Il valore dei nostri **dati personali**

Roma, 22 gennaio 2020

ing. Giuseppe G. Zorzino
DPO, UNI11697, ERMCP, CISA, CISM, CGEIT, CRISC, LA27001, ...

Bio

Giuseppe Giovanni Zorzino

Consulente e docente di sicurezza delle informazioni, attualmente mi occupo di cyberstrategies, sistemi di gestione della sicurezza, governance e sicurezza delle informazioni nelle organizzazioni, privacy, compliance e awareness.

38+ anni di esperienza nell'IT e nell'analisi e sviluppo di basi di dati complesse.

20+ nell'IT security.

Accademia di Pozzuoli, Ufficiale del Corpo del Genio dell'A.M.,
Cybersecurity coordinator del CESMA (Centro Studi Militari Aeronautici) "Giulio Douhet".

Membro della Comm. Sicurezza Informatica dell'Ordine degli Ingegneri di Roma, nonché di ISACA, ERAcademy, ISACA Rome Chapter, UNIDPO, ISC2 Italian Chapter, HERMES University

Vasta attività di divulgazione e formazione c/o enti pubblici e PMI.

2 brevetti.

Varie certificazioni attive: UNI11697, ERMCP, CISA, CISM, CGEIT, CRISC, Security+, Lead Auditor ISO 27001, CMMI appr, MCSASec 2003, Certificatore etico, IBM Cert Solution Architect, IBM_Cert_Specialist, …

Obiettivi della conferenza

Al termine della conferenza i partecipanti saranno in grado di comprendere:

- quali sono i dati personali
- quando vengono diffusi (dove gli altri li possono trovare)
- quali sono i diritti e come si possono esercitare
- cosa fare per ridurre l'esposizione ai rischi

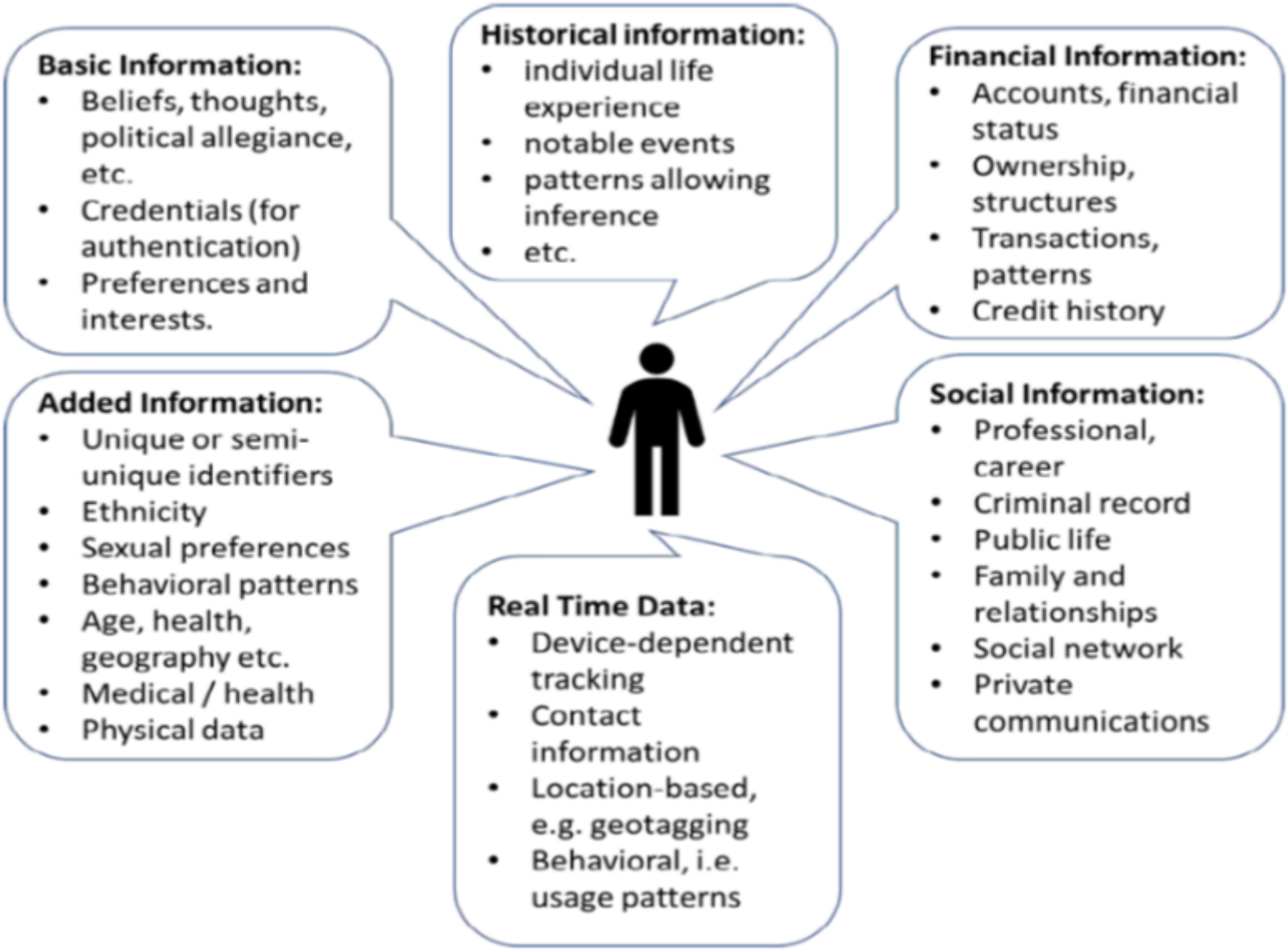
PREREQUISITI
Non sono richiesti prerequisiti specifici.

Quali sono i dati personali?

nome cognome	codice fiscale	dati relativi all'ubicazione	identificativo online (indirizzi IP)
identità fisica	identità fisiologica	identità psichica	identità genetica
dati biometrici	dati sulla salute	identità economica	identità culturale

identità sociale

Le tipologie dei dati personali



I TUOI DISPOSITIVI COSA SANNO DI TE?

Windows PCs

MACs

Android

Smartphones

Passwords

- Completamento automatico nel Web browser
- Memorizzate nel file system

Info conti bancari

- Documenti scaricati relativi ai movimenti bancari

Files cancellati

- Tutti i file cancellati, inclusi quelli non più presenti nel cestino o nel Recycle bin, possono essere recuperati finché non viene sovrascritto lo spazio fisico di memoria

Files recenti

- L'elenco dei files recenti è conservato dal sistema operativo
- Svariate applicazioni mantengono i propri elenchi di file recenti

Contatti

- Windows Contacts
- Address Book
- Contact Manager

Posizione attuale

- Leggibile dal tuo GPS

Carta di credito

- Completamento automatico nel Web browser
- Estratti conto con i movimenti della carta di credito

Codice fiscale

- Documenti scaricati da siti di Tasse, Istituzioni pubbliche, Previdenza, ecc.

Messaggi di testo

- I messaggi di testo sono memorizzati sul telefono

Telefonate

- Il registro delle chiamate è memorizzato sul telefono

Posizioni recenti

- Fotografie
- Applicazioni di navigazione

Ultimi siti visitati

- Cache del browser
- Log di history del browser
- Cookies

Nome e indirizzo

- Completamento automatico Web browser
- Windows Contacts
- Address Book
- Contact Manager

tratto da CYBER CRIME WATCH

Il valore dei dati

Shiru Cafe, il Linkedin-bar dove il conto si paga con i dati personali

Un locale che apre solo nei campus universitari. Perché i dati non servono tanto per indirizzare la pubblicità quanto per consentire alle imprese di pescare i talenti migliori

di **PAOLO FIORE** | 17 dicembre 2018,07:04

Quali dati personali?

- Nome, cognome, indirizzo, sesso, età, nazionalità, numero di telefono, e-mail, corsi di laurea frequentati, numero di matricola, anno accademico, anno di laurea previsto, interessi personali e professionali

Quali imprese?

- EY, Pwc, Yamaha, Nissan, Nikkei, Nomura, Microsoft, Accenture, Philip Morris, Softbank e Panasonic

https://www.agi.it/estero/linkedin_shiru_cafe_dati_personali-4747773/news/2018-12-17/

Il valore dei dati

I nostri dati hanno un valore … per Google, Facebook, e tante altre aziende.

Le Smart TV adattano i messaggi pubblicitari in funzione di chi è davanti allo schermo (video, voce, ecc.)

I nostri dati sono il VALORE

Se qualcosa è GRATIS, il valore siamo noi, sono i nostri dati

Il valore dei dati è:

- economico
- strategico
- sicurezza
- politico

MILANO

A- A+

Martedì, 11 aprile 2017 - 18:03:00

Stazione Centrale, i totem pubblicitari "spiano" età e sesso dei passanti

A Milano il Garante per la Privacy sta indagando sui totem pubblicitari in Stazione Centrale, che sarebbero in grado di registrare dati preziosi sui passanti

Totem pubblicitari in Stazione Centrale

I totem ci spiano? I cartelloni pubblicitari intelligenti posizionati in Stazione Centrale avrebbero al loro interno delle telecamere collegate ad un software che le rende in grado di effettuare il **riconoscimento facciale delle persone che si fermano ad osservare le immagini, desumendone dati preziosi come il sesso, l'età ed il livello di attenzione** verso la proposta pubblicitaria. Il sospetto è giunto a **Giovanni Pellerano**, responsabile dell'ufficio tecnico di Hermes, centro per la trasparenza e i diritti umani digitali, ed ha portato ad un interessamento da parte del garante per la privacy. La vicenda è stata riportata oggi dal Corriere: i dati sarebbero ceduti ad agenzie di marketing per il successo pubblicitario o per studiare nuove campagne. Ma pendolari e passanti ne sarebbero ignari. La società francese Quividi che gestisce i totem ha ora due settimane per rispondere alle richieste del Garante, soprattutto sull'anonimato delle rilevazioni effettuate.

Il principio di una sentenza del Tar Lazio. Nel mirino Facebook per pubblicità ingannevole

I miei dati? Merce di scambio

Va garantita trasparenza sulle finalità commerciali

Pagina a cura
DI ANTONIO CICCIA MESSINA

I dati personali sono un bene economico commerciabile. Le informazioni sono i valori con cui si pagano i servizi dei social network, che non possono dirsi gratuiti, proprio perché raccolgono dati. E se si definiscono tali, allora è pubblicità ingannevole. Lo dice il Tar Lazio con una sentenza (n. 261 pubblicata il 10 gennaio 2020), che esprime un principio del tutto innovativo, dai possibili effetti a cascata dirompenti, per esempio con riferimento al trattamento dei dati dei minori di età da parte dei social.

Asset. I dati personali, scrive la sentenza, possono costituire un «asset», cioè un cespite o un bene disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di «controprestazione» in senso tecnico di un contratto. Ossia: una persona potrebbe acquistare un bene o un servizio pagandolo con i propri dati, che diventano la controprestazione. I dati sono come il denaro o, comunque, la merce di scambio avente un valore economico. Sono, quindi, sia un elemento della personalità sia un asset da scambiare con un prodotto o con un servizio. La doppia natura del dato personale porta a un raddoppio delle tutele. Scrive il Tar che a fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati. Questo secondo campo di protezione è descritto, per esempio, dalle norme a tutela della concorrenza e del consumatore. Proprio su questo secondo profilo interviene il Tar a confermare la sanzione nei confronti di Facebook, ritenendo ingannevole uno slogan in cui si promettevano servizi gratuiti, anche se prevedevano la raccolta dei dati personali degli utenti. Il Tar prende atto e descrive il fenomeno della «patrimonializzazione» del dato personale, tipico delle nuove economie dei mercati digitali, e ne fa discendere alcune conseguenze. Tra questi effetti la pronuncia segnala quella dell'obbligo per gli operatori commerciali di rispettare, nelle relative transazioni commerciali, gli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere informato e consapevole dello scambio di prestazioni che è sotteso alla adesione a un contratto per la fruizione di un servizio, quale è quello di utilizzo di un «social network». A sostegno del proprio ragionamento il Tar cita gli «Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali» del 25 maggio 2016, nei quali la Commissione europea ha affermato che «i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto».

In sostanza, il patrimonio informativo costituito dai dati degli utenti e la profilazione degli utenti medesimi a uso commerciale e per finalità di marketing «acquista, proprio in ragione di tale uso, un valore economico idoneo, dunque, a configurare l'esistenza di un rapporto di consumo tra il Professionista e l'utente»

Slogan ingannevoli. Sulla base di queste riflessioni, il Tar sostiene che il valore economico dei dati dell'utente impone al professionista di comunicare al consumatore che le informazioni ricavabili da tali dati saranno usate per finalità commerciali che vanno al di là della utilizzazione del social network. Pertanto, in assenza di adeguate informazioni, o nel caso di affermazioni fuorvianti, la pratica posta in essere può quindi qualificarsi come ingannevole.

Nel caso specifico Facebook ha utilizzato nella pagina di registrazione al social lo slogan «Iscriviti, è gratis e lo sarà per sempre», uno slogan che lasciava intendere l'assenza di una controprestazione richiesta al consumatore in cambio della fruizione del servizio. E in effetti non c'era nessuna richiesta del pagamento di una somma di denaro. Questo slogan è stato sanzionato, però, per incompletezza delle informazioni fornite, che a fronte del richiamo alla «gratuità» del servizio non consentivano al consumatore di comprendere che il professionista avrebbe poi utilizzato i dati dell'utente a fini remunerativi, perseguendo un intento commerciale.

Per i minori il consenso alle app non vale

Se scambiare dati per scaricare una app è un contratto, allora i minori non possono dare il consenso a trattare i propri dati ai social network e ai gestori di servizi della società dell'informazione. È questo uno degli effetti dell'applicazione del principio enunciato dalla sentenza del Tar Lazio n. 261/2020. Così ci vorrebbe il consenso dei genitori se un minorenne vuole scaricare una app dando in cambio i dati. La conseguenza a cascata dalla pronuncia del giudice amministrativo incide sull'articolo 8 del regolamento Ue sulla privacy n. 2016/679 (Gdpr), che, per il caso di offerta diretta di servizi della società dell'informazione ai minori, pretende il minimo di 16 anni per poter esprimere il consenso. Sotto i 16 anni ci vuole il consenso del genitore. Gli stati europei possono stabilire per legge un'età inferiore (ma non sotto i 13 anni). In Italia l'articolo 2-quinquies del Codice della privacy, modificato dal decreto legislativo 101/2018, ha previsto che il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Però l'articolo 8 del Gdpr aggiunge che rimangono valide le disposizioni generali del diritto dei contratti dei singoli stati, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore. A questo punto ci si deve chiedere se scambiare dati personali con una app sia già un contratto oppure no. Nel caso si ritenga di sì, ci vuole il consenso dei genitori perché il minorenne non è capace, per il codice civile, ai fini contrattuali. Nel caso in cui, invece, dare il consenso a trattare i dati personali sia cosa diversa dal concludere un contratto, allora si deve riconoscere al minorenne la capacità di autodeterminarsi. La sentenza del Tar del Lazio spinge a considerare che lo scambio dati contro servizi internet sia un contratto. Anche su questo aspetto né il legislatore europeo né quello italiano hanno dato regole chiare, con il risultato che il quesito sarà molto probabilmente sciolto da pronunce della magistratura, chiamata su un caso concreto.

Informazione

Non solo informazioni

2.4

asset

anything that has value to the organisation

NOTE There are many types of assets, including:

- *information;*
- *software, such as a computer program;*
- *physical, such as computer;*
- *services;*
- *people, and their qualifications, skills, and experience; and*
- *intangibles, such as reputation and image.*

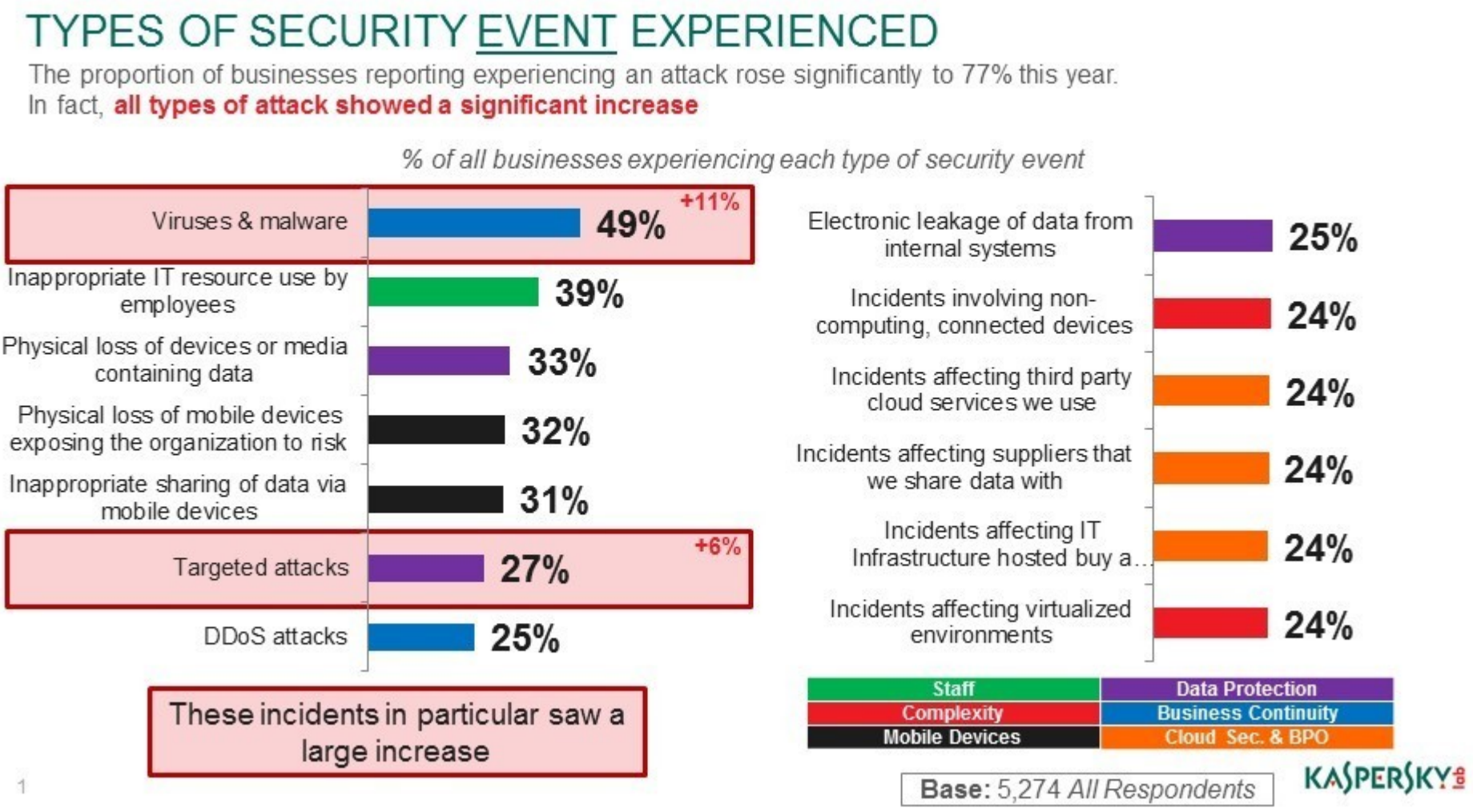
ISO/IEC 27000:2012 https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-2:v1:en

FBI

Top 10 Crime Types Reported to IC3 in 2017 (by Victim Loss)

IC3 = Internet Crime Complaint Center ➔(FBI), National White Collar Crime Center (NW3C), Bureau of Justice Assistance (BJA). https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

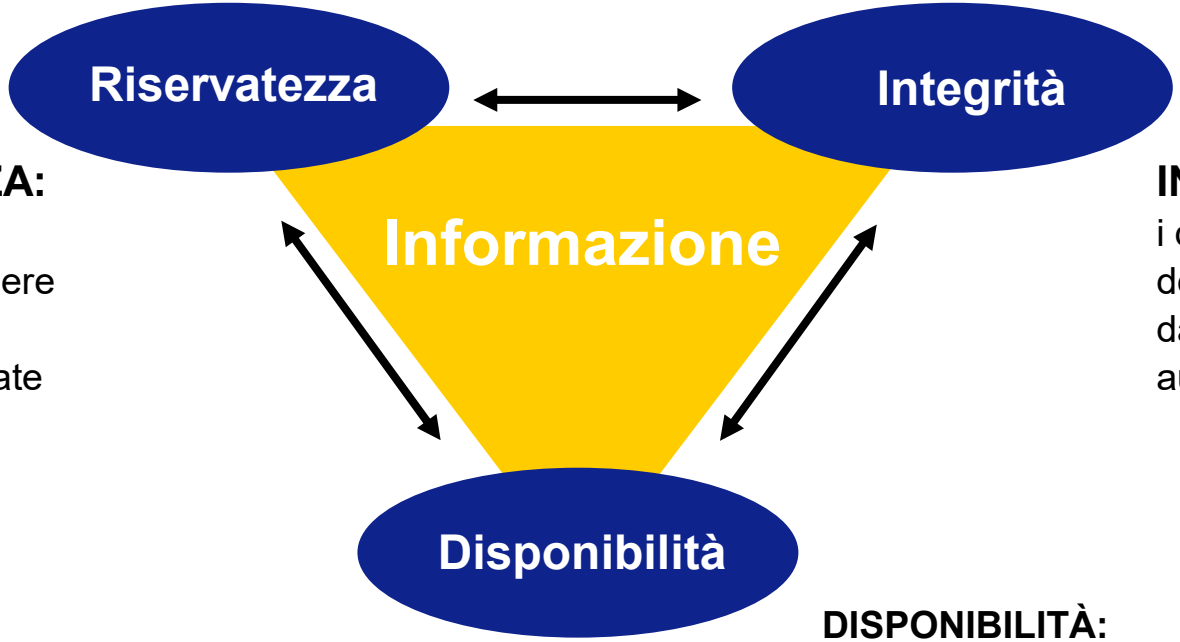
Le azioni dei dipendenti causano incidenti di sicurezza



Source: IT Security Risks Survey 2017, global data

Che cos'è la Sicurezza delle Informazioni?

Attività volta a definire, conseguire e mantenere:



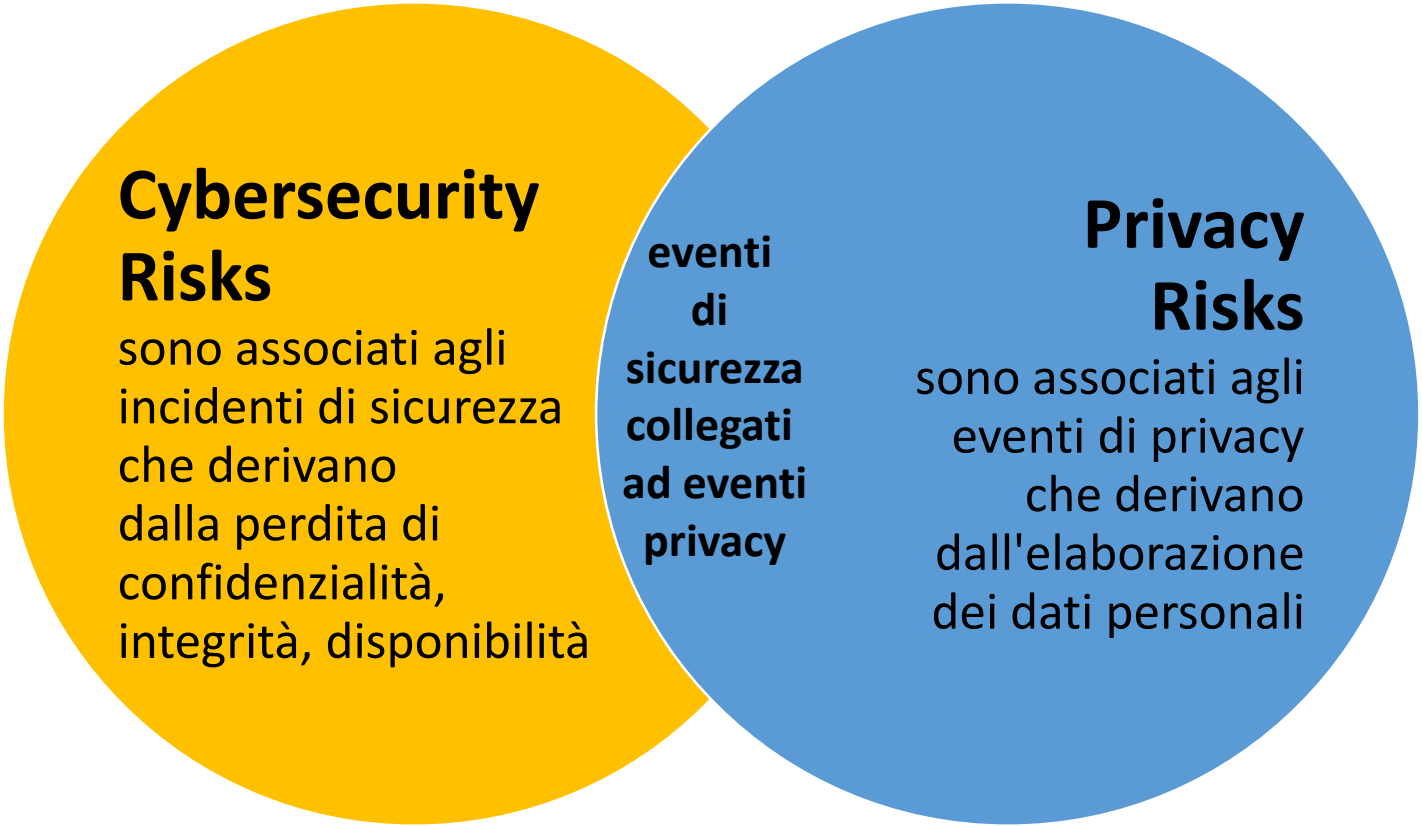
RISERVATEZZA:
le informazioni devono poter essere accedute solo da persone autorizzate

INTEGRITÀ:
i dati e le informazioni devono essere protette da modifiche non autorizzate

DISPONIBILITÀ:
i sistemi e le applicazioni devono essere disponibili quando necessario

paradigma R.I.D.

Cybersecurity e Privacy Risk



Privacy: multa di 11,5 milioni a Eni Gas e Luce per telemarketing e contratti non richiesti

La stangata del Garante per trattamenti illeciti di dati personali nell'ambito di attività promozionali e attivazione di forniture non richieste

Il Garante per la privacy ha applicato a Eni Gas e Luce (Egl) due sanzioni, per complessivi 11,5 milioni di euro, riguardanti rispettivamente trattamenti illeciti di dati personali nell'ambito di attività promozionali e attivazione di contratti non richiesti. Le sanzioni sono state determinate tenendo conto dei parametri indicati nel Regolamento Ue, tra i quali figurano l'ampia platea dei soggetti coinvolti, la pervasività delle condotte, la durata della violazione, le condizioni economiche di Egl.

La prima sanzione di 8,5 milioni di euro riguarda trattamenti illeciti nelle attività di telemarketing e teleselling. La seconda sanzione di 3 milioni di euro riguarda violazioni nella conclusione di contratti non richiesti nel mercato libero della fornitura di energia e gas.

https://www.repubblica.it/tecnologia/sicurezza/2020/01/17/news/privacy_multa_di_11_5_mln_a_eni_gas_e_luce_per_telemarketing_e_contratti_non_richiesti-246007879/

GDPR – Art. 5
Princìpi applicabili al trattamento di dati personali

- Liceità, correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

GDPR – Art. 5
Princìpi applicabili al trattamento di dati personali

1. I dati personali sono:
   a) trattati … («**liceità, correttezza e trasparenza**»);
   b) raccolti … («**limitazione della finalità**»);
   c) adeguati, pertinenti e limitati … («**minimizzazione dei dati**»);
   d) esatti e, se necessario, aggiornati … («**esattezza**»);
   e) conservati … («**limitazione della conservazione**»);
   f) trattati … («**integrità e riservatezza**»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).

Informativa e consenso

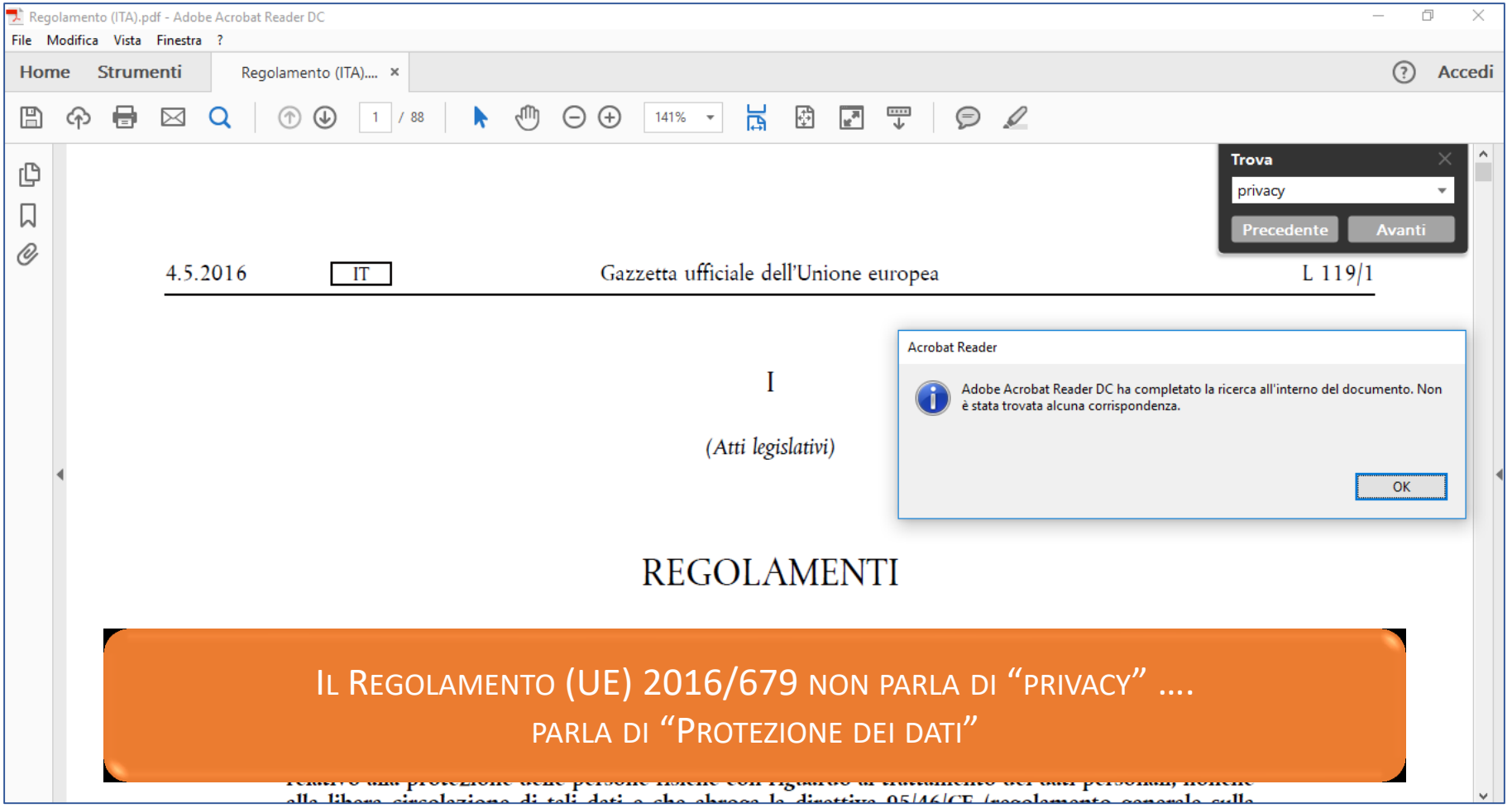
Liceità del trattamento (Art. 6)

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

Condizioni per il consenso (Art. 7)

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. …la richiesta di consenso è presentata in modo **chiaramente distinguibile** dalle altre materie, in **forma comprensibile** e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.

GDPR – protezione dei dati vs privacy



IL REGOLAMENTO (UE) 2016/679 NON PARLA DI "PRIVACY" ….
PARLA DI "PROTEZIONE DEI DATI"

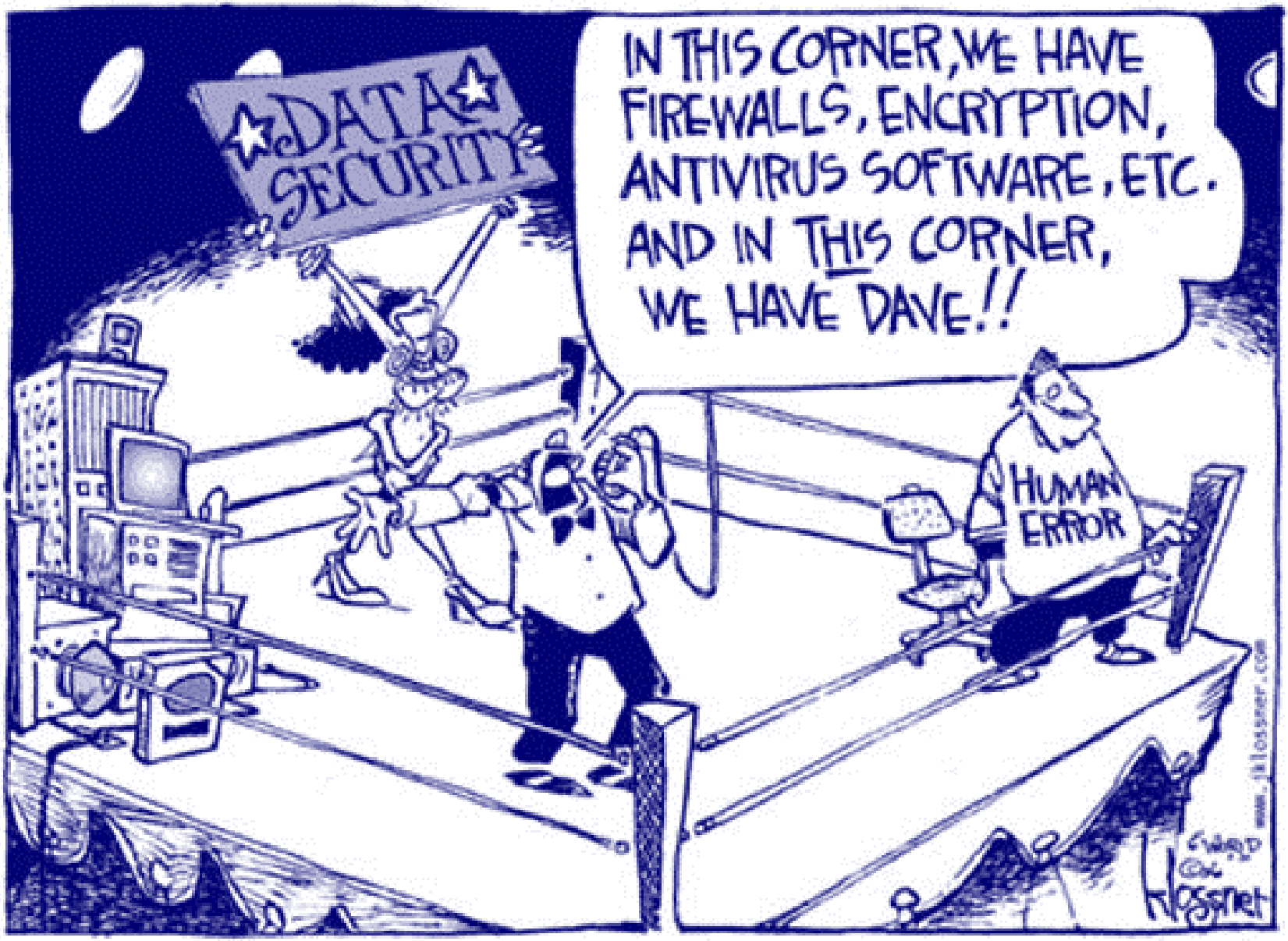
I diritti dell'interessato e l'accesso ai dati

- Diritto di accesso (Art. 15)
- Diritto di rettifica (Art. 16)
- Diritto alla cancellazione (Art. 17)
- Diritto di limitazione di trattamento (Art. 18)
- Diritto al portabilità dei dati (Art. 20)
- Diritto di opposizione (Art. 21)
- Diritto di proporre reclamo all'autorità di controllo (Art. 77, 78, 79)

Cosa si può fare?

- **Prevent**
  - Comprendere quale può essere la minaccia e com… …taccati
- **Protect**
  - Ci sono molti modi per proteggere le i… …esenza online, ma nessuna è quella risolutiva
- **Deter & Detect**
  - Prevenire e proteggere… …entalità orientata alla sicurezza. Il modo migliore è adottare… …tto
    - **… volte, clicca una volta!**
    - **Think twice, click once**!
  - L'… …entale è mantenere la vita privata fuori da Internet
    - …promissione, recuperare le informazioni e gestire l'impatto, la …
- **Have I been pwned?**
  - www.haveibeenpwned.com (https://haveibeenpwned.com/)

HUMAN FIREWALL


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Social Networking Security - 10 punti fondamentali

1. Una volta che un'informazione/immagine/scritto è su Internet, rimane in Internet
2. Ogni cosa che dici/scrivi rimane associata alla tua identità digitale
3. Quello che scrivi ora avrà un impatto sul tuo futuro
4. Chiunque può pubblicare su Internet, quindi controllare prima
5. Chiunque può essere chi vuole su Internet, bisogna essere cauti dei profili
6. Controlla i profili degli amici, poi controlla in altra parte, quindi controlla nuovamente
7. Attenzione ad esprimere giudizi non adeguati, vale il punto 1.
8. Pensa due volte, clicca una volta
9. Leggi e rileggi il tuo post prima di inviare
10. Cerca informazioni su di te saltuariamente, è incredibile quello che si scopre

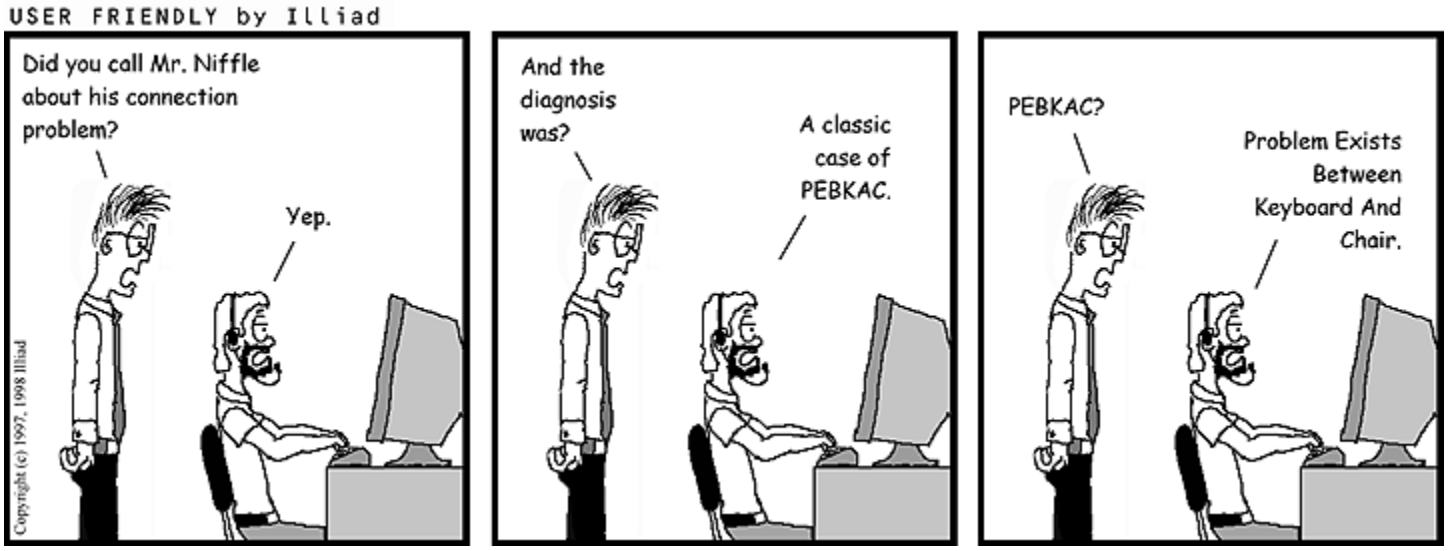
Mobile security

- Non lasciare il laptop/tablet/smartphone/pendrive incustodito e non protetto
- Per evitare il furto del laptop/tablet, utilizzare un cavo Kensington
- Assicurarsi che il disco del laptop/tablet sia crittografato
- Assicurarsi che i dispositivi abbiano una passphrase robusta
- In viaggio, non lasciare insieme dispositivi di back-up e laptop/tablet
- Utilizzare email o cloud sicuri per memorizzare informazioni importanti
- Installare una VPN
- Non accedere a reti Wi-Fi pubbliche se non tramite una VPN
- Non utilizzare dispositivi USB personali o acquistati localmente
- Usare sempre dispositivi USB crittografati per informazioni di backup o se utilizzati per trasferire informazioni
- Utilizzare gli appositi alimentatori per la ricarica di smartphone e dispositivi USB, → **NON usare le porte USB!**
- Utilizzare un filtro di schermo per impedire la vista dai lati

"Stupendo spot belga sull'ingenuità …"

https://www.youtube.com/watch?v=eASGFYqX7sg

PEBKAC
problem-exists-between-keyboard-and-chair



Domande?


MATICMIND
makes IT easy
Giuseppe G. Zorzino
DPO & Security Advisor
T: +39 06 51065417
M: +39 335 6281204
Mail: giuseppe.zorzino@maticmind.it
Via M. Carucci, 131
00143 ROMA
Tel. +39 06 510651
info@maticmind.it
www.maticmind.it