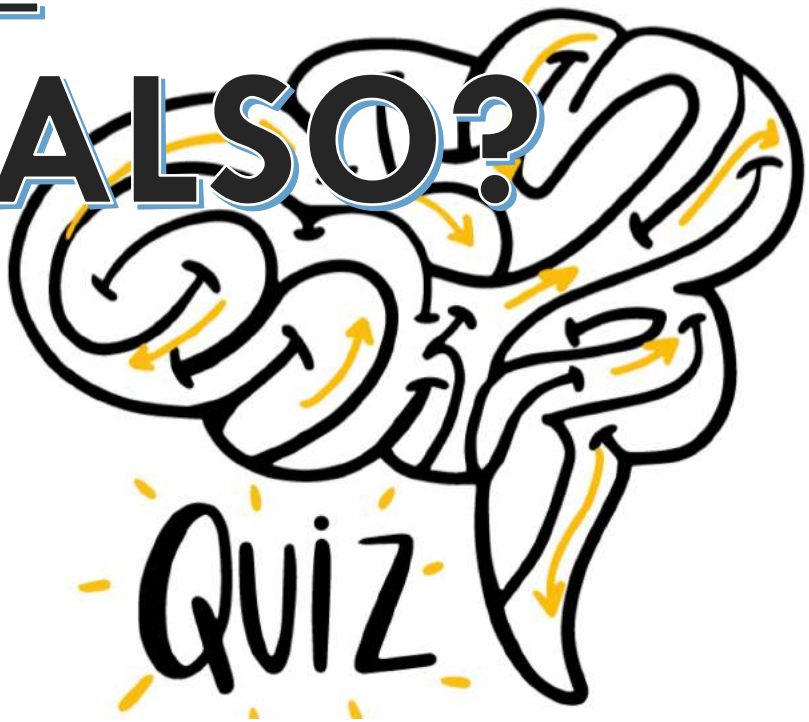
In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un *form* da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.



TEST

VERO O FALSO?





LE MISURE DI SICUREZZA

LE MISURE DI SICUREZZA

M **Messaggio fax NoReply [amministratore]** <noreply@efacks.com>
a me

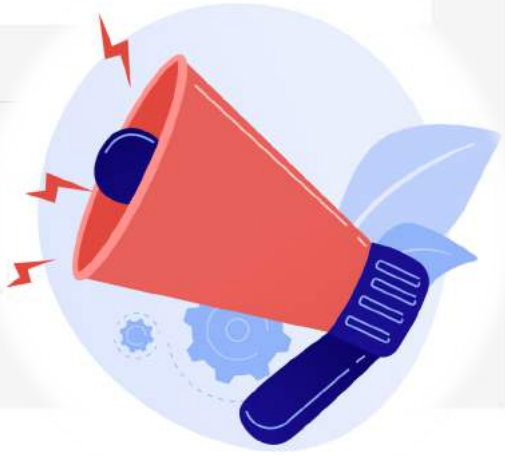
11:53

Il giorno 08/05/22, 11:53 hai ricevuto un fax di 1 pagina
Fai clic qui per visualizzare questo fax online

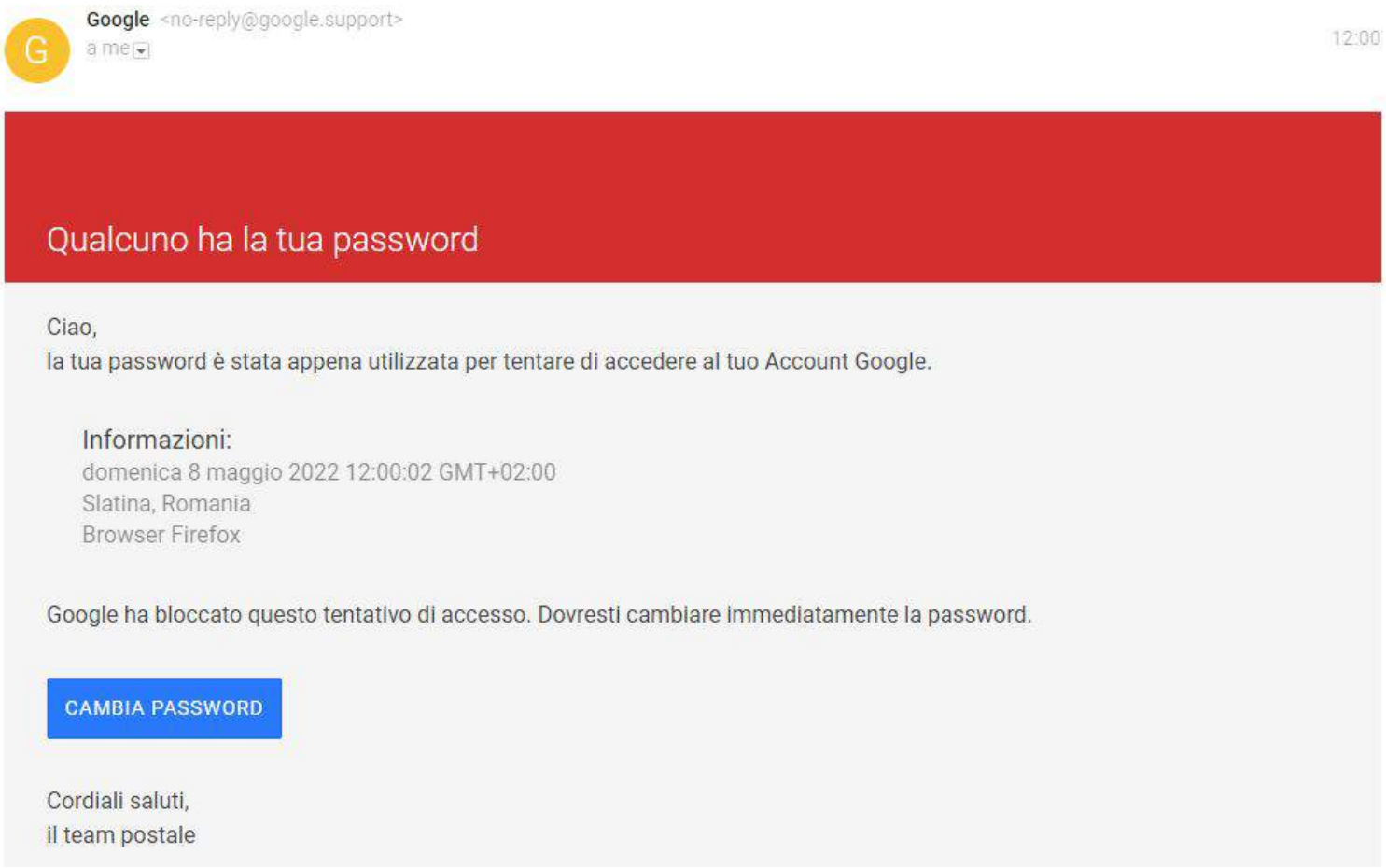
eFax

Grazie per aver utilizzato il servizio eFax! Visita il sito www.eFax.com/en/efax/page/help se hai domande o credi di a

eFax Inc (c) 2022



LE MISURE DI SICUREZZA



Google <no-reply@google.support>
a me

12:00

Qualcuno ha la tua password

Ciao,
la tua password è stata appena utilizzata per tentare di accedere al tuo Account Google.

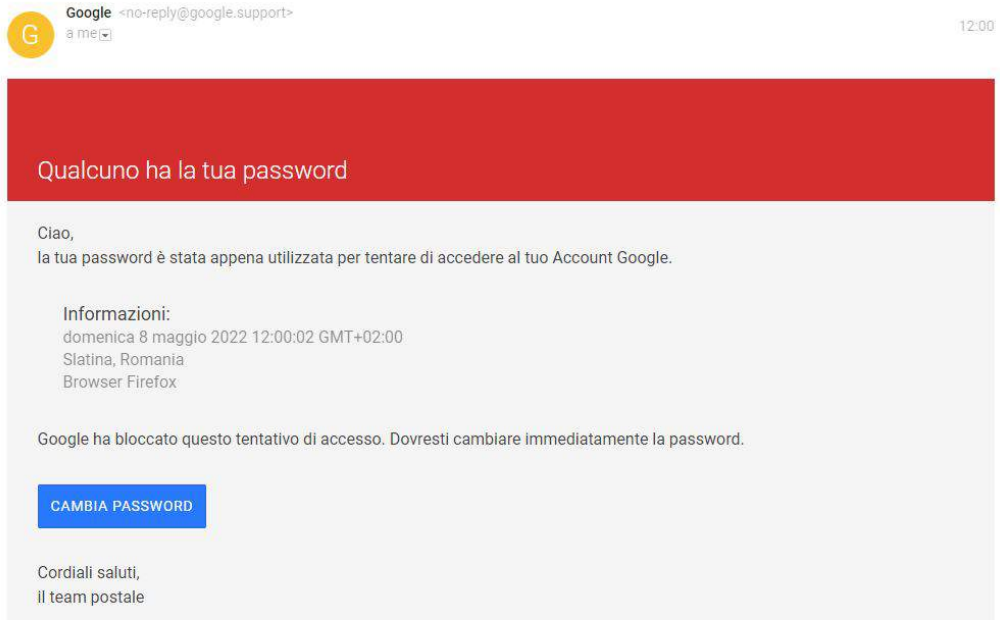
Informazioni:
domenica 8 maggio 2022 12:00:02 GMT+02:00
Slatina, Romania
Browser Firefox

Google ha bloccato questo tentativo di accesso. Dovresti cambiare immediatamente la password.

CAMBIA PASSWORD

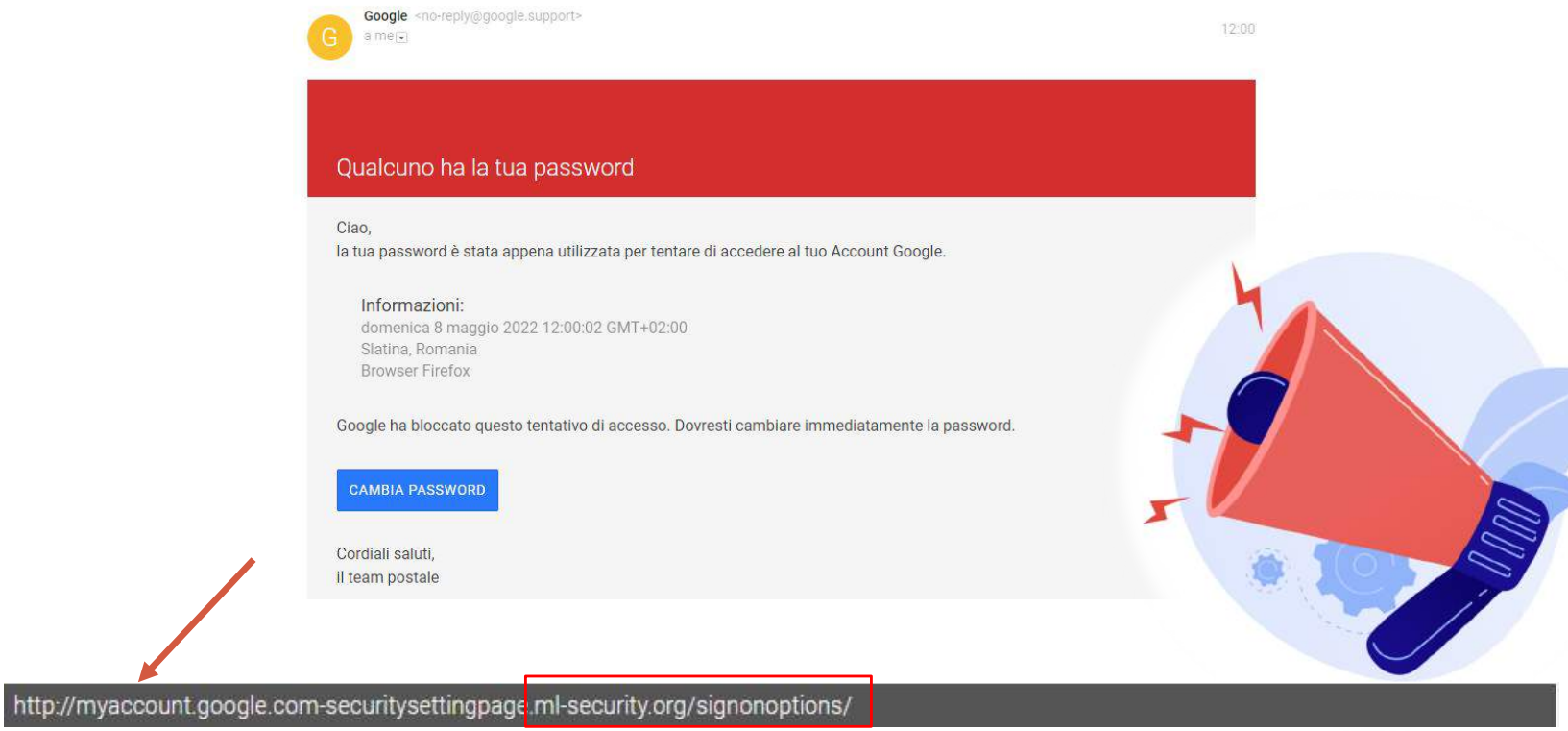
Cordiali saluti,
il team postale

LE MISURE DI SICUREZZA

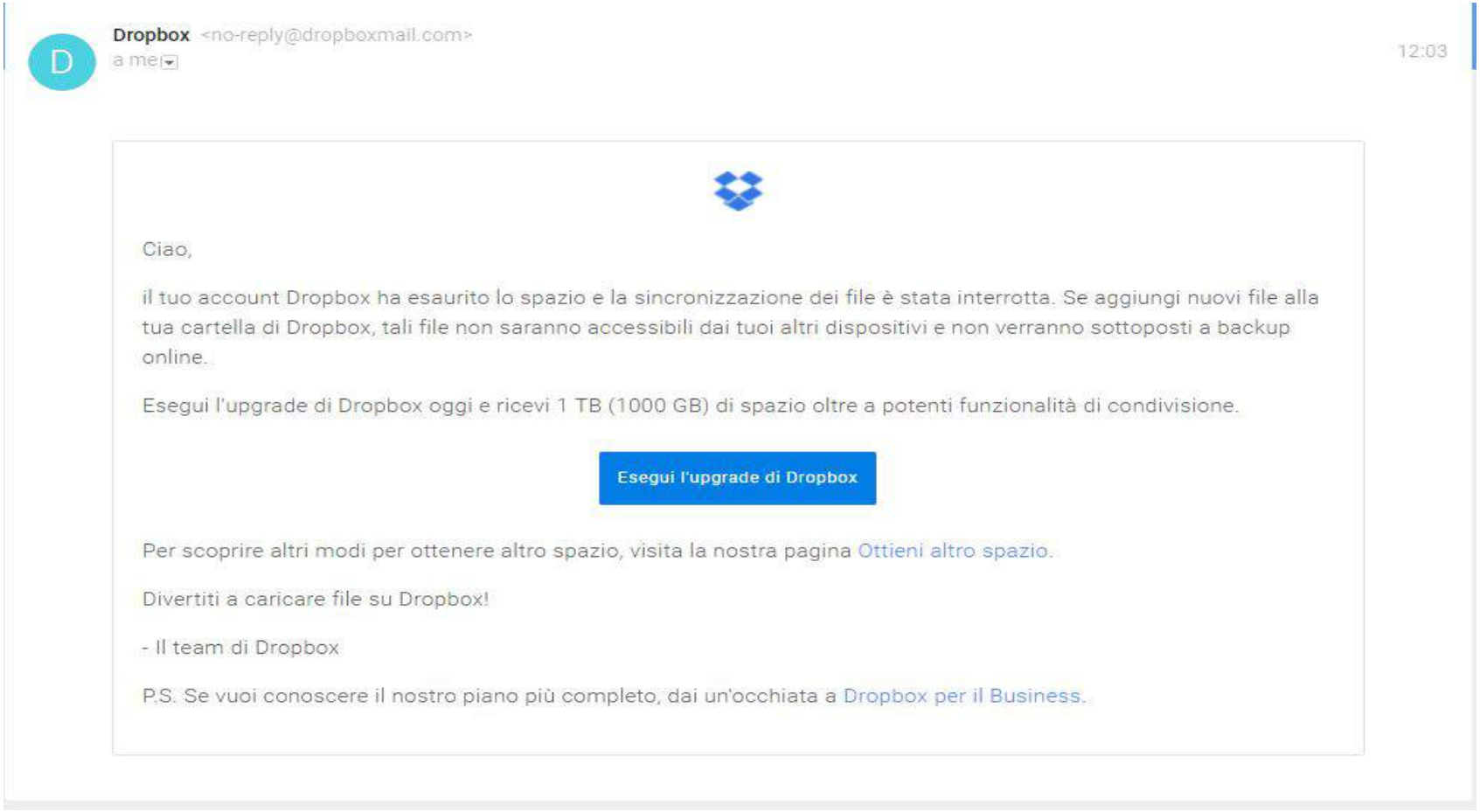


http://myaccount.google.com-securitysettingpage.ml-security.org/signonoptions/

LE MISURE DI SICUREZZA



LE MISURE DI SICUREZZA



D

Dropbox <no-reply@dropboxmail.com>
a me

12:03

Ciao,

il tuo account Dropbox ha esaurito lo spazio e la sincronizzazione dei file è stata interrotta. Se aggiungi nuovi file alla tua cartella di Dropbox, tali file non saranno accessibili dai tuoi altri dispositivi e non verranno sottoposti a backup online.

Esegui l'upgrade di Dropbox oggi e ricevi 1 TB (1000 GB) di spazio oltre a potenti funzionalità di condivisione.

Esegui l'upgrade di Dropbox

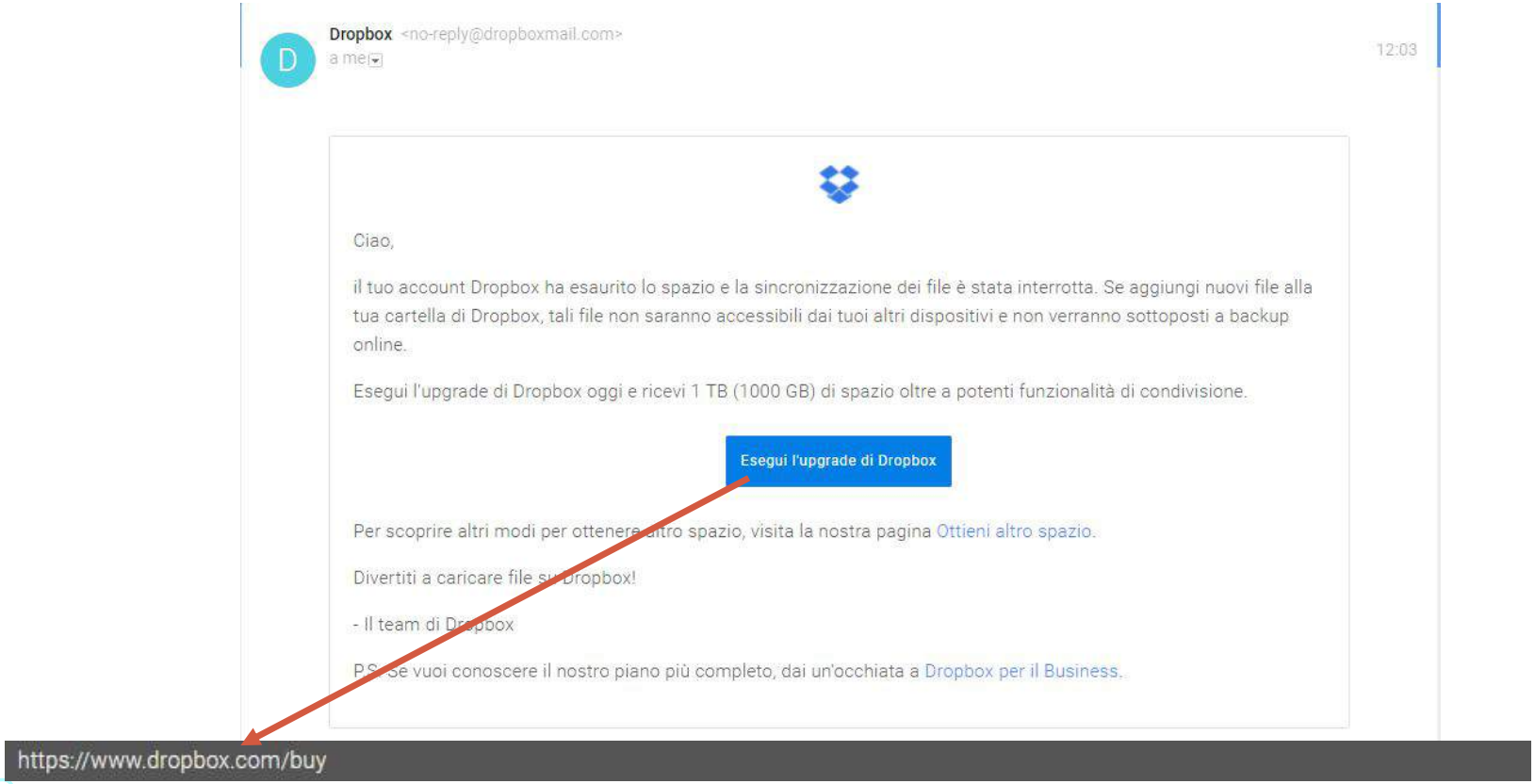
Per scoprire altri modi per ottenere altro spazio, visita la nostra pagina Ottieni altro spazio.

Divertiti a caricare file su Dropbox!

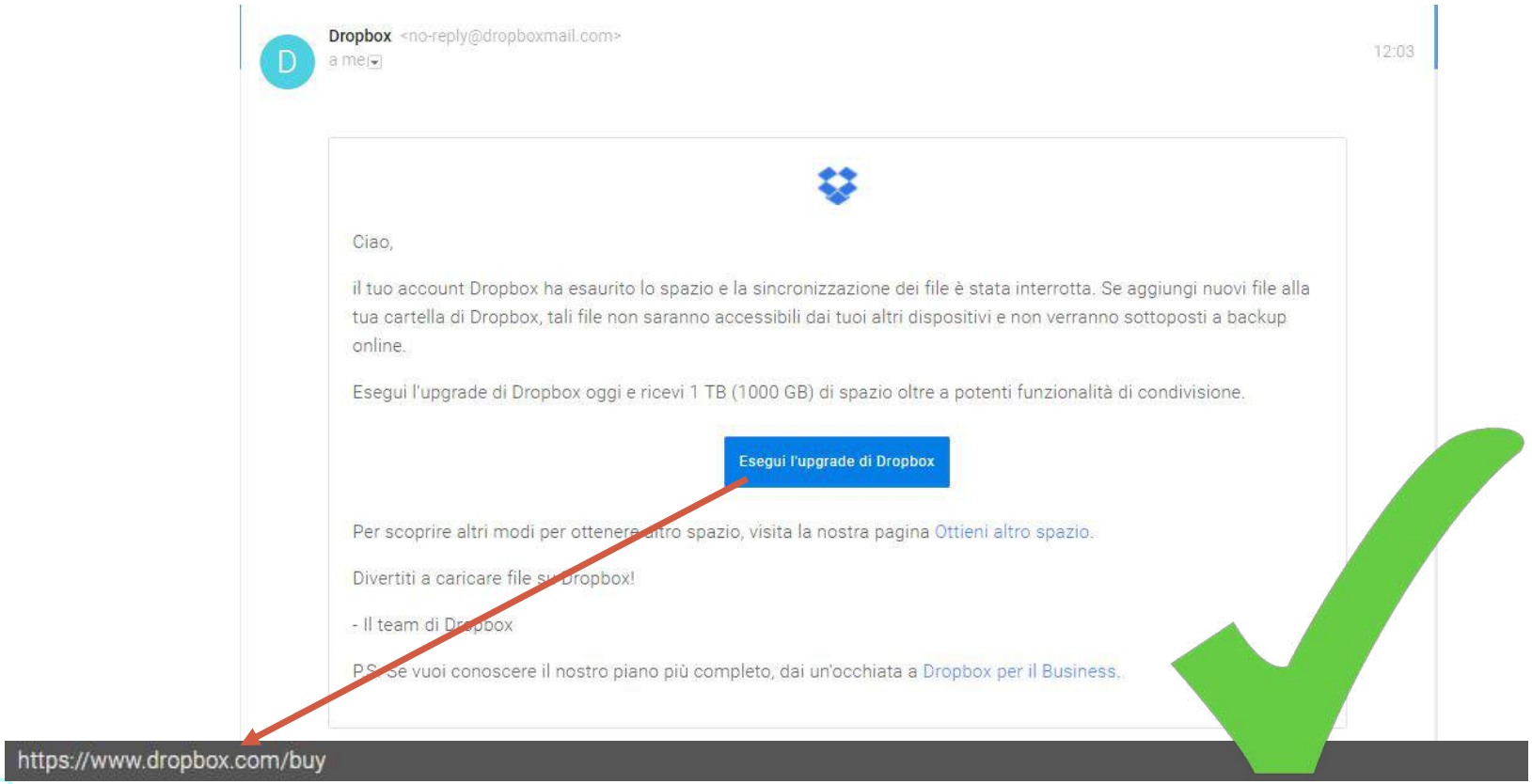
- Il team di Dropbox

P.S. Se vuoi conoscere il nostro piano più completo, dai un'occhiata a Dropbox per il Business.

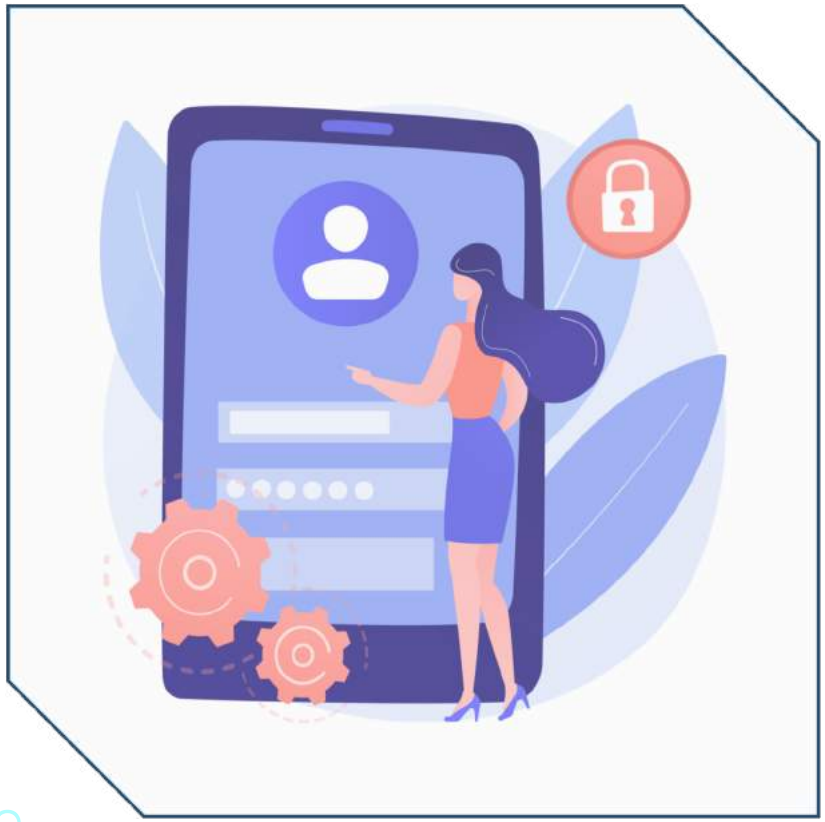
LE MISURE DI SICUREZZA



LE MISURE DI SICUREZZA



LE MISURE DI SICUREZZA



SUGGERIMENTI PER CREARE E GESTIRE LE PASSWORD

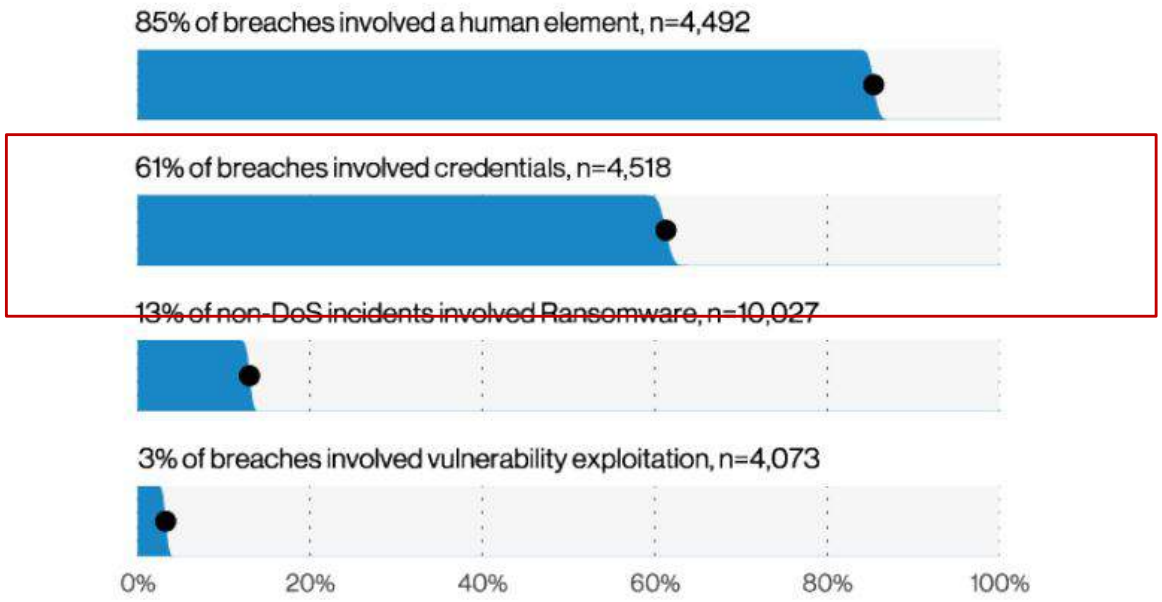
LE MISURE DI SICUREZZA

La prima linea di difesa dei nostri dati personali è sempre la consapevolezza su come gestiamo, conserviamo ed eventualmente diffondiamo le informazioni che ci riguardano.

La **password** è, in ambito informatico e crittografico, una sequenza di caratteri alfanumerici e di simboli utilizzata per accedere in modo esclusivo a una risorsa informatica o per effettuare operazioni di cifratura.

PRINCIPALI FONTI DI VULNERABILITÀ

FONTE: VERIZON - 2021 DATA BREACH INVESTIGATIONS REPORT



LE PEGGIORI PASSWORD DEL 2022 IN ITALIA

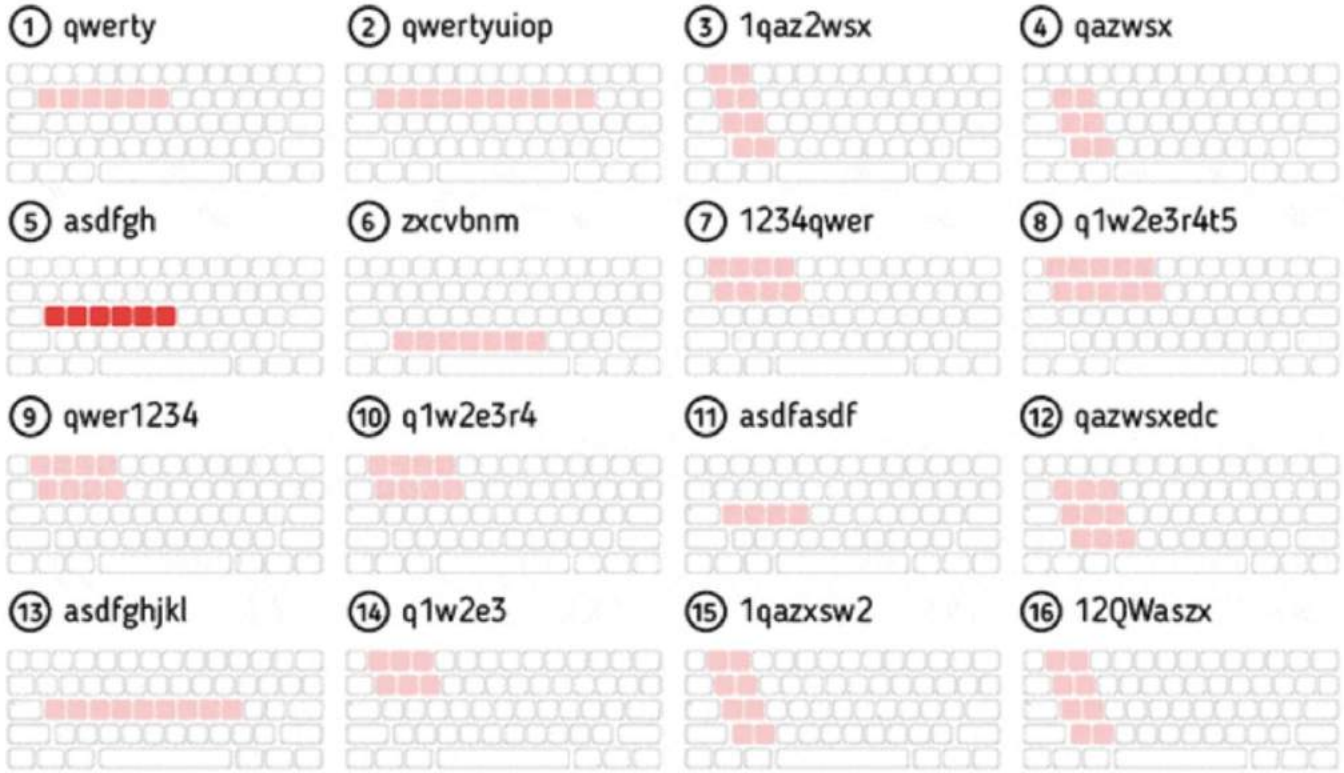
1. 123456
2. 123456789
3. password
4. ciao
5. juventus
6. napoli
7. ciaociao
8. 12345
9. 12345678
10. martina

Fonte: NORDPASS.COM

I METODI DI CREAZIONE PASSWORD MENO SICURI

1. password uguale al nome utente
2. al nome di figlia o figlio
3. al nome del partner
4. al nome del cane o altro animale domestico;
5. al proprio nome
6. alla data di nascita o di quella dei figli
7. al proprio codice fiscale
8. alla squadra sportiva o celebrità preferiti
9. al nome del sito o servizio al quale accedere
10. a una delle precedenti, ma con varianti deboli come 123 alla fine

PASSWORD COMUNI DA EVITARE
ATTENZIONE ALLE «LINEE»



LE MISURE DI SICUREZZA

Suggerimenti per creare e gestire password a prova di privacy

- deve essere abbastanza lunga: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa “robusta” (si suggerisce intorno ai 15 caratteri);
- deve contenere caratteri di almeno 4 diverse tipologie;

LE MISURE DI SICUREZZA

Suggerimenti per creare e gestire password a prova di privacy

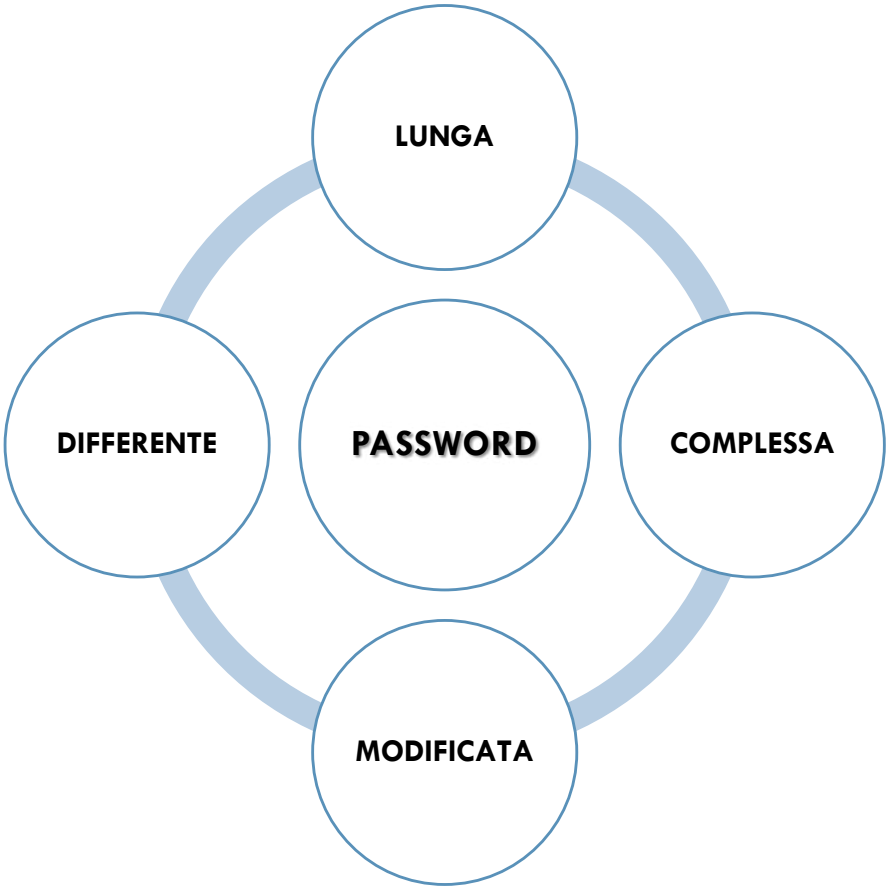
- non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente;
- andrebbe periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

LE MISURE DI SICUREZZA

Suggerimenti per creare e gestire password a prova di privacy

- password diverse per account diversi (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password si evita così il rischio che anche gli altri profili possano essere violati;
- eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.

LE MISURE DI SICUREZZA



www.garanteprivacy.it/flash

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network*, ecc.).

Consigli flash

X TUTELARE

la tua privacy

con buone password

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet.*
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

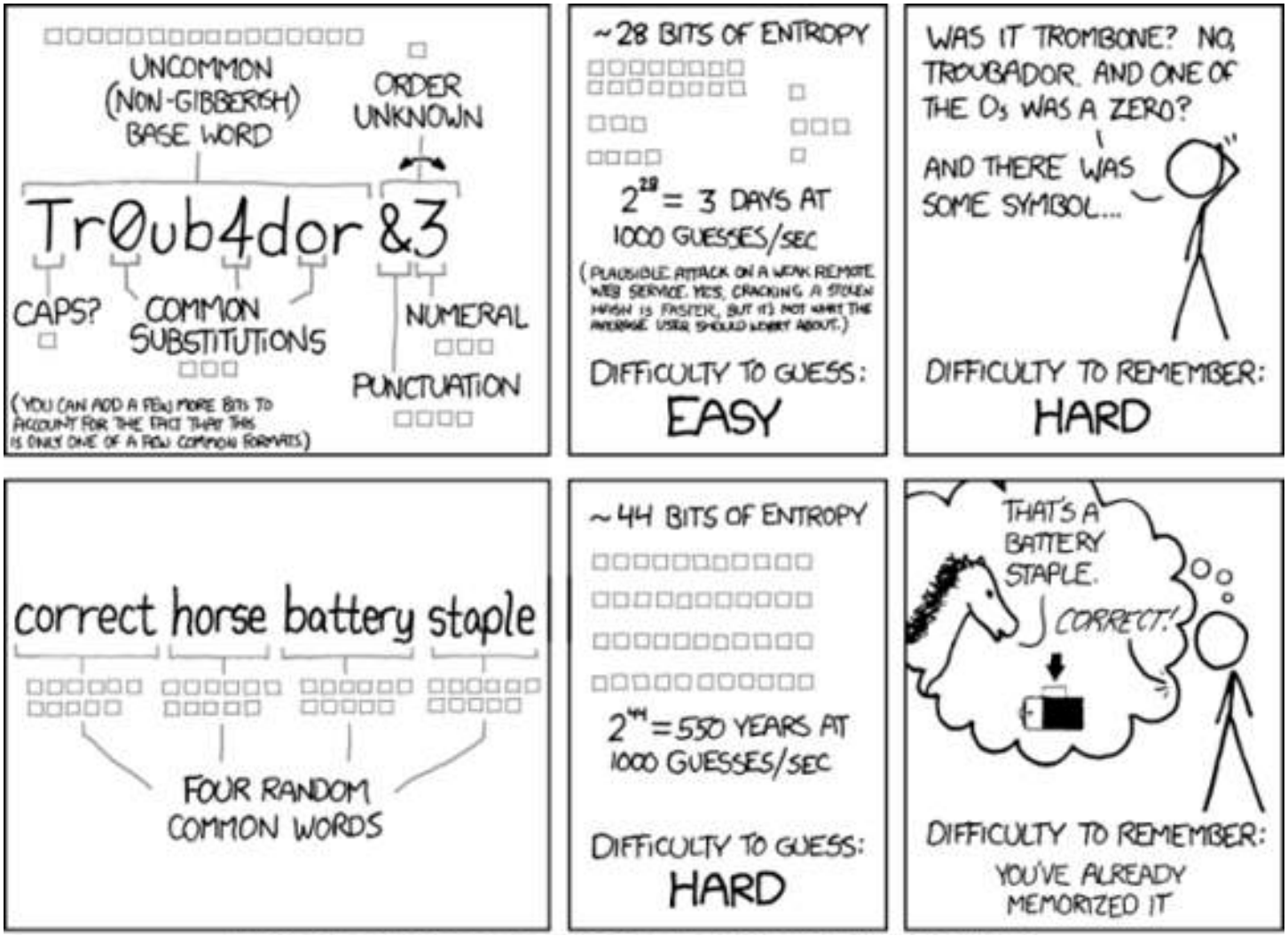
PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD» 4

Si tratta di programmi specializzati che **generano password sicure** e **consentono di appuntare sul pc tutte le password salvandole in un database cifrato sicuro.**
Ce ne sono di vario tipo, gratuiti o a pagamento.

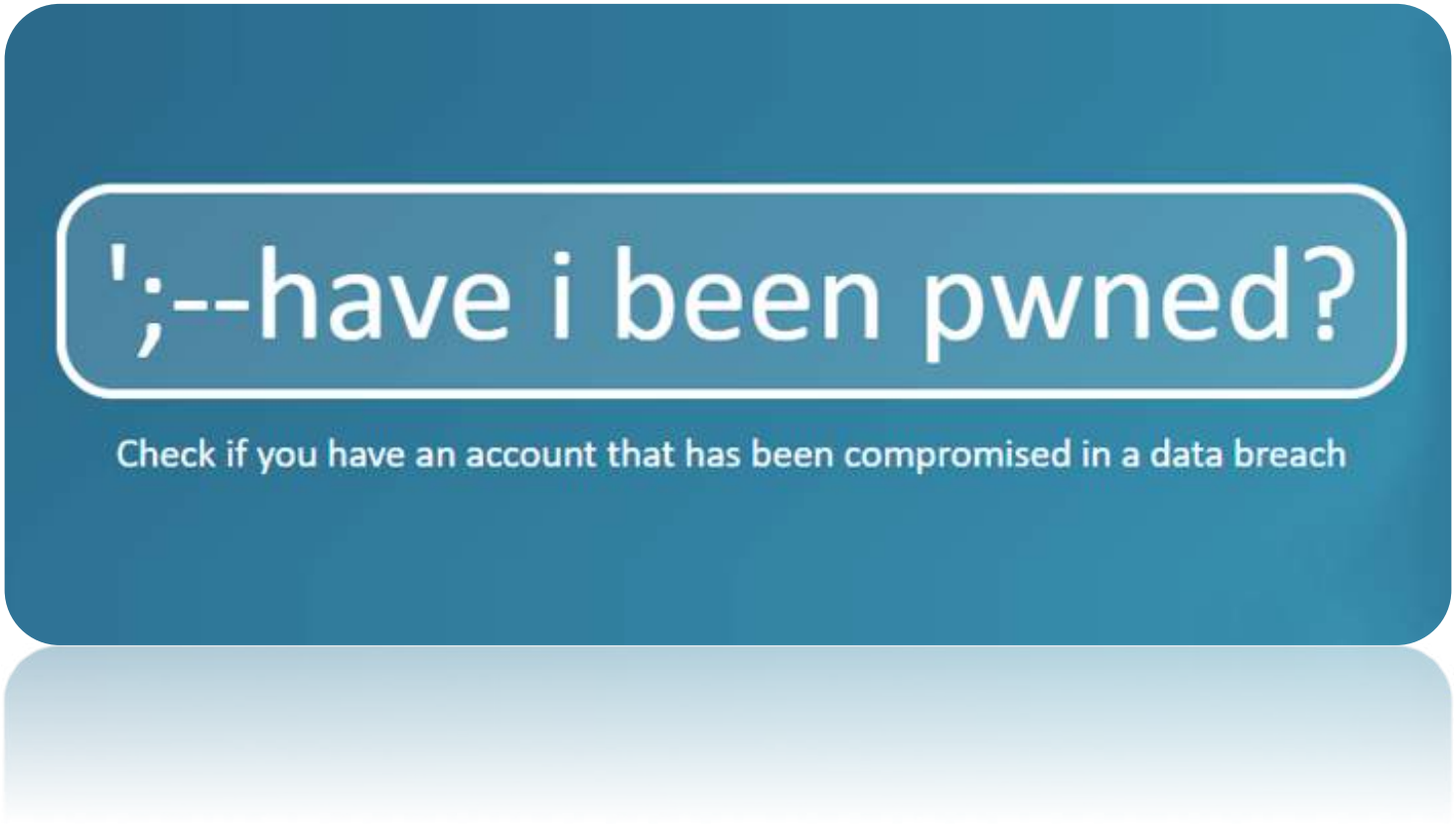
Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash e le nostre campagne di comunicazione «Social privacy», «Fatti smart» e «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante:
www.garanteprivacy.it/home/urp

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

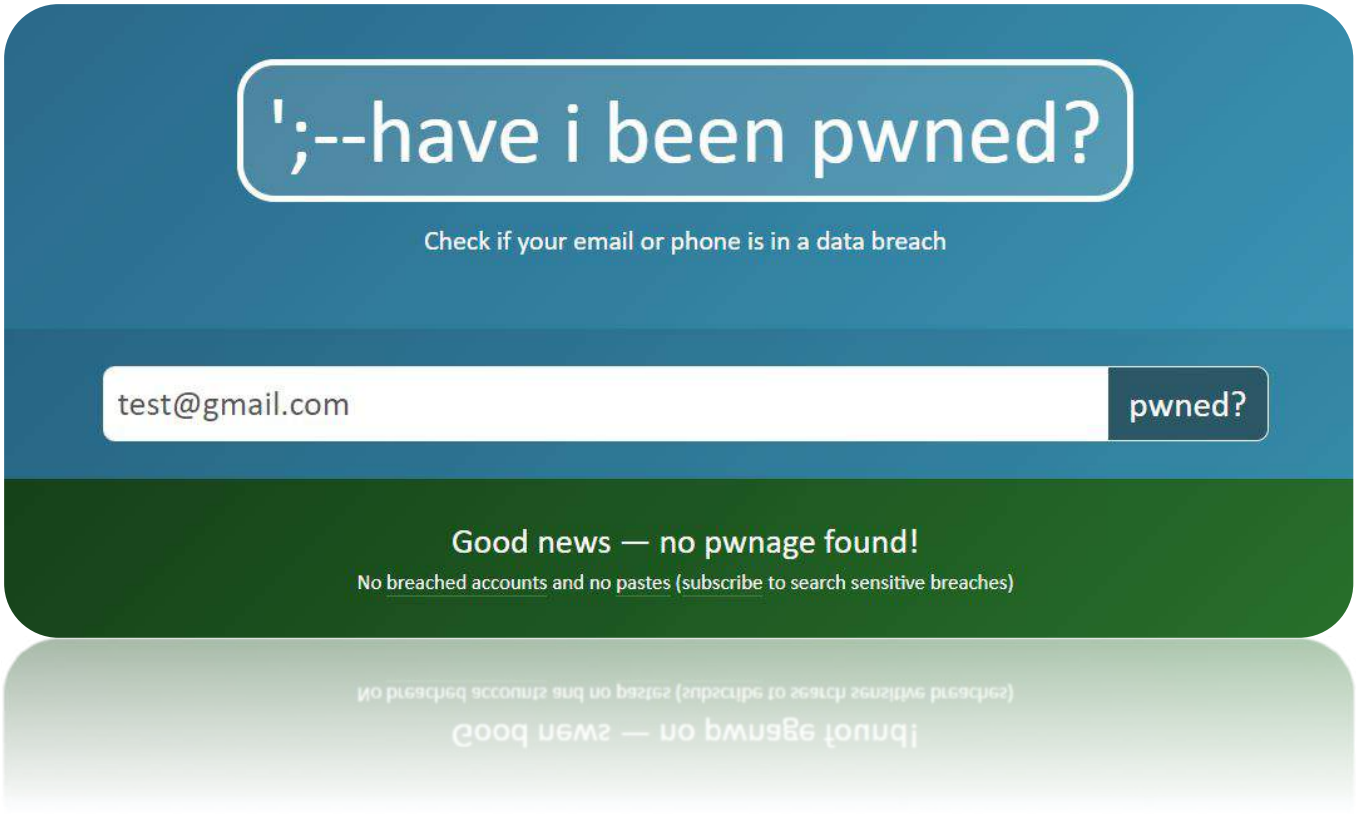
LE MISURE DI SICUREZZA


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

LE MISURE DI SICUREZZA



LE MISURE DI SICUREZZA

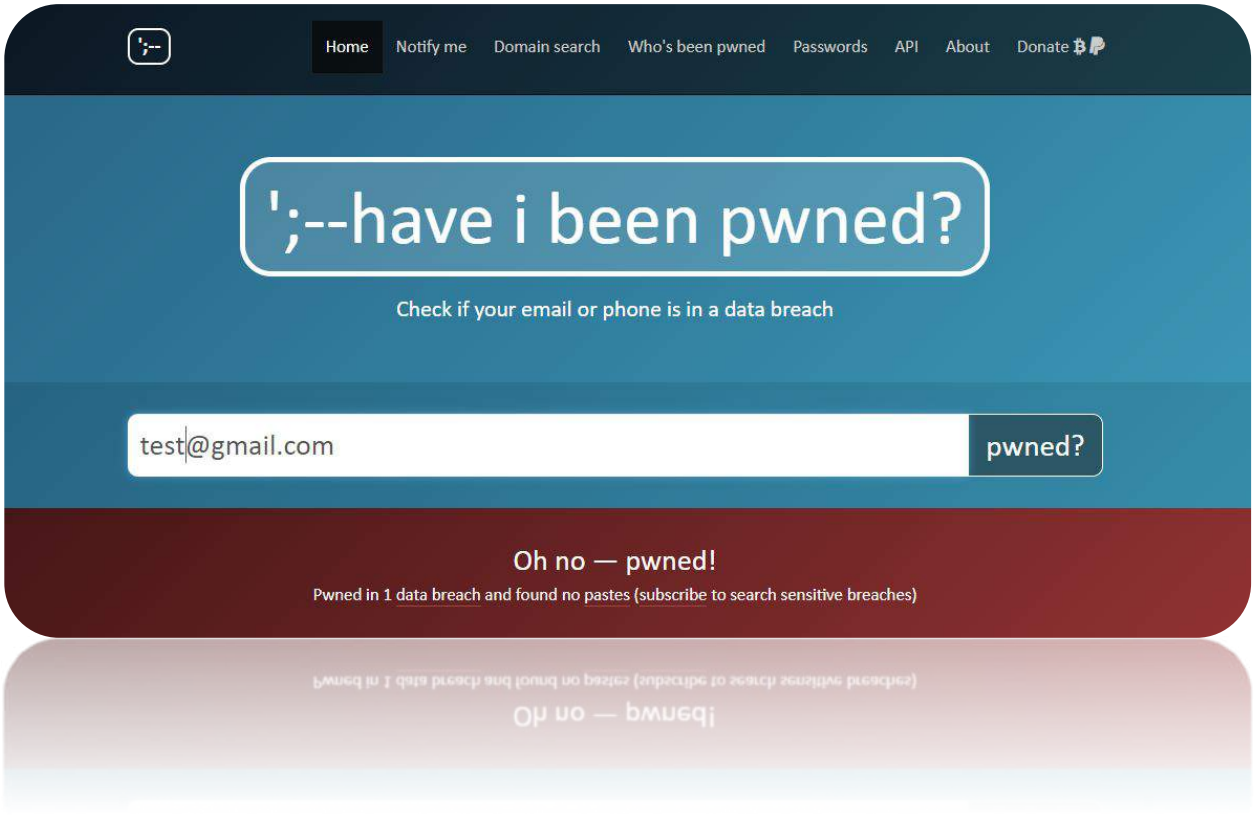


LE MISURE DI SICUREZZA

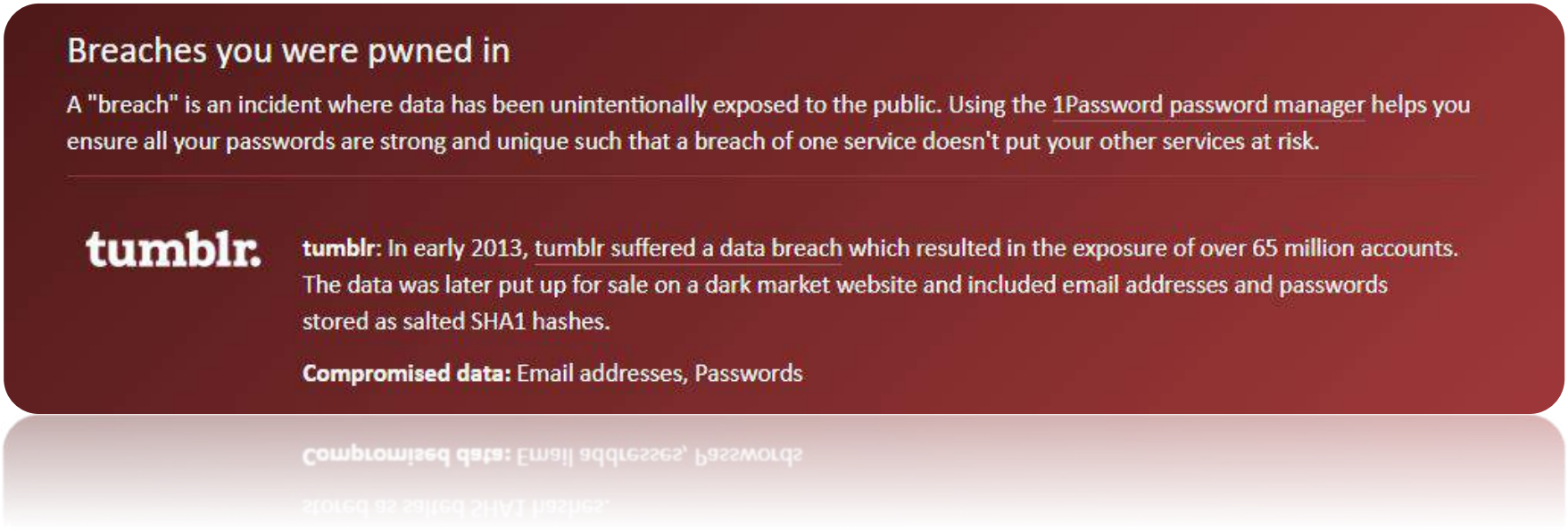
PWned vuol dire essere stati soggetto di una sottrazione di password, a nostra insaputa, da un servizio a cui ci siamo iscritti e che è stato nel tempo hackerato o soggetto a data breach.

Usare la stessa password su diversi siti in questo caso diventa un danno incalcolabile e "*non verificabile*"!

LE MISURE DI SICUREZZA



LE MISURE DI SICUREZZA



«Non è la specie più forte o la più intelligente a sopravvivere, ma quella che si adatta meglio al cambiamento»

Charles Darwin

GRAZIE PER L'ATTENZIONE

Avv. Antonio Valentini
+39 348 1134 952
a.valentini@operaprofessioni.it