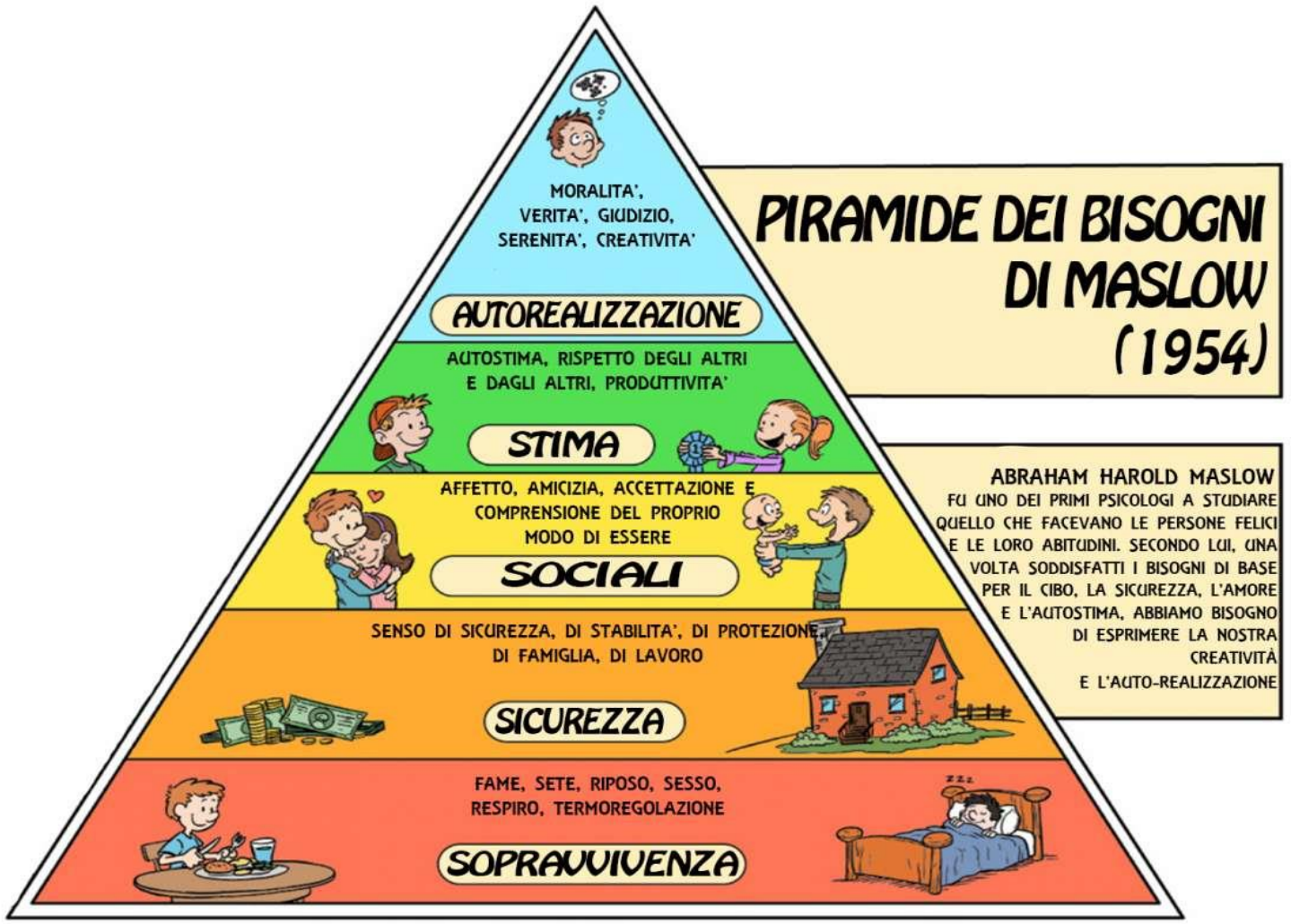
Odcec Torino
La gestione dei rischi negli studi professionali e nelle pmi

Dott. Giovanni FINETTO - ANRA

Giovedì 6 aprile 2023 alle ore 17.00 **- WEBINAR**

PERCHE’ SIAMO QUI OGGI


MORALITA',
VERITA', GIUDIZIO,
SERENITA', CREATIVITA'
AUTOREALIZZAZIONE
AUTOSTIMA, RISPETTO DEGLI ALTRI
E DAGLI ALTRI, PRODUTTIVITA'
STIMA
AFFETTO, AMICIZIA, ACCETTAZIONE E
COMPRENSIONE DEL PROPRIO
MODO DI ESSERE
SOCIALI
SENSO DI SICUREZZA, DI STABILITA', DI PROTEZIONE
DI FAMIGLIA, DI LAVORO
SICUREZZA
FAME, SETE, RIPOSO, SESSO,
RESPIRO, TERMOREGOLAZIONE
SOPRAVVIVENZA
PIRAMIDE DEI BISOGNI
DI MASLOW
(1954)
ABRAHAM HAROLD MASLOW
FU UNO DEI PRIMI PSICOLOGI A STUDIARE
QUELLO CHE FACEVANO LE PERSONE FELICI
E LE LORO ABITUDINI. SECONDO LUI, UNA
VOLTA SODDISFATTI I BISOGNI DI BASE
PER IL CIBO, LA SICUREZZA, L'AMORE
E L'AUTOSTIMA, ABBIAMO BISOGNO
DI ESPRIMERE LA NOSTRA
CREATIVITÀ
E L'AUTO-REALIZZAZIONE

«*Una buona **strategia di gestione dei rischi** si sta configurando sempre di più come uno dei più **importanti fattori di competitività per le imprese** ed è, inoltre, percepita come una componente fondamentale dello **sviluppo sostenibile***»

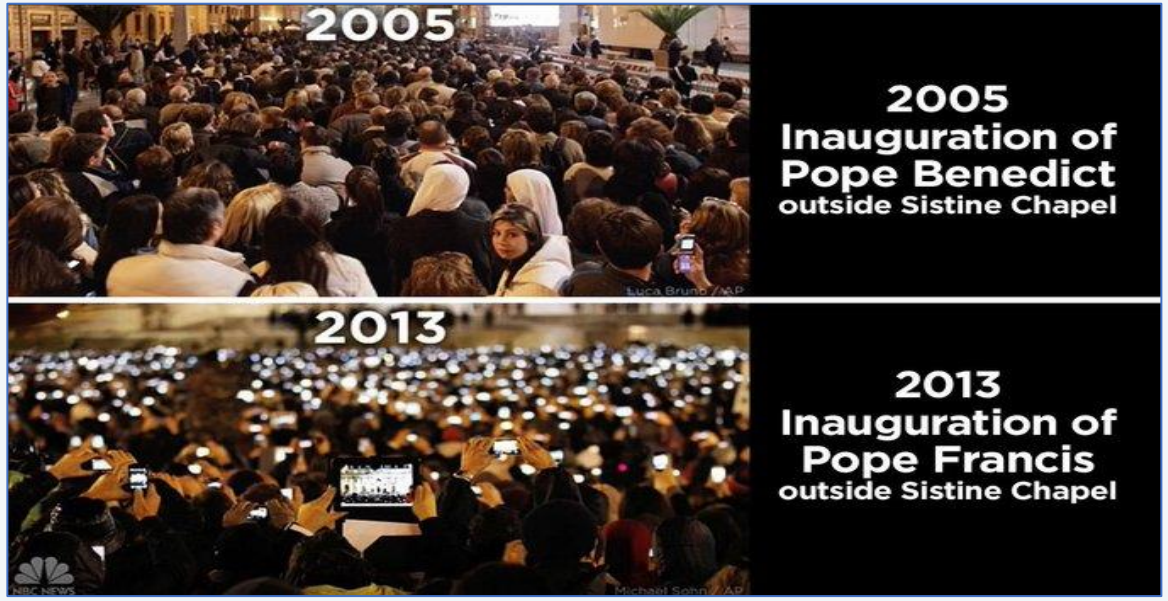
IX edizione dell'*Osservatorio sulla diffusione del risk management nelle medie imprese italiane* del Consorzio universitario del Politecnico di Milano, Cineas. LMF LaMiaFinanza - 22/06/2022 17:44:26 (updated 24/06/2022 12:26:26)

Dal Rapporto emerge che quasi l'80% delle aziende ritiene ci sia una **stretta correlazione tra risk management e sviluppo sostenibile**, ma che solo il 44% presenta una **mappatura dei rischi a livello di CdA**, un numero ancora ridotto e che rivela il grande lavoro che ancora deve essere fatto in Italia.

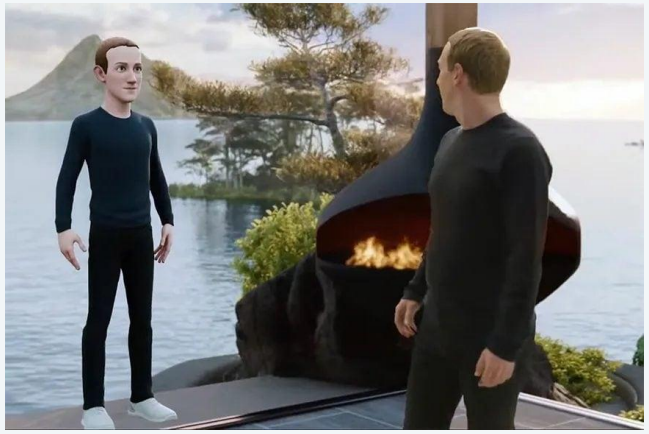
*Le aziende in cui il board è coinvolto vedono il **risk management come un investimento strategico** anche per prevedere e gestire i nuovi rischi e assicurare la business continuity.*

IX edizione dell'*Osservatorio sulla diffusione del risk management nelle medie imprese italiane* del Consorzio universitario del Politecnico di Milano, Cineas. LMF LaMiaFinanza - 22/06/2022 17:44:26 (updated 24/06/2022 12:26:26)

Fonte: Tassonomia Rischi ANRA

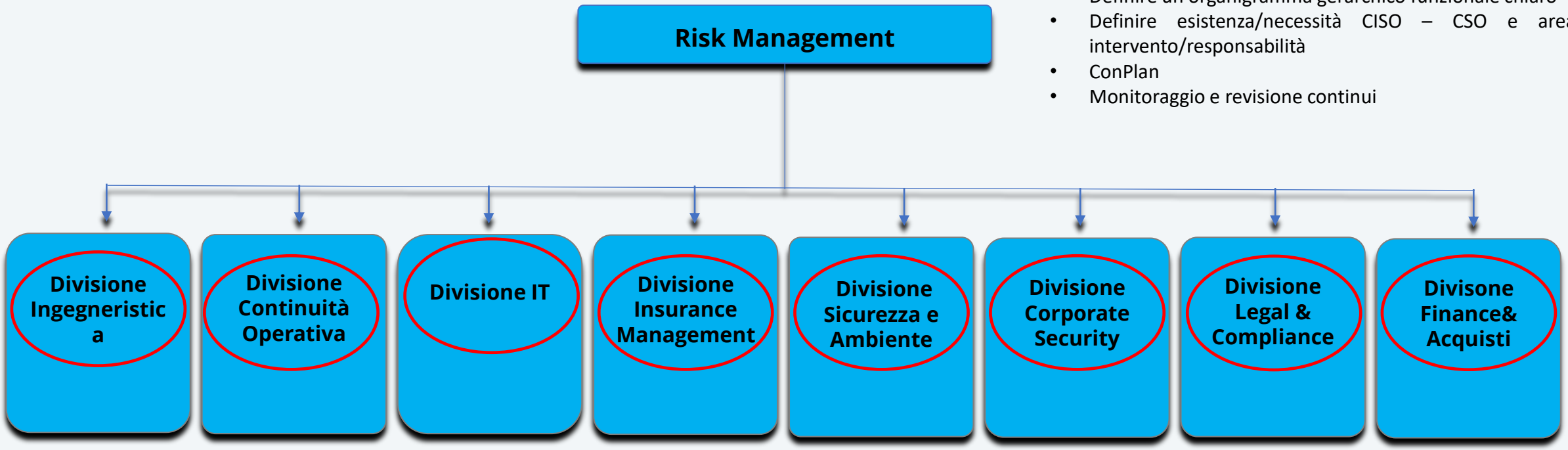

2005
2005
Inauguration of
Pope Benedict
outside Sistine Chapel
2013
2013
Inauguration of
Pope Francis
outside Sistine Chapel


THE METAVERSE



Fonte: Tassonomia Rischi ANRA

- Definire un organigramma gerarchico funzionale chiaro
- Definire esistenza/necessità CISO – CSO e area di intervento/responsabilità
- ConPlan
- Monitoraggio e revisione continui



- Privacy by design, default
- Code review

- Back-up
- Incident management

- Back-up
- Incident management
- VA
- PT
- …

- **Cyber Risk Insurance**

- Cyber security dei sistemi di safety

- Cyber security dei sistemi di security

- Reati informatici 231/2001
- GDPR art.32

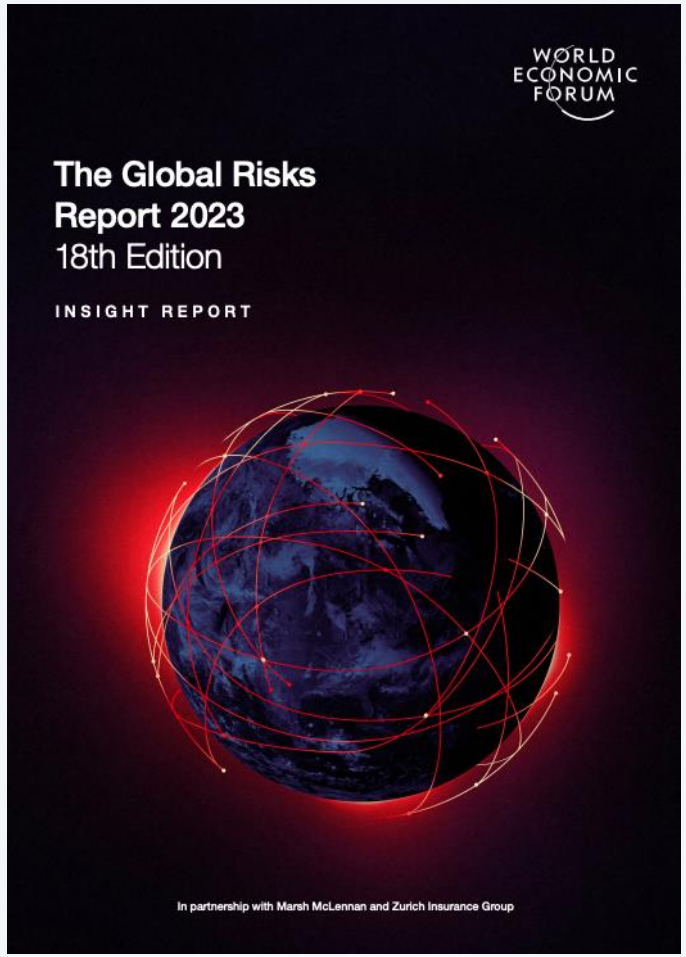
- Protezione metodi pagamento
- …

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period"

	2 years	10 years
1	Cost-of-living crisis	Failure to mitigate climate change
2	Natural disasters and extreme weather events	Failure of climate-change adaptation
3	Geoeconomic confrontation	Natural disasters and extreme weather events
4	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	Large-scale involuntary migration
6	Large-scale environmental damage incidents	Natural resource crises
7	Failure of climate change adaptation	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	Widespread cybercrime and cyber insecurity
9	Natural resource crises	Geoeconomic confrontation
10	Large-scale involuntary migration	Large-scale environmental damage incidents

Risk categories: Economic | Environmental | Geopolitical | Societal | Technological



Analisi dei principali cyber attacchi noti del 2022 a livello globale

Italia nel mirino

Osservando la situazione dal punto di vista quantitativo, negli ultimi 5 anni la situazione è peggiorata nettamente, seguendo un trend pressoché costante. Confrontando i numeri del 2018 con quelli del 2022 la crescita del numero di attacchi rilevati è stata del 60% (da 1.554 a 2.489).

Art. 32 GDPR – Regolamento Generale sulla Protezione dei Dati (UE/2016/679)

Torna all'indice

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:

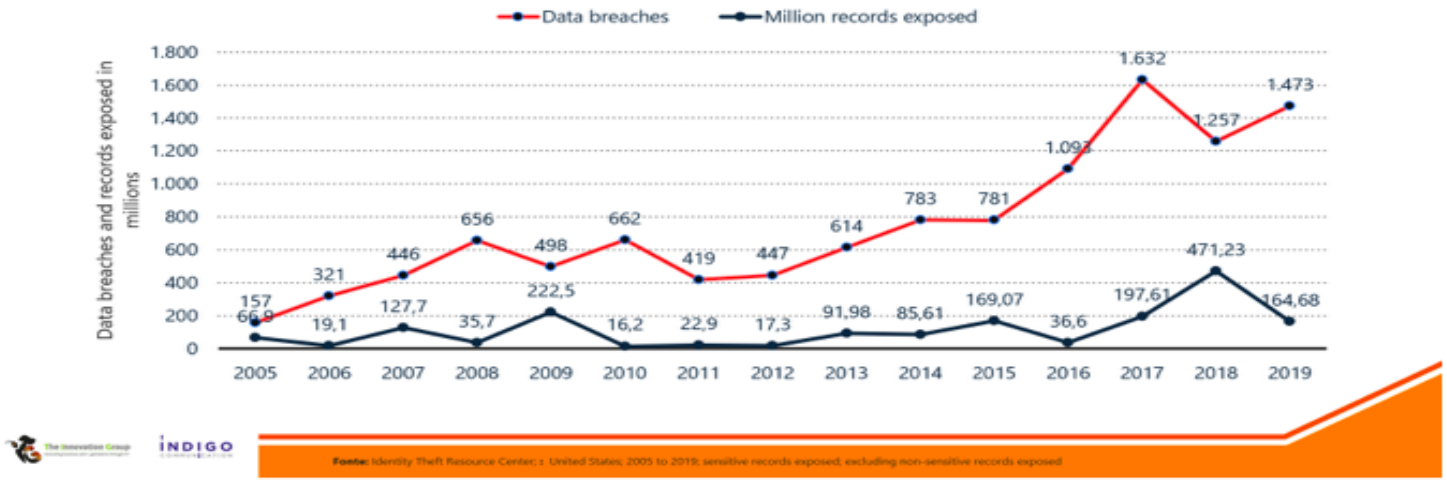
a)	la pseudonimizzazione e la cifratura dei dati personali;
b)	la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c)	la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali 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.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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.

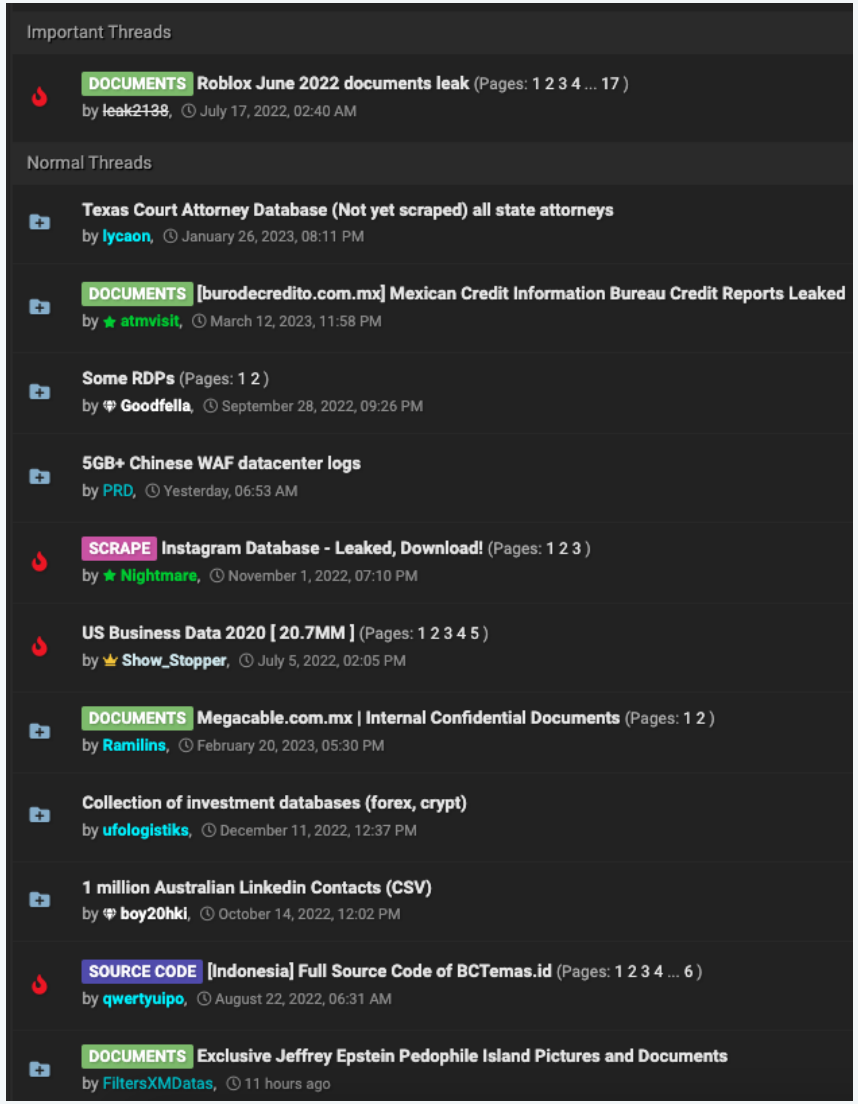
Cyber crime: numero di breach e record esposti (in millioni), 2005-2019



Fonte: Identity Theft Resource Center; i United States; 2005 to 2019; sensitive records exposed; excluding non-sensitive records exposed

Qual è il costo che un'azienda deve sostenere in caso di attacco hacker che comporti un data breach di queste dimensioni?

Una nota ricerca che risponde a questa domanda è quella svolta annualmente da Ponemon Institute, il "**2019 Cost of a Data Breach Report**", che quest'anno, sulla base di interviste a 500 organizzazioni medio grandi di tutto il mondo che hanno subito un data breach, stima che il costo medio per record sottratto sia pari a 150 dollari (era 145 dollari nel 2014). Per le aziende italiane che hanno partecipato allo studio il costo medio si attesta a un valore leggermente inferiore, **146 dollari per record sottratto**. L'analisi prende in considerazione un centinaio di fattori di costo potenziali, tecnologici, legali, regolatori, legati alla perdita del valore del brand, perdita di clienti e mancata produttività dei dipendenti.



Casagrande Group

Files hacked from a drilling and foundation equipment manufacturer.

RELEASE

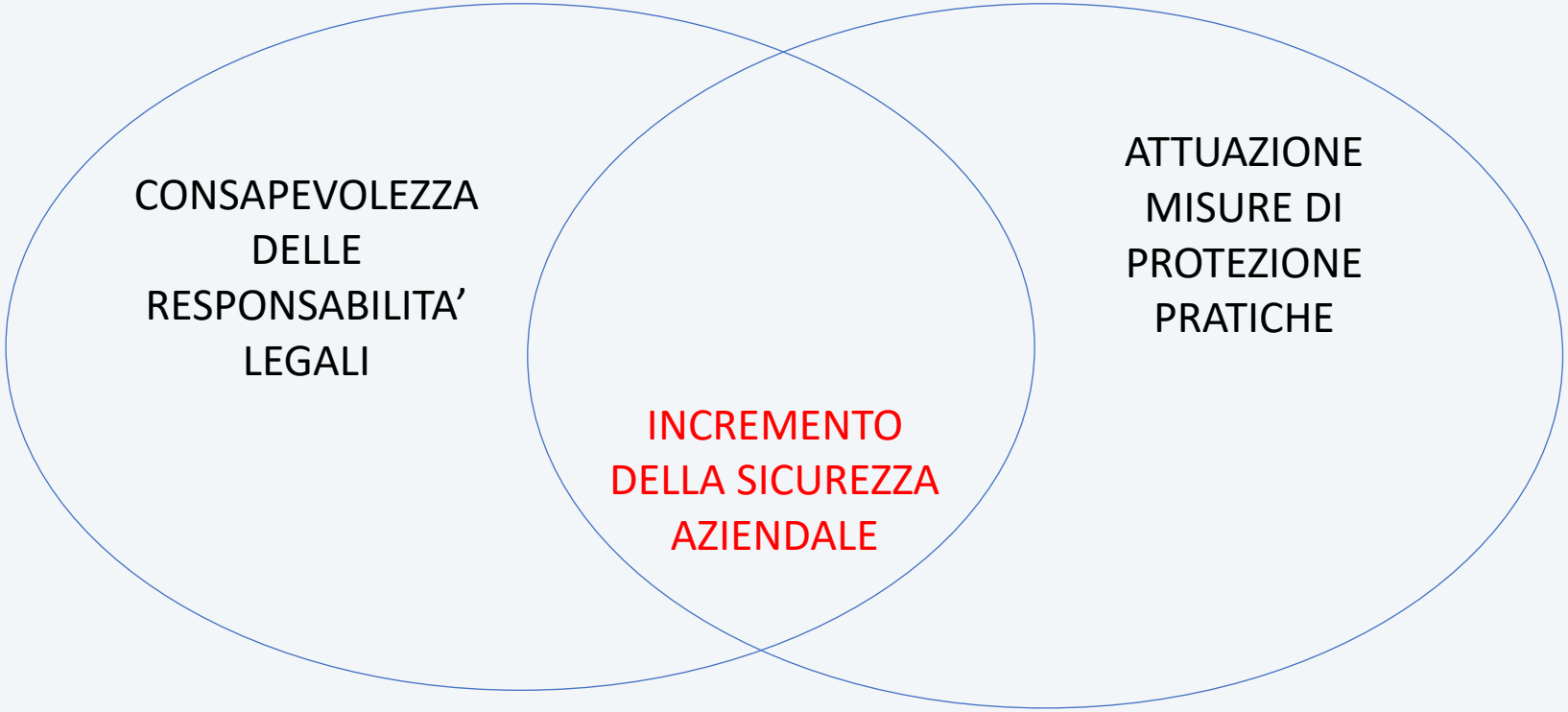
Casagrande Group

Files hacked from a drilling and foundation equipment manufacturer.

DATASET DETAILS

COUNTRIES	Italy
TYPE	Hack
SOURCE	BlackMatter
FILE SIZE	10.5 GB

DOWNLOADS (How to Download)



COMUNICAZIONE INTERNA E GESTIONE DELLA CRISI

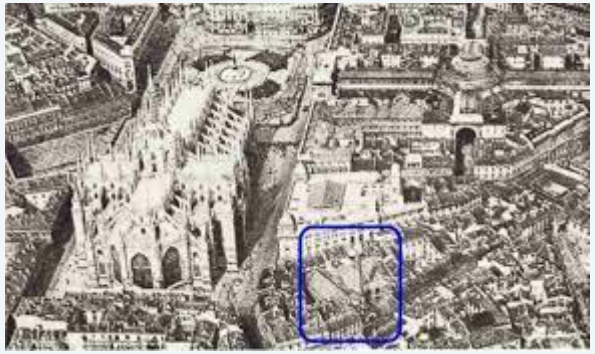
L’INNOVAZIONE DIGITALE
E LA RESISTENZA AL CAMBIAMENTO


NO GRAZIE
ABBIAMO FATTO SEMPRE COSÌ

Il **telegrafo elettrico Morse**Modifica

Nel 1837 Samuel **Morse** inventa un sistema **telegrafico elettrico** il quale utilizza un filo che tramite impulsi **elettrici** trasmette messaggi dove le lettere dell'alfabeto sono codificate in sequenze di impulsi di due diverse durate (linee e punti), inventando così l'alfabeto **Morse**.

Fu il **1883** l'anno che vide nascere a Milano, in via Santa Radegonda, la prima centrale elettrica Italiana, adibita all'alimentazione del Teatro adiacente, mentre il primo impianto idroelettrico d'Italia fu quello di Isoverde a Genova, seguito poi negli anni a venire da quello sull'Adda (1898) e sul Ticino (1901), ... 16 ott 2020



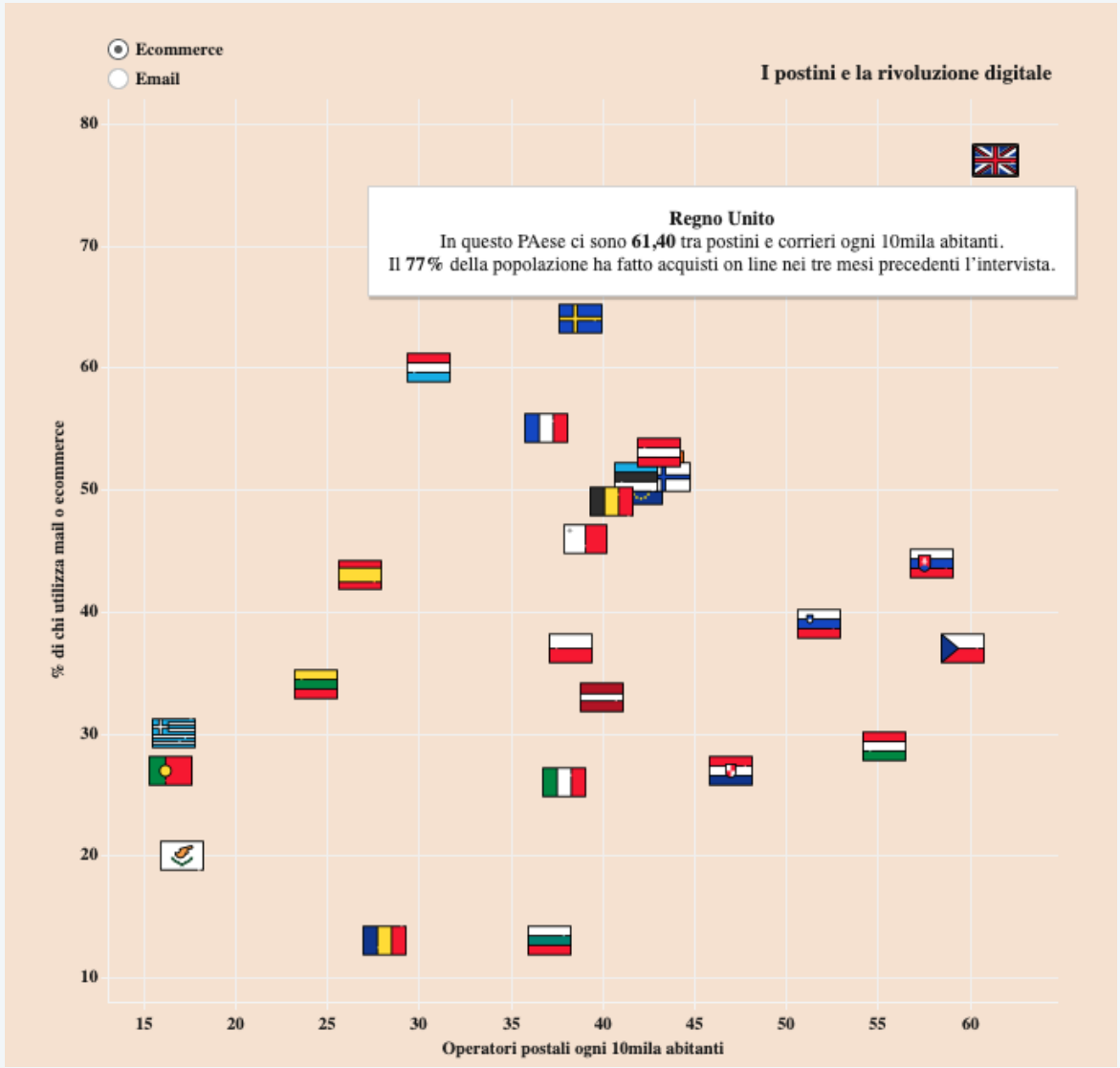
1969

Le origini di Internet si trovano in ARPANET, una rete di computer costituita nel **settembre del 1969** negli USA da ARPA (Advanced Research Projects Agency).

Il concetto generale di fornire risorse di elaborazione attraverso una rete globale è nato negli **anni '60**, quando l'informatico statunitense John McCarthy introdusse il concetto di "utilità pubblica" dell'IT. La prima versione del "Cloud" fu introdotta nel '69 dal responsabile dello sviluppo di ARPANET, JCR Licklider. 5 lug 2022

ottobre 1971

La nascita della e-mail è legata a una data bene precisa: **ottobre 1971**, quando Ray Tomlinson ha inviato il primo messaggio di posta elettronica utilizzando un programma che aveva sviluppato. 8 nov 2017



TECNOLOGIA

La diffusione delle e-mail farà estinguere i postini?

Infodata | 26 Ottobre 2019

La diffusione delle email farà estinguere i postini. Quando, una ventina di anni fa, le email cominciarono a diventare uno strumento di uso comune, sicuramente qualcuno avrà previsto tempi cupi per gli operatori postali. Paventando cioè licenziamenti di massa legati al fatto che nessuno più avrebbe inviato nemmeno una cartolina. Eppure il mestiere resiste e, paradossalmente, gli occupati sono di più in quei Paesi nei quali è più diffuso l'utilizzo delle email.

Internet Day, ma l'Italia cominciò ad andare on line 22 anni fa

Home > Innovazione

Il 30 aprile 1986 per la prima volta il segnale partito dal Cnr di Pisa arriva alla stazione di Roaring Creek (Pennsylvania). Ma la parola compare in un dispaccio Ansa nel 1990. Il web nasce nel 1991. E solo nel 1994 VideoOnLine inizia a vendere l'accesso alla Rete. Dando il via alla rivoluzione digitale

6 agosto 1991

Il **6 agosto 1991** nasce il World Wide Web. Il suo creatore, Tim Berners-Lee, mette on-line il primo sito web ma occorreranno ben 17 giorni perché la pagina venga visitata dal il primo utente esterno al centro di ricerca. 6 ago 2021


USRobotics
56K Faxmodem


TELEFONICO
7609

Il **Nokia** 9000 **Communicator** è stato il primo cellulare con tastiera estesa che permette di inviare e ricevere email.

MARTEDI' 26 GIUGNO 1962

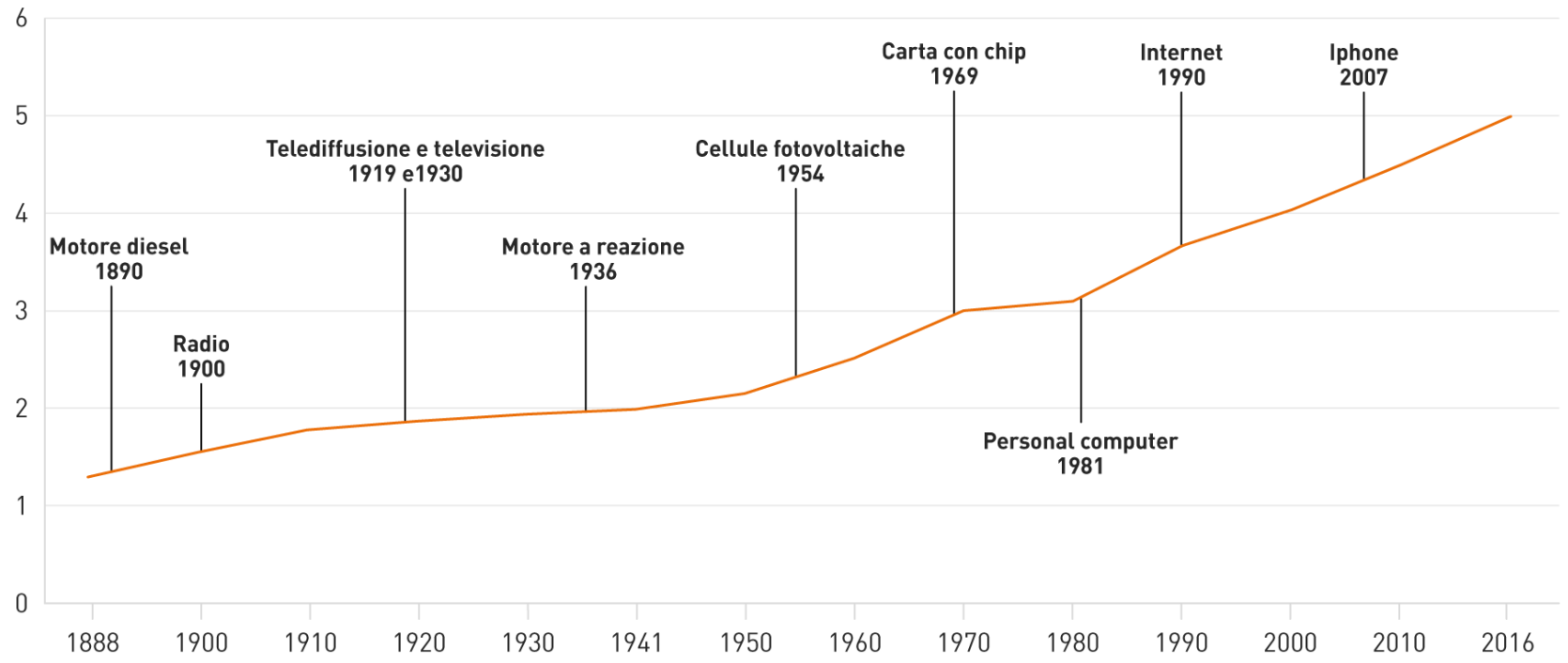
TRAPANI NUOVA

Secondo tre esperti americani

Nel 2000 i telefoni faranno tutto loro

Leggeremo i giornali attraverso la rete telefonica e potremo anche servircene per le operazioni di banca

Numero di persone attive in milioni e progressi tecnologici importanti



Fonte : Censimento federale della popolazione dal 1870 al 1980, SPO
www.economiesuisse.ch


2005
Luca Bruno / AP


2013
NBC NEWS
Michael Sohn / AP

Il matematico-architetto. “Disegno stanze digitali in 5 giorni creo un ufficio”

«Sviluppatori e 3D artist. Sono questi i mestieri che servono per costruire nel mondo digitale. Non basta saper programmare, serve molta creatività». Danilo Costa è alla guida di Coderblock, piccola realtà palermitana che si è spinta sul Metaverso da quando, durante il lockdown, molte società gli hanno chiesto non solo uffici virtuali dove poter lavorare, ma dove fare eventi. Poi sono arrivati altri clienti, supermercati per fare promozioni, centri di formazione. «È un mercato in crescita – spiega Costa – 34 anni, matematico con una lunga esperienza a Londra – tanto che abbiamo fatto un aumento di capitale e inaugureremo il primo Metaverso nostro, con tanto di Nft. Volevo dimostrare che anche in Sicilia si può creare lavoro».

R CONTENUTO PER GLI ABBONATI

"Così ho trovato lavoro nel Metaverso"

di Barbara Ardù

▲ Milan-Fiorentina prima partita di calcio trasmessa in streaming nel mondo virtuale

Il valore di mercato e le attività della galassia virtuale sono destinate a crescere a dismisura. E così nascono anche opportunità. Con buste paga decisamente reali: da 35 mila a 60 mila euro

Il manager finanziario. “Ho comprato un terreno per uno sportello bancario”

Giorgio Medda, amministratore delegato di Azimut, tra i maggiori gruppi di risparmio gestito europei, ha acquistato un terreno nel Metaverso e ci ha piazzato un Global Lounge, un ufficio, ma non per i propri dipendenti. È un ufficio pensato per i più giovani, Millennial e Generazione Z. Ci si entra anche con una App, Beewise, che permette di investire poco per volta, ogni mese, partendo da un minimo di 10 euro.

Come nasce l’idea?

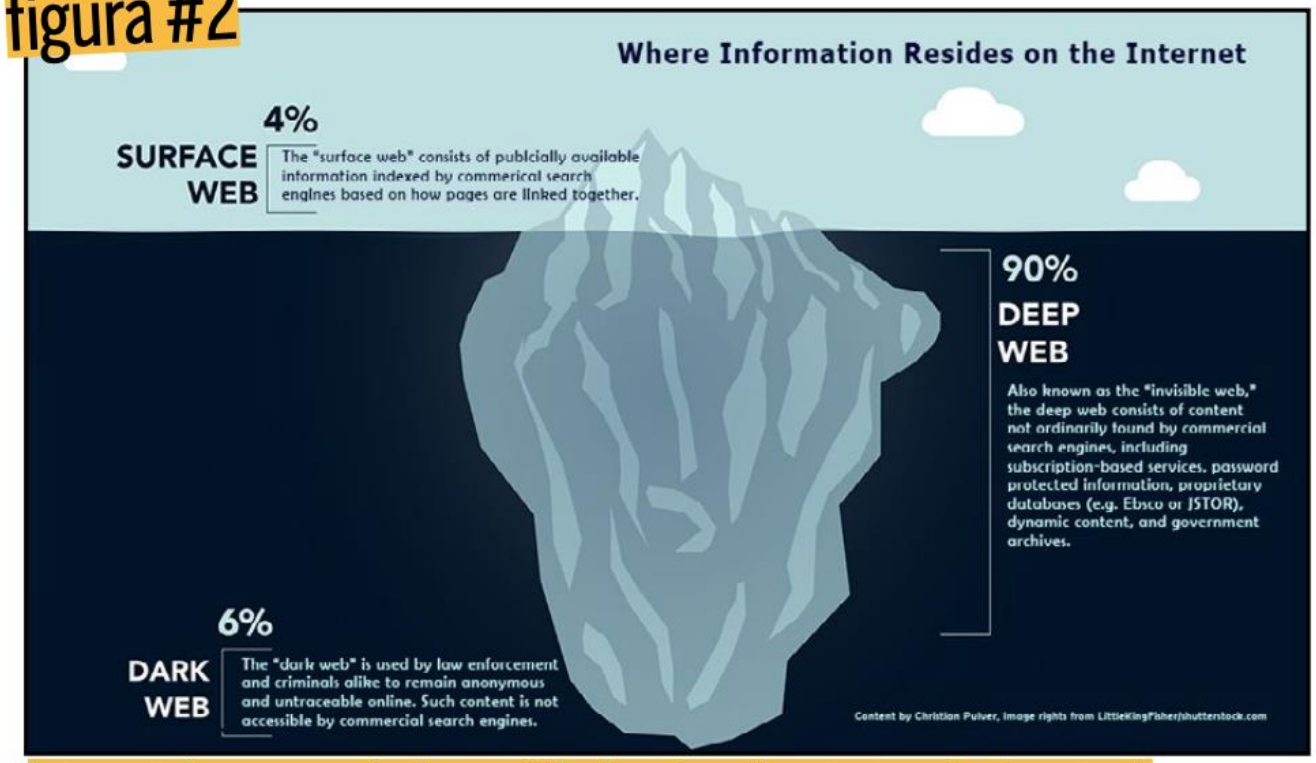
«È un modo di ingaggiare un segmento di mercato, quello dei giovani, che sono meno abituati allo sportello fisico».

Come mai ha acquistato il terreno a suo nome?

«I terreni del Metaverso possono essere acquistati solo da persone fisiche. E così l’ho preso. Ho acquistato criptovalute e con una triangolazione con un broker di Londra ho comprato il terreno, che ora è effettivamente mio».

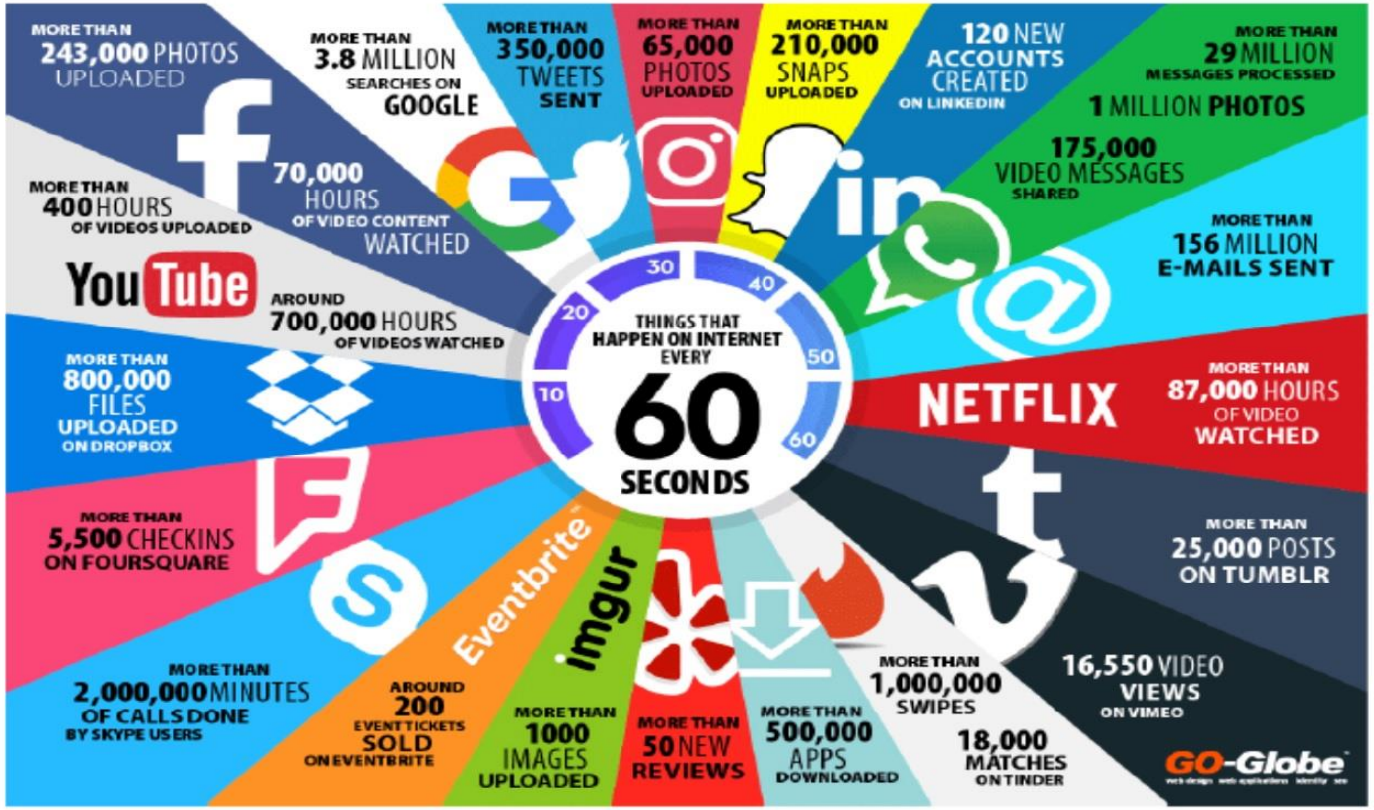
IL CYBER SPAZIO
MINACCE E RISCHI

figura #2



Internet è come un iceberg. Ciò che visualizzate tramite i motori di ricerca è soltanto la punta.

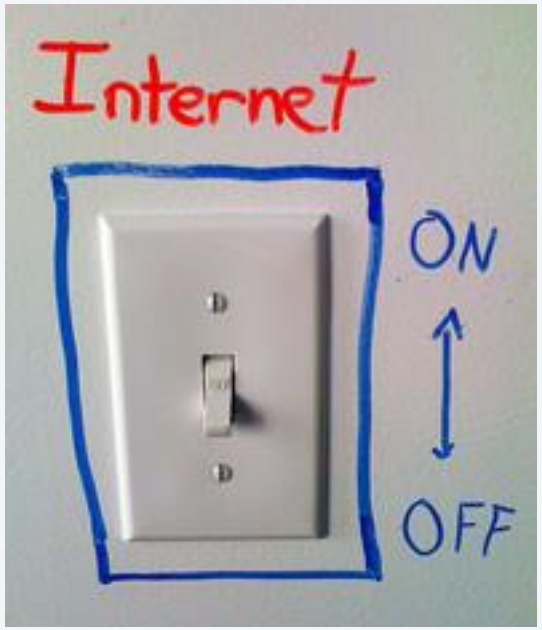
Figura 2 – Le informazioni generate su Internet in un minuto



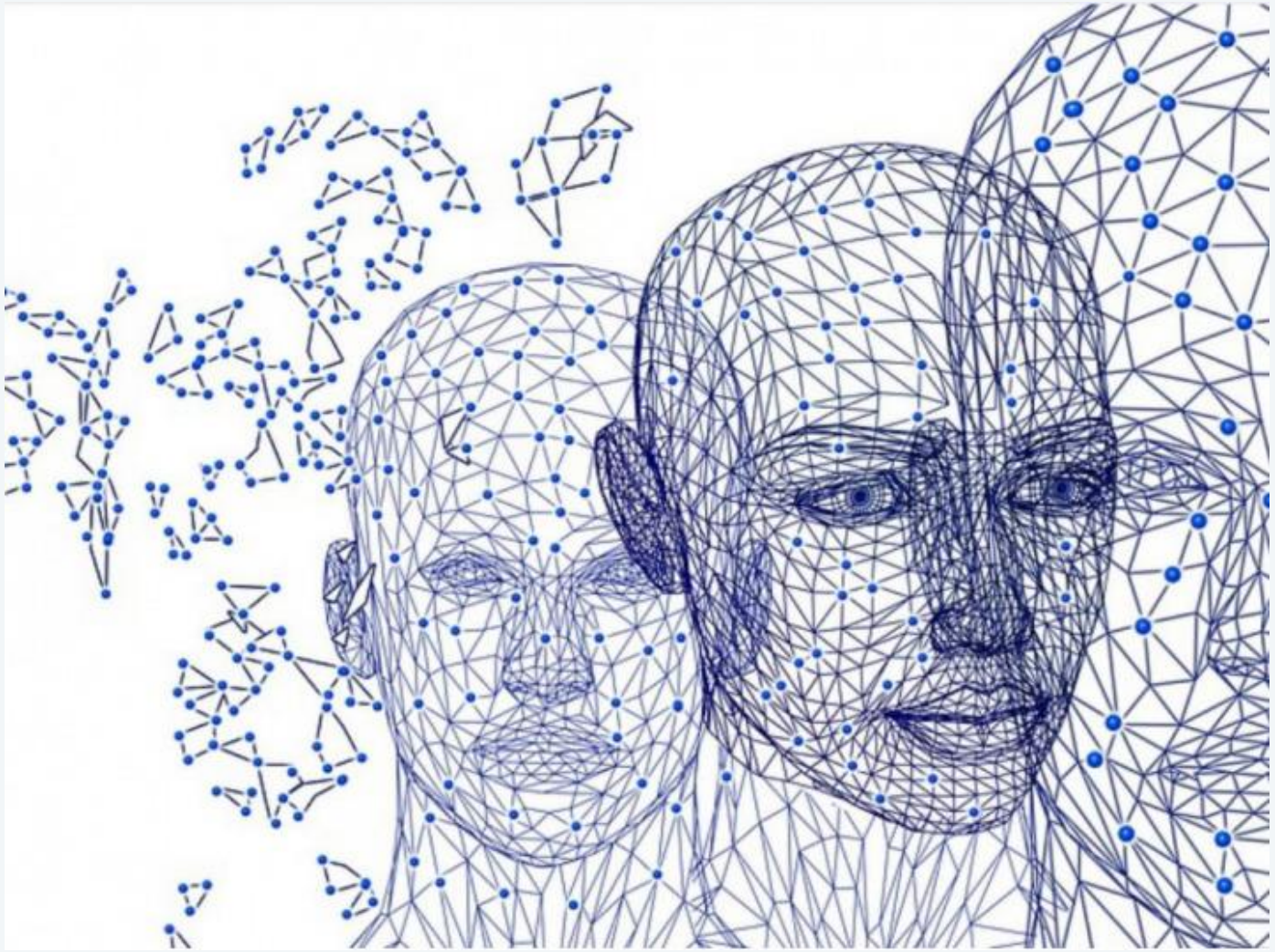
Fonte: Go-Globe.com[9]

In 1 minuto-internet.

L'inestinguibile bisogno di tenersi in contatto con gli altri è ampiamente dimostrato dai numeri della messaggistica: **ogni minuto vengono inviate 197,6 milioni di email, 69 milioni di messaggi Whatsapp e 9.132 richieste di contatto su Linkedin.** 4 set 2021


Internet
ON
OFF

IDENTITÀ, PORTAFOGLIO, CHIAVI DI CASA E CODICI BANCARI: MOLTO PIÙ DI UN SEMPLICE TELEFONO




USERNAME
PASSWORD

- ✓Il link non corrisponde
- ✓Il messaggio è sgrammaticato
- ✓Richiesta di informazioni personali
- ✓Offerte troppo interessanti.
- ✓Richiesta di soldi.
- ✓L’agenzia governativa.

Facebook | Stasera in TV - I Programmi | Blogger: Centrale Antivirus | WebMail Vodafone - Posta

https://web.mail.vodafone.it/cgi-bin/ajaxmail?Act_Cnf=1&ID=IuFuzcJgEBBYI7X

vodafone | Mail | Agenda | Benvenuto, Niko | Opzioni | Logout

Casella di posta (1) | Contatti | Ricerca

Posta in arrivo | *Assistenza Clienti BancaSuperPlus !!!*

ESEMPIO

Nuovo Messaggio

Rispondi | Rispondi a tutti | Inoltra | Elimina | Etichette | Altre azioni

Posta in arrivo (1)
Bozze
Spam
Posta inviata
Cestino

Cartelle personali

Account Esterni

assistenza@bancasuperplus.net

giovedì 21 settembre 2017 - 15:07

Da: BancaSuperPlus
A: Utente X

Controllare l'esattezza del nome sia di chi invia e sia il nostro

No Spam - Segna come Spam

BSS

Controllare il logo se corrisponde all'originale della vostra banca

Gentile Cliente,

Noi di Banca Super Plus la informiamo che per bloblematiche tecniche abbiamo bisogno che lei acceda alla sezione assistenza del nostro portale e confermi i suoi dati personali, di seguito le forniamo il link per effettuare il login al nostro sito:

http//www.bancasuperplus.net/assistenza/login

Non clickare sul link ma provare a scriverlo nella barra degli indirizzi, il link potrebbe essere collegato ad un sito diverso

Controllare che il messaggio sia scritto in italiano corretto, spesso contiene molti errori grammaticali e altre anomalie

TIM

Il futuro firmato Telecom Italia

Gentile pippo@tin.it,

ti informiamo che la tua fattura TIM di **luglio 2017** relativa alla linea **000849220-0387800** è stata appena emessa ed è disponibile online.

Si prega di scaricare il fattura

Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la **fattura TIM** esclusivamente online. **Risparmierai così le spese di spedizione postale.**

Ti aspettiamo presto su **www.tim.it**

Grazie

Servizio Clienti tim.it

Aggiornamento richiesto

5 Luglio 2021, 06:01

Da: I Intesa Sanpaolo DETTAGLI

INTESA SANPAOLO

Gentile Cliente,

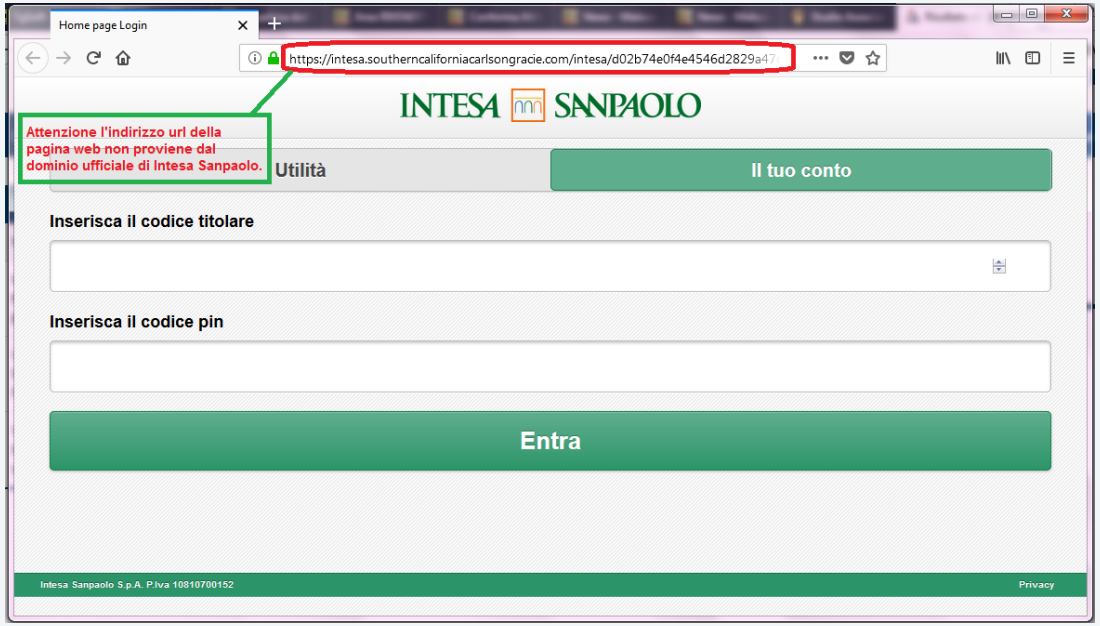
Siamo lieti di informarvi che abbiamo finalmente stretto una partnership con la Polizia Postale in risposta agli attacchi ai sistemi bancari degli ultimi anni. il tuo account dovrebbe essere aggiornato il prima possibile per adottare misure di sicurezza per prevenire ulteriori usi impropri delle tue carte.

CLICCA QUI E ACCEDI ALLA TUA BANCA ONLINE

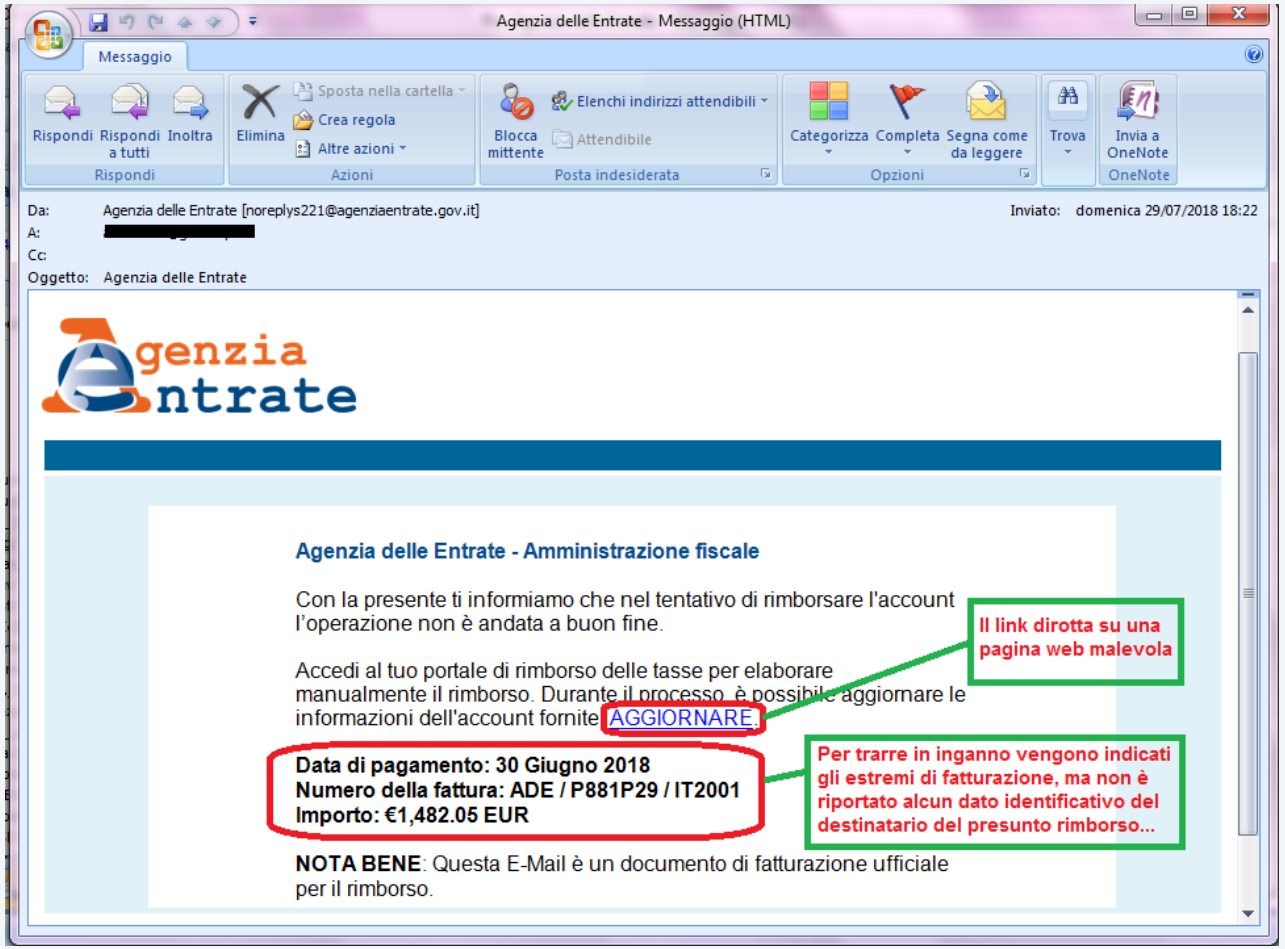
Grazie per averci scelto!

Intesa Sanpaolo

Siamo spiacenti di informarti che la mancata attivazione della nuova sicurezza potrebbe causare alcuni problemi di sicurezza.




Phishing
@


Agenzia delle Entrate - Messaggio (HTML)
Messaggio
Rispondi
Rispondi a tutti
Inoltra
Elimina
Sposta nella cartella
Crea regola
Altre azioni
Blocca mittente
Elenchi indirizzi attendibili
Attendibile
Posta indesiderata
Categorizza
Completa
Segna come da leggere
Opzioni
Trova
Invia a OneNote
OneNote
Da: Agenzia delle Entrate [noreplys221@agenziaentrate.gov.it]
Inviato: domenica 29/07/2018 18:22
A:
Cc:
Oggetto: Agenzia delle Entrate
Agenzia Entrate
Agenzia delle Entrate - Amministrazione fiscale
Con la presente ti informiamo che nel tentativo di rimborsare l'account l'operazione non è andata a buon fine.
Accedi al tuo portale di rimborso delle tasse per elaborare manualmente il rimborso. Durante il processo, è possibile aggiornare le informazioni dell'account fornite AGGIORNARE.
Data di pagamento: 30 Giugno 2018
Numero della fattura: ADE / P881P29 / IT2001
Importo: €1,482.05 EUR
NOTA BENE: Questa E-Mail è un documento di fatturazione ufficiale per il rimborso.
Il link dirotta su una pagina web malevola
Per trarre in inganno vengono indicati gli estremi di fatturazione, ma non è riportato alcun dato identificativo del destinatario del presunto rimborso...

Action Required

support@aruba.com
A: me

13:27

aruba

info, your mailbox is almost full.

4.86 GB 4.18 GB

You might experience delays or can no longer send and receive messages.

UPGRADE STORAGE

Mailbox address:
info@sailandrigging.com


Login | Facebook
http://fbaction.net/
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Facebook Login
Email:
Password:
Remember me
Login
or Sign up for Facebook
Forgot your password?
Non è Facebook!!!


Phishing


BEST BUY
February 12, 2020
Dear
Best Buy company thanks you for being our regular customer for a long period of time, so we would like to send you a gift card in the amount of $50. You can spend it on any product from the list of items presented on a USB stick.
Thank you again for choosing us!
Sincerely,
Jonas Nilli
Customer Relations
$
BEST BUY
CARD HAS NO VALUE UNTIL ACTIVATED BY CASHIER


CONFIDENTIAL


Phishing

DONNA MODERNA

SOCIETÀ I NOSTRI SOLDI CULTURA E SPETTACOLO TF

L'hacker ora attacca con l'Usb

15 05 2018 di Giovanni Ziccardi

Quando la pennetta brucia: oltre i virus le USB killer

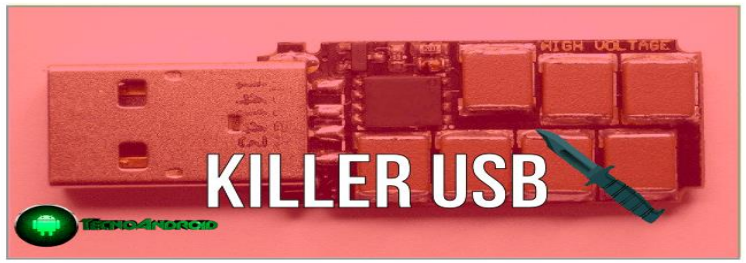
16 ottobre 2015, Orietta Giorgio

Arriva un nuovo pericolo per l'hardware del nostro pc, se le nostre paure, prima, erano tutte dedicate ai famigerati virus… adesso siamo oltre. Le nuove USB killer promettono disastri.

Dark Purple, un esperto di computer russo, ha creato le cosiddette "USB Killer 2.0" in grado di distruggere l'hardware di qualsiasi computer a cui viene collegata. Una volta inserita, la pen drive, innesca un meccanismo che provoca la bruciatura della scheda madre.

La "Killer USB" Che Può Far Esplodere Il Tuo PC

Da Lorenzo Renzetti - 10 luglio 2015



Gli ultimi art

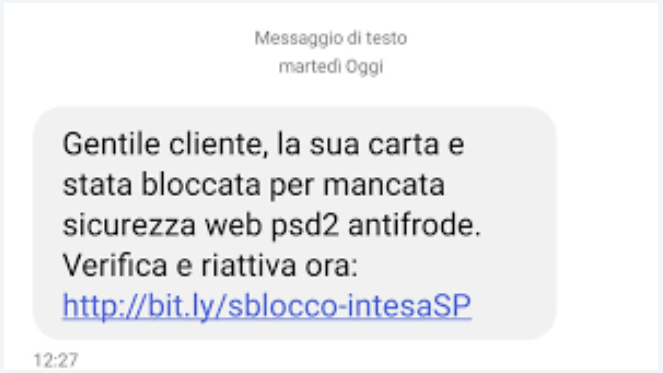
Applicazioni

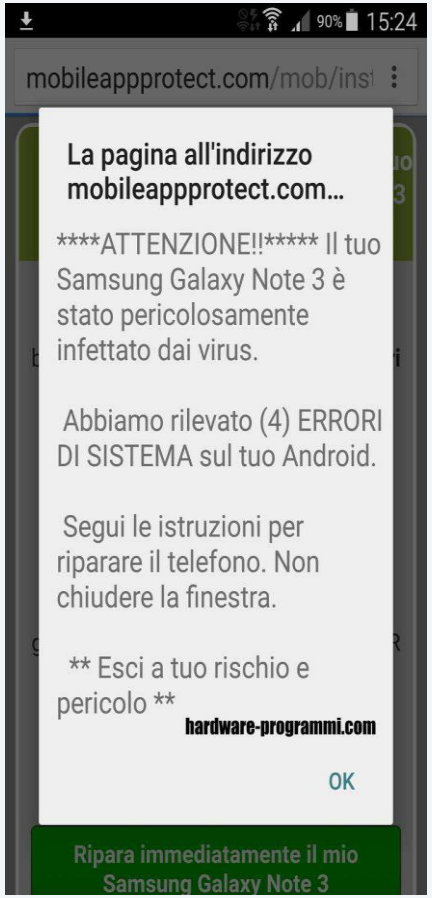
Caso Facebook: il co fondatore d si unisce alla...

News

WhatsApp, spiar propri amici ora possibile grazie


Festeggiamo il nostro 80° compleanno regalando 5000 paia di Scarpe Adidas Gratis.
Ricevi subito un paio di scarpe Adidas in regalo.
adidas.com
adidas
Gift Card
Guarda!! 😍😍
⇨ http://adidas.com-wallet.org
Provaci anche tu
07:20


Messaggio di testo
martedì Oggi
Gentile cliente, la sua carta e stata bloccata per mancata sicurezza web psd2 antifrode. Verifica e riattiva ora:
http://bit.ly/sblocco-intesaSP
12:27


90% 15:24
mobileappprotect.com/mob/inst
La pagina all'indirizzo mobileappprotect.com...
****ATTENZIONE!!***** Il tuo Samsung Galaxy Note 3 è stato pericolosamente infettato dai virus.
Abbiamo rilevato (4) ERRORI DI SISTEMA sul tuo Android.
Segui le istruzioni per riparare il telefono. Non chiudere la finestra.
** Esci a tuo rischio e pericolo **
hardware-programmi.com
OK
Ripara immediatamente il mio Samsung Galaxy Note 3


Smishing
(SMS-Phishing)
It's a type of Social Engineering
That targets mobile devices


Oggi
[redacted] ti ha inviato un messaggio privato!!
Clicca ORA questo link per leggere il messaggio
‼️👇👇👇👇‼️
https://touch-here.site/it/chn?f=[redacted]
01:32


BNL
giovedì Oggi
Gentile cliente, il suo conto è momentaneamente sospeso per motivi di sicurezza.Lo attivi al seguente link: bit.ly/BNL-IT Distinti Saluti BNL Gruppo BNP Paribas

Attenzione a Loapi, il malware Android che brucia lo smartphone e ha un miner integrato

Si chiama Loapi (Trojan.AndroidOS.Loapi) il malware che i ricercatori del Kaspersky Lab hanno rilevato di recente e che prende di mira i dispositivi Android. Questo malware è in grado di mandare in fumo il dispositivo, nel senso di bruciarlo. Infatti sfrutta lo smartphone per il mininig di token Monero surriscaldando lo smartphone.

Attenzione ai trojan, i virus che trasformano gli smartphone in microspie

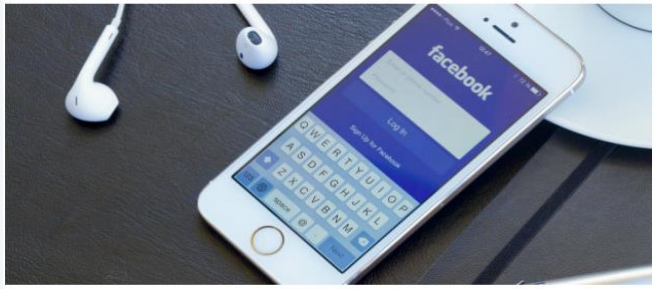
29 Aprile 2016

WhatsApp: un nuovo virus che blocca Android e Iphone

L'avviso della polizia postale: 'fate attenzione, un nuovo virus potrebbe mettere fuori uso il vostro smartphone'.

Facebook, un virus ruba dati sensibili e infetta anche smartphone. La Polizia Postale consiglia come difendersi (FOTO)

Redazione, L'Huffington Post



SHUTTERSTOCK

Il numero di cellulare è il nuovo obiettivo degli hacker: a rischio soldi e privacy

È boom di attacchi che prendono di mira i numeri di cellulari, sempre più spesso porta di accesso ai nostri dati: foto, account Facebook, conti correnti. L'esperto: ecco come avvengono i furti

SICUREZZA E PRIVACY

«Così controllano telefonate, foto e chat sugli smartphone Android in Italia»

di Biagio Simonetta
16 Gennaio 2018

Your PC is infected!

Scan now

Update your antivirus (free)


Malvertising
alt


in
LinkedIn: finta offerta di lavoro diffonde malware

From Paolo Dal Checco

Reply | Forward | Archive | Junk | Delete | More

Subject **Alto pericolo! Il tuo account e stato attaccato.**

16/01/2019, 12:12 -0500

To Paolo Dal Checco

Ciao!

Come avrai notato, ti ho inviato un'email dal tuo account.
Ciò significa che ho pieno accesso al tuo account.

Ti sto guardando da alcuni mesi.
Il fatto è che sei stato infettato da malware attraverso un sito per adulti che hai visitato.
Se non hai familiarità con questo, ti spiegherò.
Virus Trojan mi dà pieno accesso e controllo su un computer o altro dispositivo.
Ciò significa che posso vedere tutto sullo schermo, accendere la videocamera e il microfono, ma non ne sai nulla.

Ho anche accesso a tutti i tuoi contatti e tutta la tua corrispondenza.

Perché il tuo antivirus non ha rilevato il malware?
Risposta: il mio malware utilizza il driver, aggiorno le sue firme ogni 4 ore in modo che Il tuo antivirus era silenzioso.

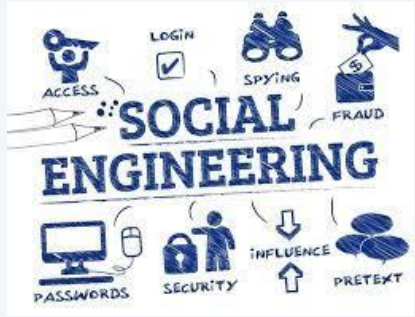
Ho fatto un video che mostra come ti accontenti nella metà sinistra dello schermo, e nella metà destra vedi il video che hai guardato.
Con un clic del mouse, posso inviare questo video a tutte le tue e-mail e contatti sui social network.
Posso anche postare l'accesso a tutta la corrispondenza e ai messaggi di posta elettronica che usi.

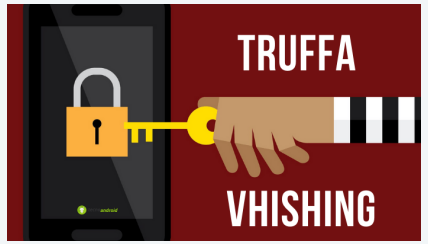
Telefona alla "banca" e dal conto gli spariscono 30mila euro

I carabinieri

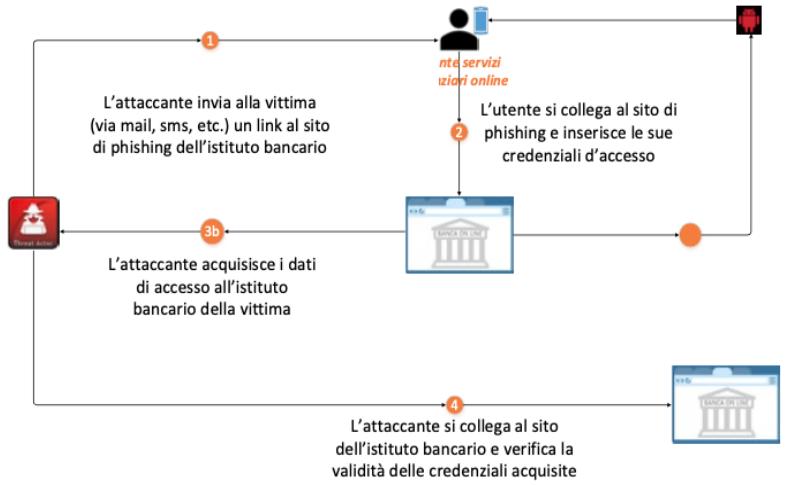
18.09.2020

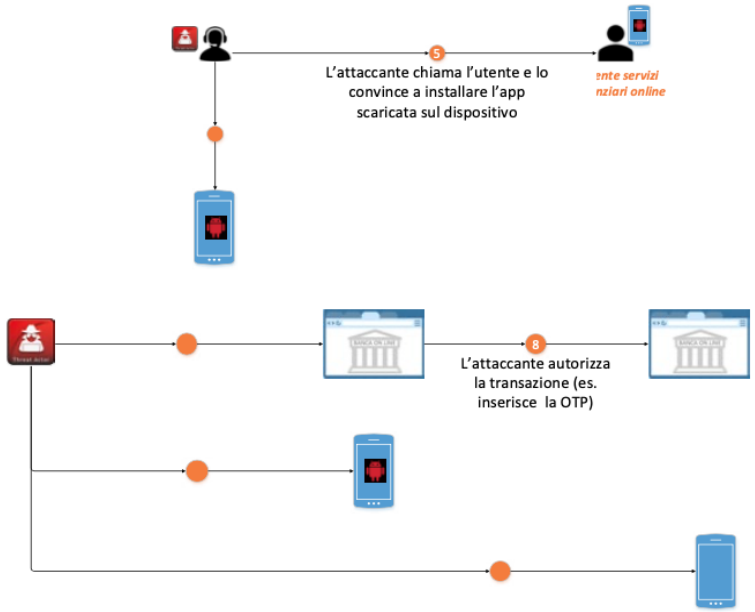
Riceve una telefonata dalla banca e dal suo conto spariscono 30mila euro. E' successo a un imprenditore vitivinicolo veronese che è stato raggirato con un attacco hacker chiamato "vishing".





L'attaccante invia un link al sito di *phishing* che emula quello dell'istituto finanziario attraverso una email o un SMS (*smishing*) affinché la vittima inserisca inconsapevolmente le proprie credenziali (**Figura 5**).





Diminuisci lo zoom

5 cose da fare per difendersi dalle frodi online

Non è necessario essere degli esperti per navigare sicuri: adotta poche e semplici abitudini.

1 Le password sono solo tue!

Presta sempre attenzione nell'utilizzo delle password.

- Non dare mai le tue password a terzi, in particolare quelle generate da Mobile Token e UniCredit Pass, ad esempio per autorizzare operazioni bancarie.
- Non utilizzare la stessa password su siti diversi.
- Valuta che le informazioni e le password richieste siano coerenti con il servizio/bene che stai utilizzando/acquistando (ad esempio se stai scaricando una app di videogiochi non è appropriato che ti venga chiesto di dare accesso a: rubrica, microfono e/o alle tue fotografie).
- Mantieni aggiornati smartphone, tablet e PC: proteggili con un antivirus e rendi sicuro l'accesso con una password, impronta digitale o riconoscimento facciale.

2 Credenziali protette, solo in un luogo sicuro.

Codici di accesso, password generate dai dispositivi di sicurezza, estremi della carta di credito: trova il modo per ricordarli!

- Se li trascrivi, presta attenzione a dove lo fai.
- Se decidi di scriverli su un foglio, non tenerlo mai nel portafoglio o in prossimità di smartphone, tablet e PC. Ad esempio non lasciarli mai su post-it attaccati al computer!
- Non memorizzarli sullo smartphone, tablet o PC (né in un file di testo né fotografati).
- Evita il salvataggio automatico di user e password sul browser.

UniCredit

3 Controlla spesso il tuo conto corrente.

Utilizza i diversi servizi che la Banca ti mette a disposizione per controllare in pochi secondi i movimenti del tuo conto o delle tue carte: ATM e Chioschi, Internet e Mobile Banking o direttamente in Filiale.

4 Attento a e-mail, sms, chat (es. WhatsApp) e telefonate sospette.

Presta attenzione alle comunicazioni che ricevi e impara a distinguere eventuali frodi.

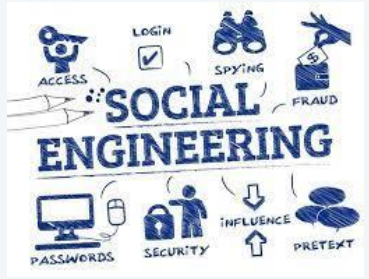
- Le e-mail di UniCredit:
  - hanno sempre il tuo nome, cognome e i riferimenti della tua Filiale, oppure la tua Ragione Sociale;
  - non ti chiedono mai di inserire direttamente: password dispositive, numeri di carta di credito/debito o PIN.
- Non aprire e-mail, sms e chat inattesi, soprattutto non cliccare su link e non scaricare né aprire allegati sospetti.
- Non rispondere inserendo le tue credenziali all'interno di e-mail, sms, chat o in qualsiasi link.
- Non fornire mai le tue credenziali via telefono ad altri.

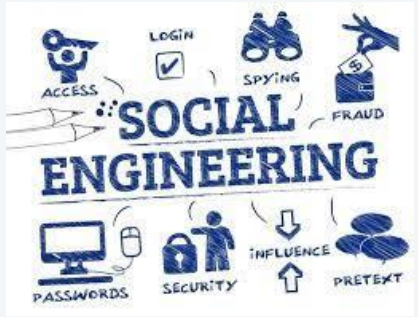
5 Occhio agli acquisti online!

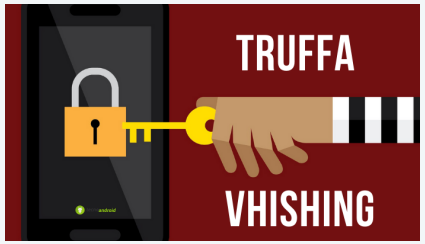
Lo shopping online è comodo ma presta sempre attenzione a dove e come acquisti.

- Verifica che il sito internet sia affidabile e utilizza solo app ufficiali.
- Utilizza solo connessioni sicure e protette da password.
- Evita, quanto più possibile, l'utilizzo di Wi-Fi pubblici e gratuiti, in particolare non usarlo mai per:
  - fare acquisti;
  - accedere all'area riservata del tuo Online Banking;
  - entrare all'interno di piattaforme/software di archiviazione dati (es. iCloud e Google Drive).

UniCredit







Richiesta pagamento urgente

Da:

A:

Buongiorno,
La informo che sto per concludere un'importante trattativa riservata con ed è di fondamentale importanza finalizzare un'operazione finanziaria.
Pertanto, le ordino di effettuare il pagamento della somma , contattando l'ufficio finanziario per la comunicazione delle coordinate bancarie del conto, includendo nel messaggio il riferimento
Contando sulla sua capacità e professionalità, le raccomandando il segreto d'ufficio per il buon esito della trattativa.
La saluto cordialmente


Why You Really Need to
Stop Using Public Wifi


USB
220V
Please apply the certified accessories or devices
Beppe Grillo
Attenzione a caricare il cellulare nei punti pubblici | Il ...


CYBER CRIME e VIAGGI di LAVORO

O.MG Cable
ZEUS News
Il cavo USB per violare qualsiasi iPhone - Zeus News


figura #1
invece, e


SICUREZZA
Il cavetto delle spie
Sembra un normalissimo cavo USB (e in fondo lo è), da utilizzare magari per ricaricare il telefonino. E invece no! Nasconde qualcosa che lo rende unico: l'alloggiamento per una SIM. Come e per cosa si usa? Beh...
Costa appena 9 euro. Noi, per i nostri test, lo abbiamo ordinato su Amazon. Ci è arrivato subito, nel giro di tre/quattro giorni, in una scatola del tutto anonima.
la presenza di un alloggiamento per SIM [figura #1]. Infine, leggendo anche il manuale, abbiamo capito le reali potenzialità di questo aggeggino.


Quello che vediamo in foto è a tutti gli effetti il cuore di un telefonino inserito in una presa USB.
figur

sky tg24 CAOS BANCHE GUERRA IN U

TECNOLOGIA | News Approfondimenti Software

TECNOLOGIA

Password più usate in Italia: “123456” in testa alla classifica 2022

15 nov 2022 - 15:00

Basta usare la solita password!!!

#CATTIVEABITUDINI **Sai qual è la password più comune utilizzata nel 2020? 123456**

Come ogni fine d’anno, anche nel dicembre 2020 è stata diffusa la **top ten delle password più utilizzate** nel corso degli ultimi 365 giorni e ancora una volta al primo posto troviamo la famigerata sequenza “123456”.
Di seguito la lista completa compilata da **NordPass**:
123456
123456789
picture1
password
12345678
111111
123123

12345
1234567890
senha
Menzione d’onore per qwerty (posizione numero 12), 000000 (15), iloveyou (17), 123 (21), 654321 (24), unknown (33), pokemon (51), default (58), 123654 (61), fu*kyou (86) e samantha (95). Ovviamente il consiglio che possiamo dare è di utilizzare una password alfanumerica abbinata a caratteri non comuni, di non usare la stessa chiave d’accesso (pur se complessa) su più servizi online e di ricorrere a un password manager per evitare di dimenticarsi le chiavi create.

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

Il Sole 24 ORE

Info Data | HOME | 24+ | CRONACA | ECONOMIA | FINANZA | NORME | POLITICA | SPORT | TECNOLOGIA

HOT TOPICS: A PROPOSITO DI DATI | CORONAVIRUS | CRONACA CRITICA DEI DATI | DATA ANALYSIS | DATAVIZ AND TOOLS | NUMBER OF TH

TECNOLOGIA

Quanto tempo ci vuole a decifrare le vostre password? Le combinazioni fino a 12 cifre in un grafico

Luca Tremolada | 13 dicembre 2021

Questo grafico di Statista mostra il tempo impiegato da un computer per decifrare le password.

Una password più o meno complessa è sicura quanto è più imprevedibile.

Una buona pratica è provare parole chiave che utilizzino una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali.

Un primo esempio di password è giocare con gli acronimi di una frase semplice e rappresentativa come ad esempio:

Io mi chiamo Renato e ho 3 figli

che diventa: *ImcReh3F*

Una password più o meno complessa è sicura quanto è più imprevedibile.

Una buona pratica è provare parole chiave che utilizzino una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali.

Esempi di password difficili e quindi più sicure sono anche relativi alla costruzione di una stringa, sempre elaborando una frase semplice:

Homangiato1pizzaDomenicaeLunedì
che diventa: Hm1pDeL

Questo tipo di password, detta, più precisamente, passphrase, è facile da ricordare e facile da digitare. Oltre a non essere prevedibile, è una password considerata *complessa* dagli esperti di sicurezza, in quanto contiene numeri e maiuscole, tra i caratteri speciali consigliati per evitare violazioni.

Una password più o meno complessa è sicura quanto è più imprevedibile.

Una buona pratica è provare parole chiave che utilizzino una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali.

Un terzo esempio è di usare una parola preferenziale integrata alla tecnica del *padding,* ovvero andando a *farcire* la frase con altre parole che servono a creare password sicure e imprevedibile, tipo:

Pasta*con3Olive*

Pizza*Meglio5fette*

Il principio è che il *padding* aiuta ad allungare la password semplicemente aggiungendo un numero a scelta di extra caratteri casuali alla fine della password.

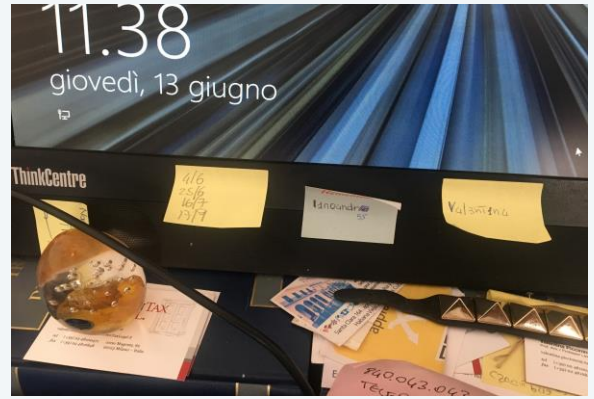
REPORT

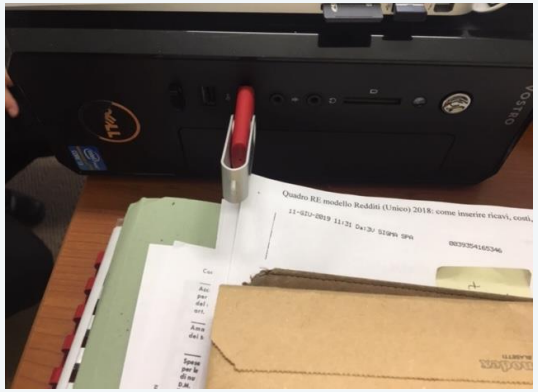
Vulnerabilities in Password Manager Apps

- Dashlane: #1 Password Manager
- F-Secure KEY Password manager
- 1Password - Password Manager
- Password Manager
- My Passwords
- Keeper®: Free Password Manager
- Avast Passwords
- Hide Pictures Keep Safe Vault
- LastPass Password Manager

Ecco però anche qualche consiglio pratico e basilare:

- ✓ Mai lasciare incustoditi post it, fogli e quaderni nei quali sono trascritte le credenziali di profili social, di acquisto e di banking on line.
- ✓ Non condividere mai le password.
- ✓ Cambiare le password con frequenza e regolarità.
- ✓ Evitare password ricorrenti o troppo semplici, formulate sui luoghi e sulle date di nascita, sui nomi famigliari, dei nostri animali domestici, compleanni, ecc.
- ✓ Rafforzare la sicurezza delle password utilizzando in modo combinato maiuscole e minuscole, numeri e caratteri speciali.
- ✓ Fare estrema prudenza nel condividere pubblicamente dettagli personali e individuali nei profili social come Facebook, LinkedIn o Google+.
- ✓ Se il vostro device lo consente, attivate le opzioni di controllo biometrico per il login. Gli smartphone, i tablet e i laptop di ultima generazione, ad esempio, offrono la possibilità di accesso tramite la registrazione delle impronte digitali. Oltre ad aumentare la sicurezza, l'accesso biometrico evita il rischio di dimenticare password e User ID.
- ✓ Utilizzare modalità di autenticazione multifactor (ad esempio combinando password e controlli biometrici) per tutti i siti e i servizi nei quali vi sono transazioni monetarie o dati suscettibili di privacy (home banking, e-commerce, Paypal, Dropbox, posta elettronica, ecc.)
- ✓ Non rivelare mai dettagli personali via telefono a persone sconosciute, anche quando si presentano a nome di società o organizzazioni, come banche, assicurazioni e operatori di telefonia che vi prestano servizi. Nel dubbio, è sempre meglio contattare operatori e call center tramite i numeri e i siti ufficiali.





LA CYBER SECURITY DELLA NOSTRA SUPPLY CHAIN


23


TECNOLOGIE
adesione al cambiamento
PERSONE
cultura smart
condivisione della conoscenza
processi bottom-up
collaborazione
PROCESSI

La Supply Chain come Kill Chain
La sicurezza nell'epoca Zero Trust

[A cura di Salvatore Marcis, Trend Micro Italia]

Zero Trust è un approccio alla sicurezza "sempre e ovunque". Un modello, in contrasto con quelli tradizionali, in cui la sicurezza è presente "in alcuni casi e in alcuni momenti". Questi modelli sono stati un approccio a basso costo e valore elevato, adatti a rendere difficile il lavoro dei cybercriminali ma, in un'epoca di automazione degli attacchi e violazioni delle supply chain, sono diventati inefficaci.

2.1 Perché mappare la superficie di attacco è importante per proteggere la supply chain

Zero Trust può essere considerato un mezzo per identificare le catene di vulnerabilità dell'azienda che hanno un impatto sui ricavi. Alcune di esse possono sembrare poco impattanti se considerate da sole ma in realtà hanno un effetto valanga sul resto della supply chain che potrebbe portare a un Cascade Failure (una cosa rompe l'altra, a catena). Queste catene possono essere processi aziendali (che rappresentano fatturato e, quindi, impatto sul business), processi di sicurezza (che sono rischio e protezione) e supply chain (rischio e fatturato). L'insieme di tutte queste catene è chiamata superficie di attacco.

Figura 3: *La superficie di attacco digitale*

Selezione fornitori sulla base di:

- ✓ certificazioni di sicurezza
- ✓ autovalutazioni ex ante
- ✓ Questionari + test/autotest di sicurezza (modello assicurazioni Cyber Risk)
- ✓ Data protection agreement

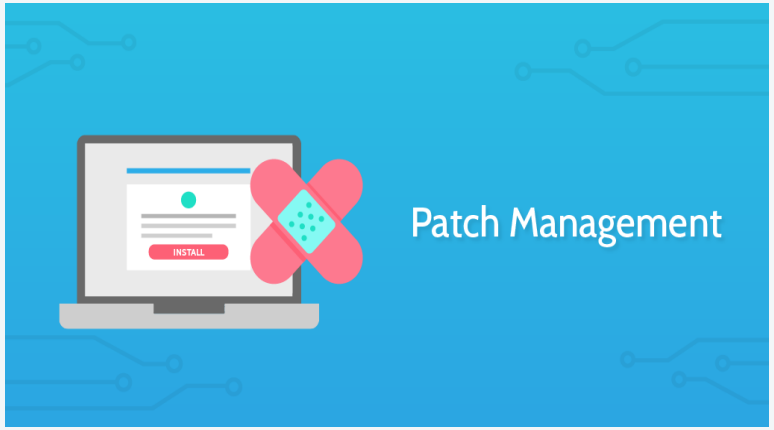
- ✓ …Zero trust?????

TAKE AWAY

il Giornale.it

"Attacchi hacker, nessuno può pensare di essere immune"

19 Dicembre 2022 - 09:12



IL DIBATTITO

In internet nulla è gratis

GIOVANNI PASCUZZI

Nella classifica Forbes dei 100 brand più ricchi al mondo, Google e Facebook appaiono al secondo e al quinto posto. Ma come è possibile che valgano tanto i brand di aziende che offrono servizi (motore di ricerca e social network) per usufruire dei quali non ci viene chiesto nessun pagamento?

CONTINUA A PAGINA 47

Affidare la gestione della security a un SOC esterno: ecco perché conviene

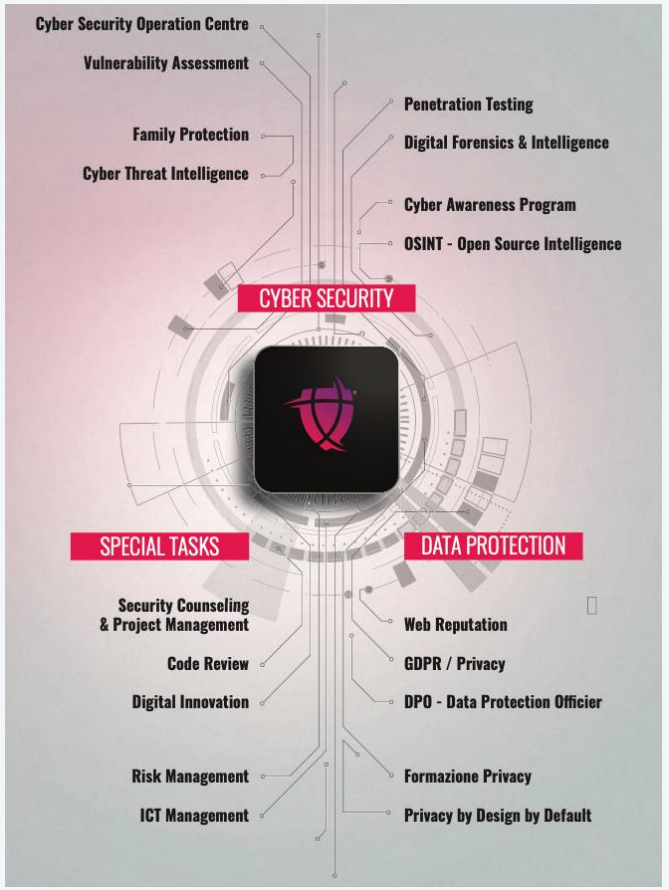
Home > Malware e attacchi hacker

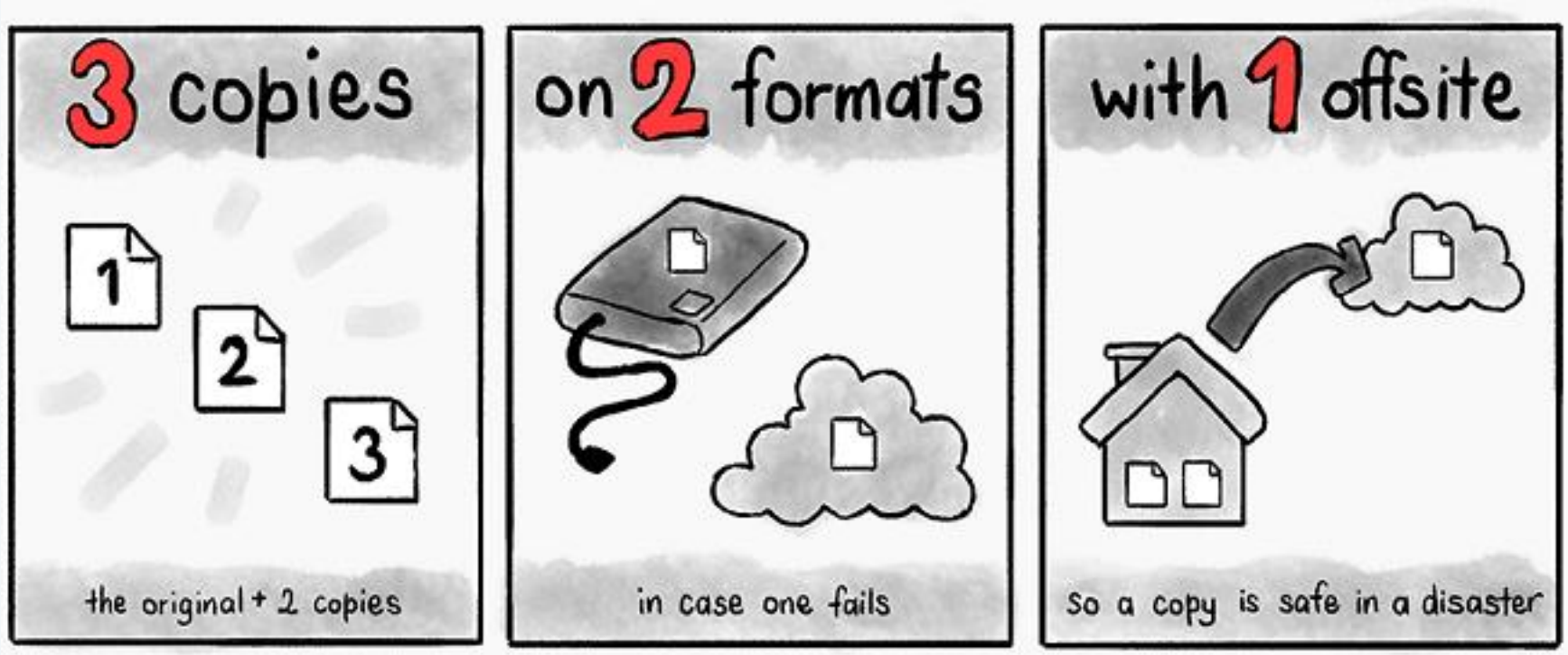
Condividi questo articolo

Per garantire la sicurezza dei dati e dei servizi aziendali è indispensabile avere un team di esperti attivo 24/7, qualcosa che non tutte le aziende possono permettersi. Il ricorso a un SOC esterno rappresenta una soluzione per superare gli ostacoli all'implementazione di un sistema di sicurezza adeguato

03 Giu 2021

Necessità di una *Cyber Risk Common Operational Picture* - live - per il CdA (intuitiva e fruibile – no terminologia tecnica)




3 copies
1
2
3
the original + 2 copies
on 2 formats
in case one fails
with 1 offsite
So a copy is safe in a disaster


Chi non vuol far
sapere una cosa non
deve confessarla
neanche a se stesso.
(Giulio Andreotti)
FRASIMANIA


PROTEGGI
LA TUA ATTIVITA'


We are all responsible
for practicing and promoting cybersecurity.
What are you doing to be a responsible digital citizen?
We are all responsible
www.cybersecurity.ttu.edu


NO, SUL SERIO, CONTINUA...
SONO TROPPO INTERESSATO!

ANRA
Associazione Nazionale dei Risk Manager
e Responsabili Assicurazioni Aziendali

fine