

Cybersecurity

DIEGO DIMALTA

avvocato esperto in data protection

Lifelong learning

IN COLLABORAZIONE CON

EUSERVICE



Perché parliamo di **CYBERSECURITY?**

CYBERSECURITY?

Perché ne parliamo?

Per rispondere a questa domanda, dobbiamo pensare ai nomi principali nel panorama tech mondiale:

Google

Youtube (Google)

META: Facebook, Instagram, Whatsapp

Spotify

Avete mai pagato un loro servizio?

NO, eppure fatturano centinaia di miliardi di dollari.

Il valore dei nostri dati

Questo perché i dati hanno un **enorme** valore.

Lo hanno nel mercato “ufficiale” come anche nel mercato “nero”, ovvero nel **DARK WEB**.

Questo il valore dei vostri dati:

Projected figures 2025



530%
increase of global data
volume
from 33 zettabytes in
2018 to 175 zettabytes



€829 billion
value of data economy
in the EU27
from €301 billion (2.4%
of EU GDP) in 2018



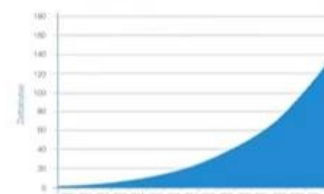
10.9 million
data professionals in
the EU27
from 5.7 million in 2018



65%
Percentage of EU
population with basic
digital skills
from 57% in 2018

Volume dei dati*:

Dal 2012 al 2016
→ Cresciuto di 7 volte



Dal 2016 al 2025
→ Si stima crescita di 10 volte

Supporti Economici del Ministero dello Sviluppo Economico & European Data Strategy

€4-6 billion to be invested in total
in common European data spaces and a European federation
of cloud infrastructure and services

*International Data Corporation

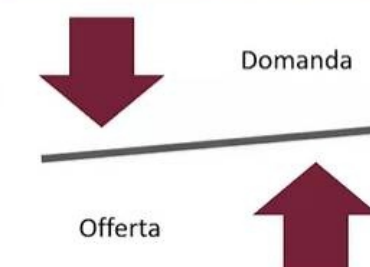
**The European Data Strategy 2020

Valore dei dati **: 2025



€829 billion
(5.8% of EU GDP)

Dati e Tecno logie



*Una **Mastercard clonata** con tanto di PIN la si può comprare a 25 dollari, 35 dollari per una American Express, un passaporto di uno qualsiasi dei Paesi dell'Unione europea arriva a costare 4.000 dollari, oppure un **passaporto** maltese può arrivare a 6.500 dollari, mentre per la carta di identità si va dai 120 dollari dei Paesi UE ai 500 dollari della Lettonia.*

Avete mai cercato *#patente* su *Instagram*?

Ci sono poi i record di migliaia di **mail rubate** che sono molto economici, attorno ai 10 dollari per centinaia di migliaia di email, fino al **furto di database di elettori degli Stati Uniti** (con le loro email per il voto elettronico), che costano più o meno 100 dollari.

FONTE: <https://www.cybersecitalia.it/si-aggiorna-il-listino-prezzi-sul-dark-web-da-4-000-dollari-per-un-passaporto-ai-25-per-una-carta-di-credito-clonata/14464/>

Ma che cosa spinge un Hacker a portare avanti la sua attività criminale?

1. Profitto
2. Dimostrazione di abilità
3. Noia
4. Scopi sessuali e/o revenge porn



Ragazzo di 16 anni entra nei sistemi del Pentagono

<https://ricerca.repubblica.it/repubblica/archivio/repubblica/2005/05/11/sedici-anni-ruba-con-il-computer.html>



È un ragazzo di 17 anni l'hacker che è riuscito ad infiltrarsi nei sistemi informatici di Twitter

<https://www.federprivacy.org/informazione/societa/e-un-ragazzo-di-17-anni-l-hacker-che-e-riuscito-ad-infiltrarsi-nei-sistemi-informatici-di-twitter#>



Sul web aumentano i reati contro i minori e si abbassa l'età anagrafica delle vittime

<https://www.interno.gov.it/it/notizie/sul-web-aumentano-i-reati-contro-i-minori-e-abbassa-leta-anagrafica-vittime>

Questi episodi ci dimostrano due cose:

1. che nessun computer è sicuro al 100%
2. che le forze dell'ordine sono ormai in grado di individuare chi viola i sistemi altrui

FALSO MITO

Le bugie che raccontiamo a noi stessi

Ma nel mio PC/Profilo non c'è nulla di importante oppure ma io non ho nulla da nascondere!

Queste sono solo bugie che raccontiamo a noi stessi. Chiunque ha qualcosa da nascondere, e non c'è nulla di male nell'ammetterlo. Il nostro io pubblico è diverso da quello privato, a partire dai vestiti. Cosa indossiamo in pubblico è diverso da cosa indossiamo a casa.

“Sostenere che non ti interessa il diritto alla privacy perché non hai nulla da nascondere è come sostenere che non ti importa della libertà di parola perché non hai nulla da dire.”

(Edward Snowden)

Tutti hanno qualcosa da nascondere

E allora bisogna proteggere la propria riservatezza!

COME?

- Selezione di cosa pubblicare
- Antivirus
- Gestione delle password
- Diffidare dei link sospetti
- Non perdere i dati altrui
- Non usare app poco chiare
- Autenticazione a due fattori, sempre ove possibile

SELEZIONE

di cosa pubblicare

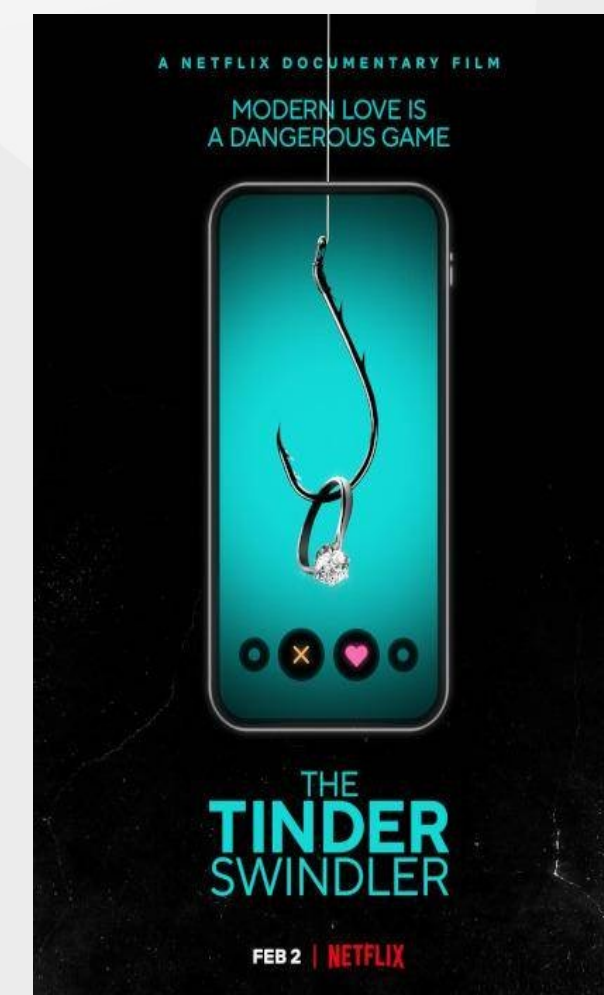
I social network sono molto utili se usati bene, ma molto pericolosi se usati male.

Tutto ciò che pubblicate resta e:

1. vi espone a malintenzionati
2. incide sul vostro futuro

ATTENZIONE! Non capita solo agli adulti o agli sprovveduti, anzi...

Ecco due esempi:



Brand reputation: i recruiter guardano anche i social prima di scegliere il candidato.

ANTIVIRUS

Statistiche, trend e fatti su Antivirus e Cyber-security nel 2022

<https://it.safetymdetectives.com/blog/antivirus-statistics-it/>

Antivirus e firewall non bastano più: una questione non solo tecnologica

<https://www.cybersecurity360.it/soluzioni-aziendali/antivirus-e-firewall-non-bastano-piu-una-questione-non-solo-tecnologica/>

LINK SOSPETTI/MALWARE

Phishing e malware sono la dimostrazione tangibile che **anche il sistema più sicuro al mondo può essere penetrato**. È l'errore umano spesso che consente l'ingresso ai malintenzionati, motivo per cui si parla anche di “**social engineering**”.

Come funziona:

CASO 1: invio massiccio di link malevoli

CASO 2: penetrazione nel sistema, studio accurato dei comportamenti e invio di una sola mail malevola

Come ridurre il rischio:

Se vi chiedono soldi o password, prima di inserirle chiamate il destinatario (apparente).

NB: non scrivete, perchè il ricevente potrebbe essere sempre il malintenzionato che si finge il destinatario.

PASSWORD

La password più usata nel mondo è 'password', in Italia '123456'

Studio: l'83% delle parole chiave si può decifrare in 1 secondo

FONTE:

https://www.ansa.it/sito/notizie/tecnologia/hitech/2022/11/15/parola-password-e-la-password-piu-usata-in-italia-123456_192143b2-77dd-402b-98ff-86e02e8cc9ea.html#:~:text=Nel%202022%20la%20password%20pi%C3%B9,utenti%20%C3%A8%20invece%22123456%22

I due errori più ricorrenti sono:

1. l'utilizzo di password “deboli”
2. l'utilizzo della stessa password per più servizi



QUANDO UNA PASSWORD PUÒ DIRSI “FORTE”

Ha almeno 8 caratteri di cui:

- 1 numero
- 1 carattere speciale
- 1 maiuscola
- 1 minuscola

ATTENZIONE: in base alle **nuove indicazioni del NIST**, questi parametri **non bastano** se usati per formare parole di senso compiuto o facilmente riconducibili al soggetto.

Es:

\$uperMan!

Di3g0dim@Ita

M1laN0!!

Non solo, sempre in base al NIST, ove possibile è opportuno usare password randomiche della lunghezza massima consentita.



NO A
PROFILI
CONDIVISI



NO A
PASSWORD
CONDIVISE

Condividere la password non è una prova d'amore, è un gesto che può esporvi a rischi importanti.

Se il vostro partner insiste per avere la vostra password... **cambiate partner!**

AUTENTICAZIONE A DUE FATTORI

La debolezza delle password ha portato all'aumento dei furti di identità sui social. Anche per questo è in ogni caso opportuno attivare L'autenticazione a due fattori.

*“Quando attivi l'autenticazione a due fattori, ti viene chiesto di scegliere tra l'invio di codici tramite SMS o un'app di autenticazione di terzi come **metodo di sicurezza principale**. Per generare codici di accesso che ci aiutano a verificare la tua identità quando accedi da un nuovo dispositivo per la prima volta è possibile usare un'app di autenticazione di terzi (come Duo Mobile o Google Authenticator).”*

Instagram.com

PERDITA DI DATI

Data breach: l'Italia brucia 3,40 milioni. Si profila il rischio cyber-tax.

<https://www.corrierecomunicazioni.it/cyber-security/data-breach-litalia-brucia-340-milioni-ibm-rischio-cyber-tax/>

CYBERBULLISMO

Con il termine «cyber-bullismo» si intende **qualunque forma di pressione, aggressione, molestia**, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, **trattamento illecito di dati personali realizzati, per via telematica**, a danno di minori, nonché la diffusione di contenuti on line riguardanti uno o più componenti della famiglia di un minore con lo scopo di isolarlo, attaccarlo o metterlo in ridicolo.

Che cosa prevede la Legge n. 71/2017?

La legge 71/2017 consente ai minori di chiedere l'oscuramento, la rimozione o il blocco di contenuti, a loro riferiti e diffusi per via telematica, che ritengono essere atti di cyber-bullismo (ad esempio, foto e video imbarazzanti o offensive, oppure pagine web o post sui social network in cui si è vittime di minacce, offese o insulti, ecc.).

Il titolare del trattamento o il gestore del sito internet o del social media che ospita i contenuti ritenuti offensivi risponde ed eventualmente provvede alla richiesta di eliminazione nei tempi previsti dalla legge. Nel caso in cui la richiesta non venga soddisfatta, **ci si può rivolgere al Garante per la protezione dei dati personali**, che entro 48 ore si attiva sulla segnalazione. Per inoltrare le segnalazioni all'Autorità si può utilizzare il modello disponibile su www.garanteprivacy.it/cyberbullismo.

FONTE: GarantePrivacy.it

REVENGE PORN

Si tratta della diffusione non autorizzata di materiale intimo.

CODICE PRIVACY Art. 144-bis (Revenge porn)

1. Chiunque, compresi i minori ultraquattordicenni, abbia fondato **motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito** che lo riguardano, destinati a rimanere privati, **possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso** ha facoltà di segnalare il pericolo al Garante, il quale, nelle quarantotto ore dal ricevimento della segnalazione, decide ai sensi degli articoli 143 e 144 del presente codice.
2. Quando le registrazioni audio, le immagini o i video o gli altri documenti informatici riguardano minori, la segnalazione al Garante può essere effettuata anche dai genitori o dagli esercenti la responsabilità genitoriale o la tutela. [...]

ATTENTI AL DEEP FAKE

I deep fake sono foto, video e audio creati grazie a software di **intelligenza artificiale** (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.



LEI NON È ILARY BLASI.



LUI NON È TOM CRUISE.

CARRIERE NELLA CYBERSECURITY

MENU

CERCA

la Repubblica

ABBONATI

GEDÌ SMILE

R

ACCEDI

Cybersecurity, in Italia servono almeno 100mila esperti in più

di Mattia Pirola

Il nostro è il terzo Paese al mondo più colpito da attacchi ransomware. Tuttavia le risorse umane disponibili non sono sufficienti a coprire le necessità di tutte le aziende

05 LUGLIO 2022 ALLE 15:57

1 MINUTI DI LETTURA

Secondo l'Agenzia per la Cybersicurezza nazionale, per far fronte alle domande delle aziende, nel nostro Paese servono almeno 100.000 esperti. Tuttavia i professionisti che contiamo



NON SOLO «HACKER»

- Pen-tester
- Consulenti
- Red team // Blue team
- Programmatori
- Ethical advisor
- Legal advisor
- CISO



GRUPPO SPAGGIARI PARMA