

I rischi informatici nella professione
dell'Ingegnere nell'era COVID-19
Ing. Mattia Siciliano

6 Maggio 2020
Commissione CyberSecurity



Agenda

- Che cosa è la Cyber Security
- Lo scenario internazionale
- Perché è importante proteggersi
- Le normative italiane e Internazionali
- Gli oggetti ed i rischi associati
- I 10 elementi e regole che un professionista deve seguire
- Conclusioni



Che cosa è la Cyber Security

La società moderna non può fare a meno di innovarsi, creando un ecosistema digitale, in cui **l'uomo e le sue informazioni rappresentano il vero valore del prossimo futuro.**

In tale contesto l'espansione di internet produrrà sempre nuovi servizi e benefici per la collettività, ma al tempo stesso aumenterà i rischi legati alla privacy, alla protezione degli asset nazionale, alla sicurezza delle grandi e delle piccole aziende.

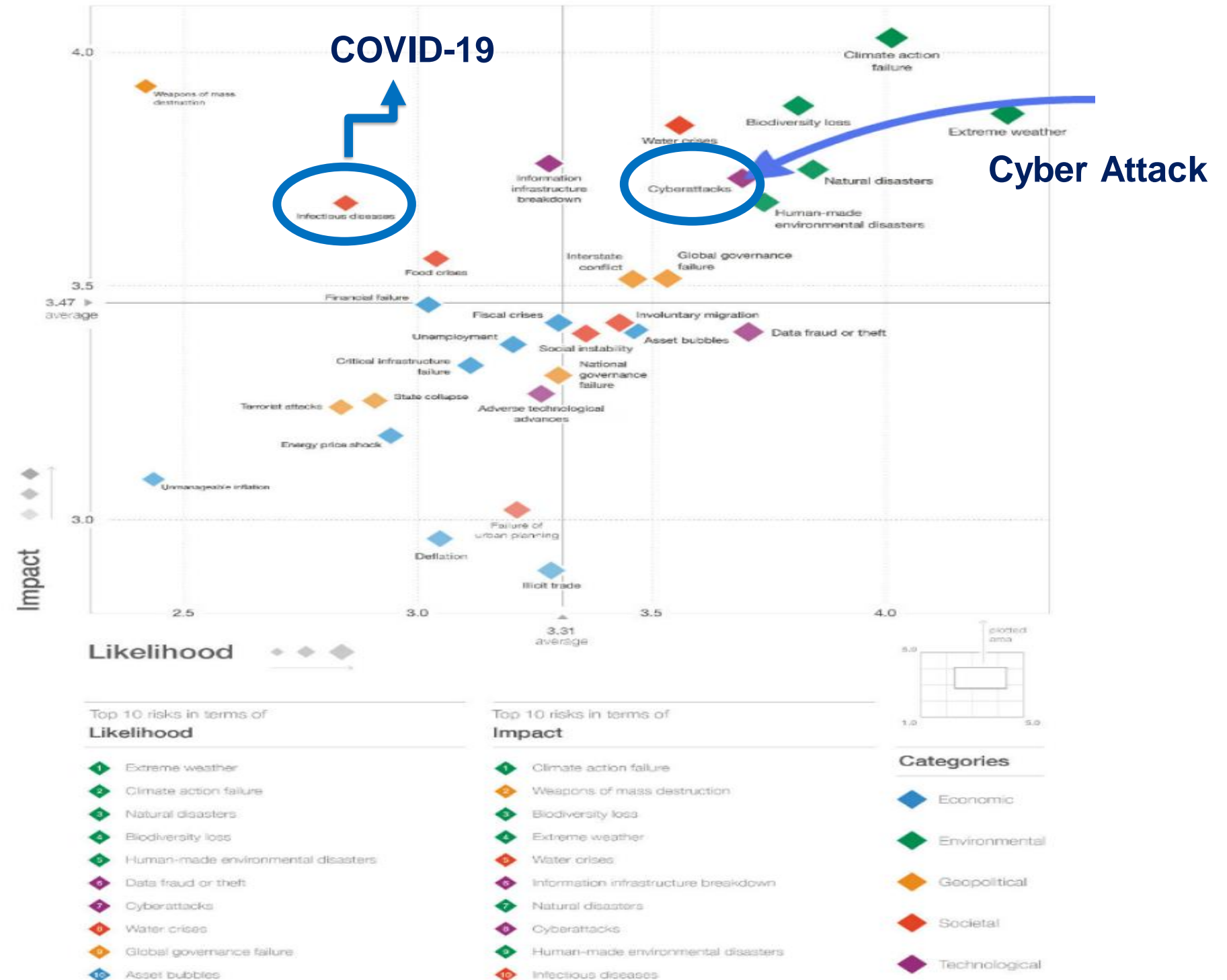
“The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive,”
– **Gartner Rethink the Security & Risk Strategy 2019**

Secondo la società d'analisi [MarketsandMarkets](#), l'industria della cyber-security potrebbe salire a oltre 248 miliardi nel 2023. Questo presuppone **un tasso di crescita annuale del 10,2% nei prossimi cinque anni.**

Lo scenario internazionale

Secondo lo studio di ENISA (Agenzia Europea per la Sicurezza Informatica) presentato al WEF – World Economic Forum , la probabilità che si verificano degli eventi «tecnologici» che possano procurare gravi impatti alla comunità internazionale seguono esclusivamente gli eventi naturali e prima delle pandemie (i.e COVID-19)

Figure II: The Global Risks Landscape 2020



Lo scenario internazionale




THE GLOBAL RISK OUTLOOK FOR 2019

Types of Risks:  ENVIRONMENTAL  GEOPOLITICAL  SOCIETAL  TECHNOLOGICAL  ECONOMIC

Top 5 Global Risks in Terms of **Impact**

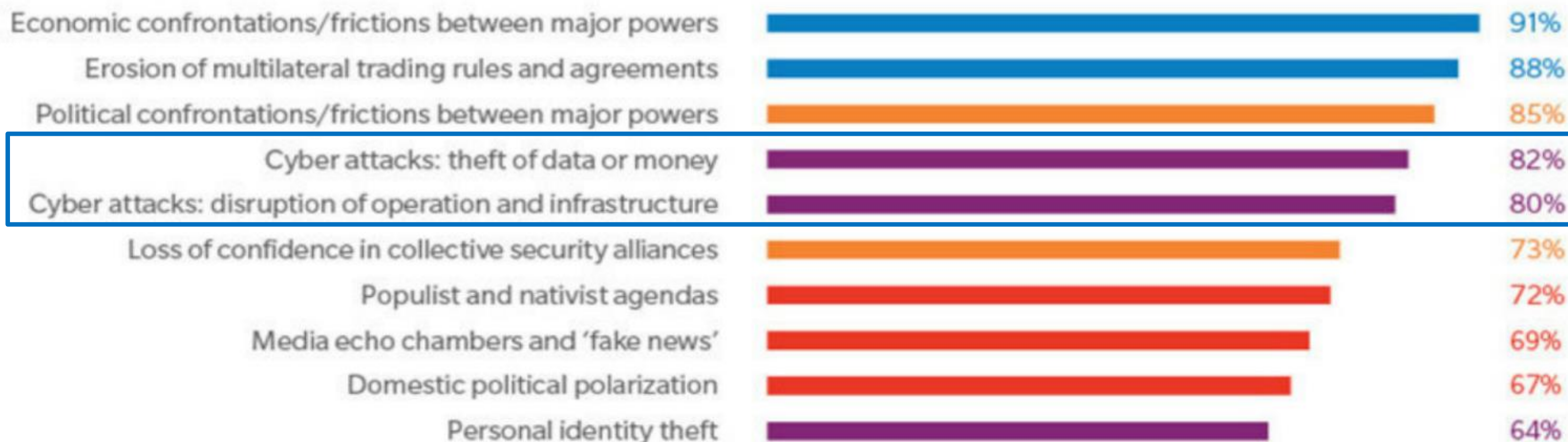
-  *Weapons of mass destruction*
-  *Failure of climate-change mitigation and adaptation*
-  *Extreme weather events*
-  *Water crises*
-  *Natural disasters*

Top 5 Global Risks in Terms of **Likelihood**

-  *Extreme weather events*
-  *Failure of climate-change mitigation and adaptation*
-  *Natural disasters*
-  *Data fraud or theft*
-  *Cyber-attacks*

Lo scenario internazionale

TOP RISKS EXPECTED TO INCREASE IN 2019



Environmental Technological Geopolitical Societal Economic

Source: World Economic Forum, Global Risks Report 2019

Lo scenario internazionale

Non tutti queste forme di minaccia sono conducibili alle normali attività di un professionista, ma più in generale esprime uno scenario completo delle possibili minacce che tenga presente anche le attività svolte da un professionista in un contesto aziendale



Perché è importante proteggersi

Gli attacchi informatici costano 8 milioni di dollari alle aziende in Italia

di Luca Tremolada



🕒 2' di lettura

In Italia il costo medio annuo per azienda delle violazioni della sicurezza informatica ha raggiunto gli 8 milioni di dollari (13 milioni di dollari per azienda a livello globale), con un incremento del 19% nel 2018 (12% a livello globale). È quanto emerge dal nono studio annuale di Accenture Security sui costi del cybercrime.

La ricerca, che ha coinvolto 11 Paesi per un totale di 2.647 responsabili security e IT intervistati. Il numero medio annuo di security breach per azienda è aumentato da 50 a 62 (+20% in Italia contro un +11% a livello

☰ MENU | 🔍 CERCA

la Repubblica

HOME | MACROECONOMIA ▾ | FINANZA ▾ | LAVORO | DIRITTI E CONSUMI ▾ | AFFARI&FINANZA | OSSERVA ITALIA

Cybersicurezza , il mercato in Italia vale 1,5 miliardi (ma è insufficiente)

Indagine della società di consulenza EY: solo il 45 per cento delle imprese ha investito contro gli attacchi informatici. Nel mondo verranno creati nel settore due milioni di posti lavoro in cinque anni

Le normative italiane e Internazionali



NIS
28 Giugno 2019
**The Directive on security of
network and information systems**

Fornisce misure legali e
definisce un quadro di
cooperazione per migliorare i
livelli di sicurezza degli
Operatori di Servizi Essenziali
(OSE) e ai Fornitori di Servizi
Digitali (FSD).

GDPR
25 Maggio 2018
**General Data Protection
Regulation**

Norma il trattamento dei dati
personali delle persone fisiche
applicabile a tutte le
organizzazioni

AGID
18 Aprile 2017
Misure Minime di sicurezza

Sono un riferimento pratico
per valutare e migliorare il
livello di sicurezza informatica
delle amministrazioni
pubbliche



Studi Camera - Istituzioni
Difesa e Sicurezza

D.L. 105/2019: perimetro di sicurezza cibernetica

Impatto per il Professionista

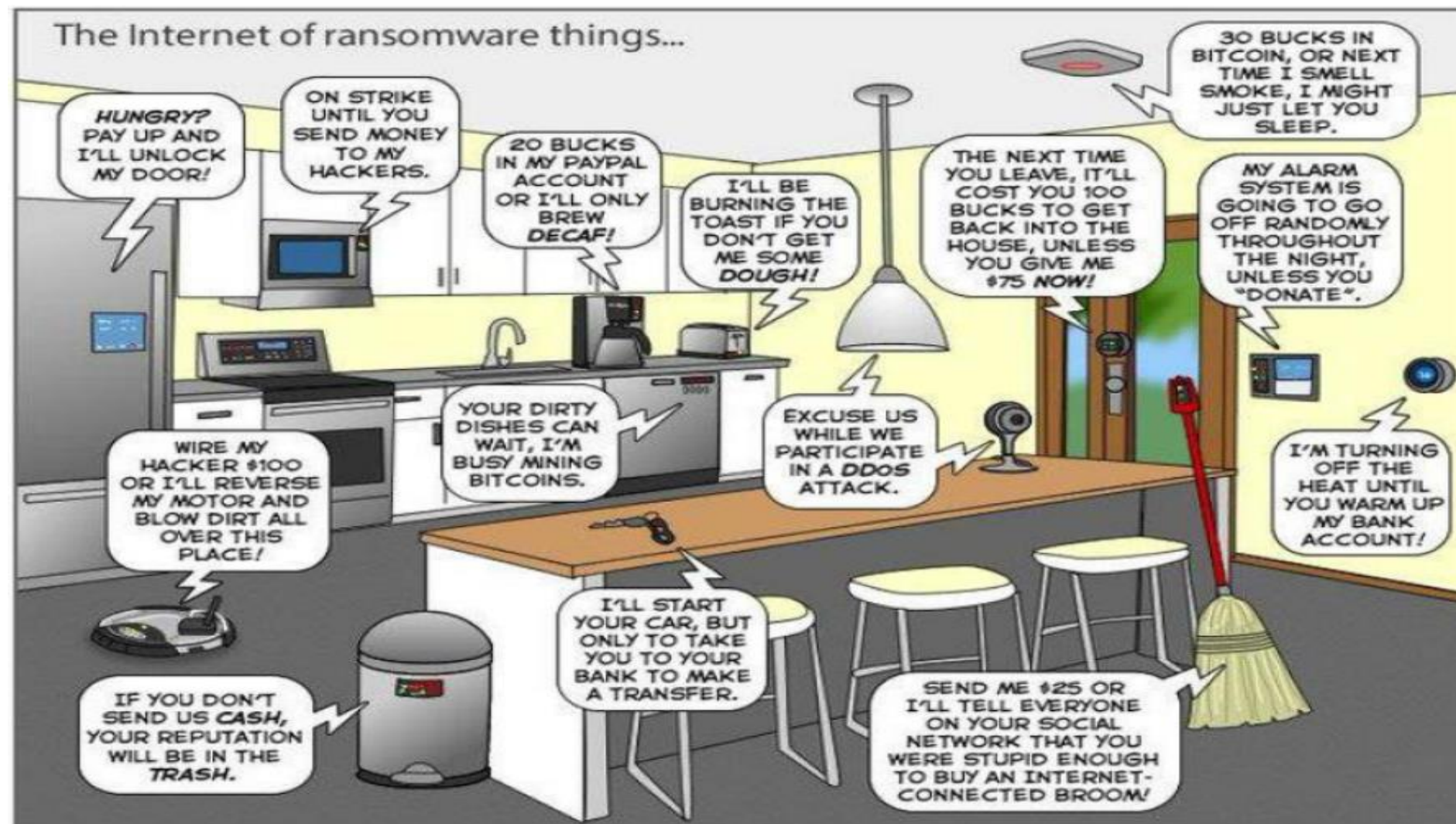
Gli oggetti ed i rischi associati - 1/2

Internet delle cose (IoT, acronimo dell'inglese Internet of things). Il concetto rappresenta una possibile evoluzione dell'uso della rete internet: gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri



Gli oggetti ed i rischi associati - 2/2

Internet delle cose (IoT) offre molte opportunità in termini di informazioni ma anche molti rischi. In un futuro non molto lontano ci ritroveremo ad affrontare minacce che possono provenire da diversi «attori», come oggetti presenti in una casa ma anche oggetti impiantati nei nostri corpi



Scenario di CASA



Scenario personale

I 10 elementi e regole che un professionista deve seguire

Lavora in modalità sicura anche da casa

Le 10 Regole da seguire per una maggiore Cyber Sicurezza dei propri dati

01

BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

02

PASSWORD

Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

03

ANTIVIRUS

Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

04

ALLEGATI

Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

05

SOCIAL ENGINEERING

Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

06

VPN

Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili

07

CONDIVISIONE

Non usare strumenti di condivisione dati pubblici (es. Wetransfer) ma cloud privati (es. Google Cloud, Azure, DropBox), proteggendo i dati con password robuste

08

CRITTOGRAFIA

Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili

09

PROCEDURE

Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

10

ACCESSI

Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

Backup

01

BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

Va effettuato almeno 1 volta a settimana in maniera incrementale e una volta a mese full. Possibilmente su supporti esterni o cloud

Se fatto con continuità il rischio di perdita dei dati è molto basso. L'efficacia in caso di attacco o cancellazione accidentale è molto alta



Indica un processo ovvero in particolare la messa in sicurezza delle informazioni di un sistema informatico (o un semplice computer) attraverso la creazione di ridondanza delle informazioni stesse

Rende i dati e le informazioni sempre disponibili in caso di attacco informatico o cancellazione accidentale

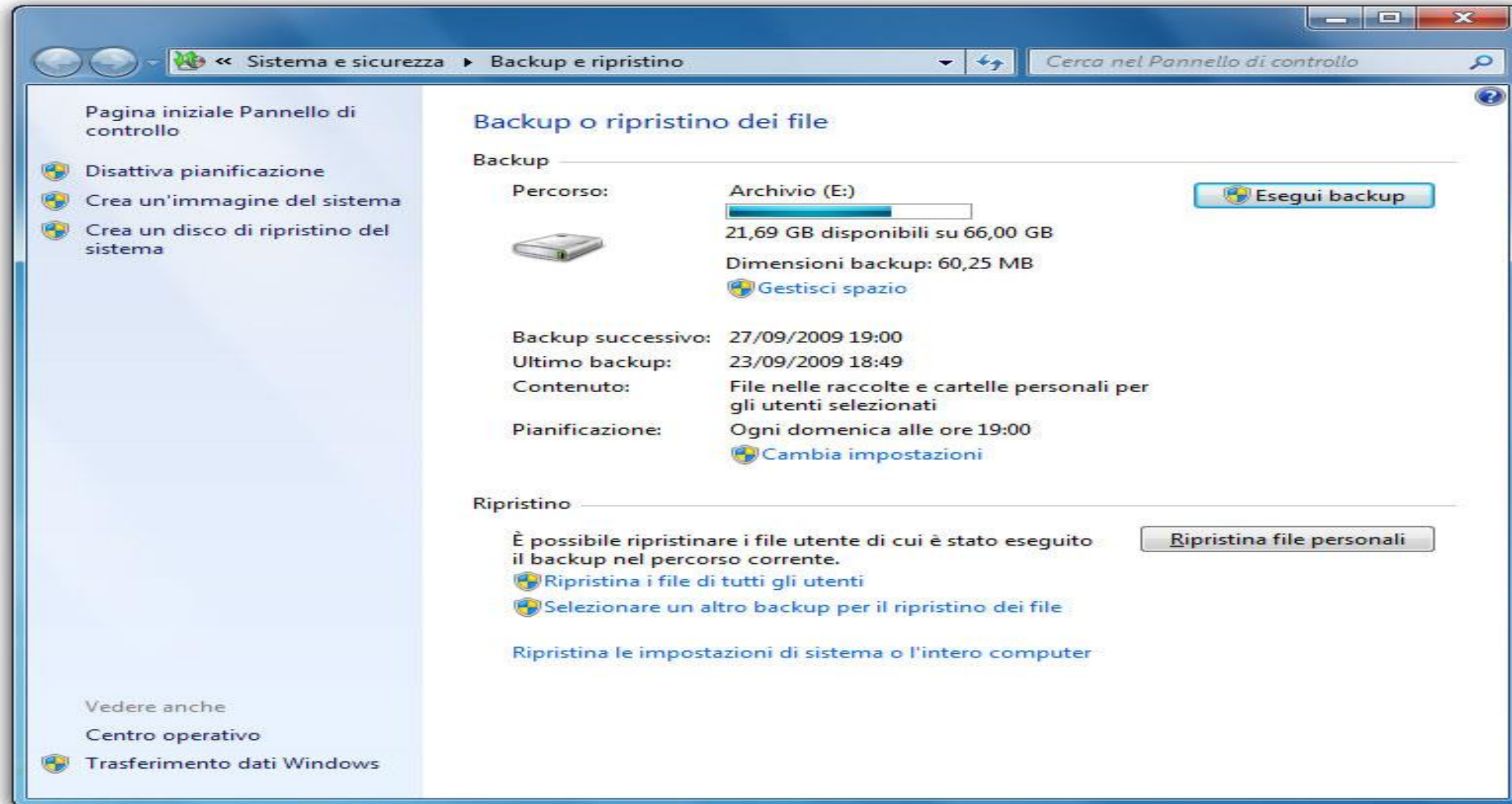
Previene principalmente da minacce di tipo Ransomware (crittografia del proprio PC)

Backup

01

BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)




The screenshot shows the Windows Backup and Restore control panel window. The title bar reads "Sistema e sicurezza > Backup e ripristino". The breadcrumb trail is "Sistema e sicurezza > Backup e ripristino". The search bar contains "Cerca nel Pannello di controllo".

Backup o ripristino dei file

Backup

Percorso: Archivio (E:) [Esegui backup](#)

 21,69 GB disponibili su 66,00 GB
Dimensioni backup: 60,25 MB
[Gestisci spazio](#)

Backup successivo: 27/09/2009 19:00
Ultimo backup: 23/09/2009 18:49
Contenuto: File nelle raccolte e cartelle personali per gli utenti selezionati
Pianificazione: Ogni domenica alle ore 19:00
[Cambia impostazioni](#)

Ripristino

È possibile ripristinare i file utente di cui è stato eseguito il backup nel percorso corrente. [Ripristina file personali](#)

[Ripristina i file di tutti gli utenti](#)
[Selezionare un altro backup per il ripristino dei file](#)

[Ripristina le impostazioni di sistema o l'intero computer](#)

Pagina iniziale Pannello di controllo

- [Disattiva pianificazione](#)
- [Crea un'immagine del sistema](#)
- [Crea un disco di ripristino del sistema](#)

Vedere anche

- [Centro operativo](#)
- [Trasferimento dati Windows](#)

Password

02

PASSWORD

Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

Cambiare la password almeno ogni 90. In alcuni casi prevedere dei sistemi di doppia autenticazione come impronta digitale o 2FA

Il rischio associato è molto alto, in caso non sia configurata correttamente. Deve avere almeno una lunghezza di 8 caratteri alfanumerica e con caratteri speciali (i.e. \$, @, etc). Meglio ancora se sono delle frasi



una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo a una risorsa informatica

Protegge l'accesso al PC o alle vostre aree riservate da parte di soggetti terzi

Se correttamente creata previene minacce di phishing, brute force, identity theft

AntiVirus

03

ANTIVIRUS

Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

Va aggiornato almeno ogni settimana. Meglio ancora se unito con un sistema di Firewall dello studio o con un contratto di prevenzione con l'operatore telefonico

Il software va sempre aggiornato. Nel caso non lo fosse il rischio di accesso da parte di un virus è molto elevato così come la perdita dei dati



è un software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware per un computer

Serve a proteggersi da Virus esterni in grado di accedere a dati e informazioni sensibili

Previene diverse minacce come : virus, adware, backdoor, keylogger, spyware, trojan, worm o ransomware

Allegati

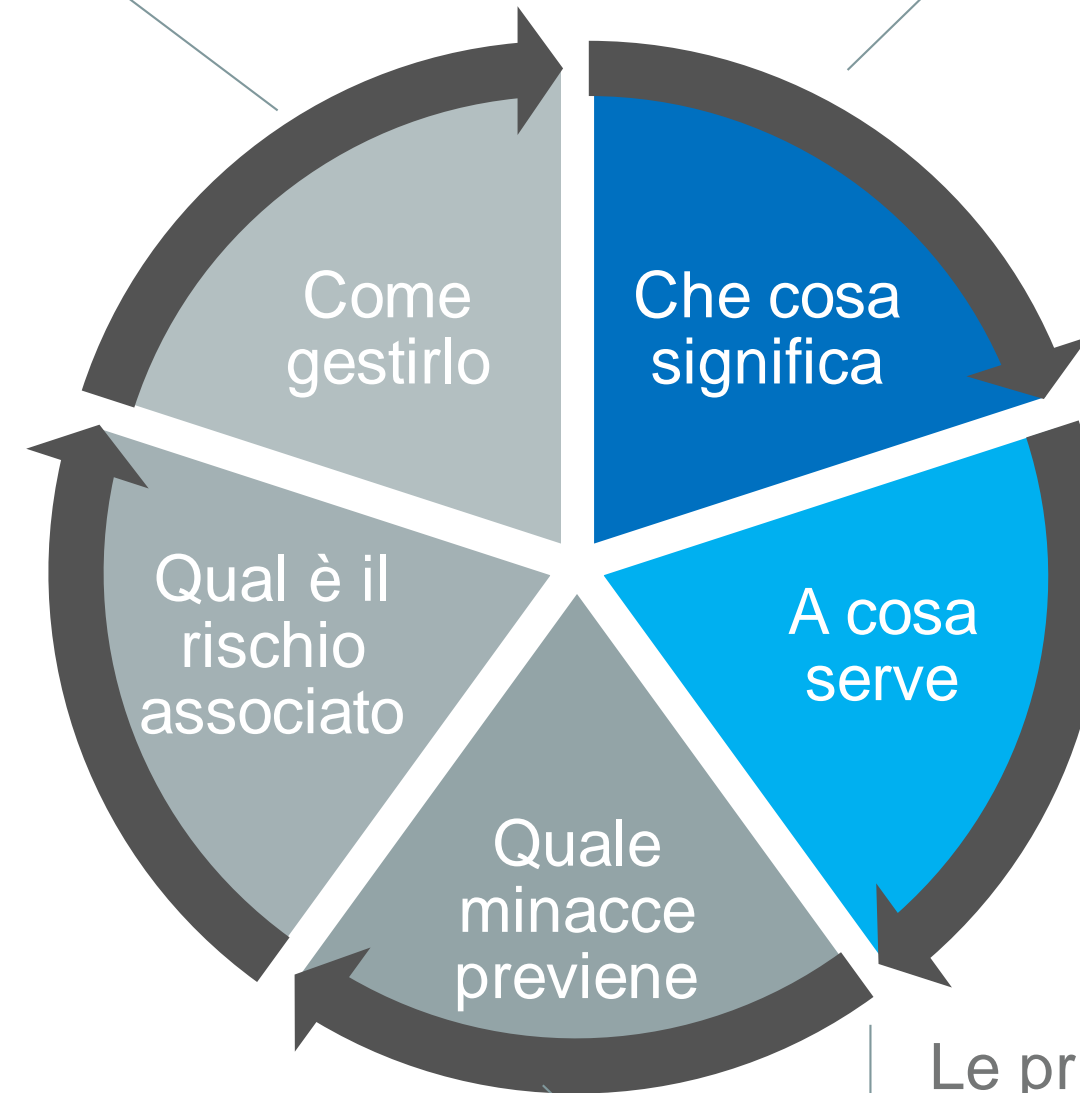
04

ALLEGATI

Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

Generalmente è consigliabile fare analizzare gli allegati all'antivirus prima di aprirlo. Nei casi più complessi si possono usare delle Sandbox così da comprenderne il rischio

Il rischio associato è molto elevato. Pertanto si consiglia di fare molta attenzione al tipo di file, all'estensione anomale (ie. Se non è Doc, docx, pdf, etc) e al creatore/mittente



è un file di un computer che viene inviato assieme a un messaggio di posta elettronica

Il generale sono utilizzati per lo scambio della informazioni, ma in alcuni casi possono nascondere dei codici malevoli

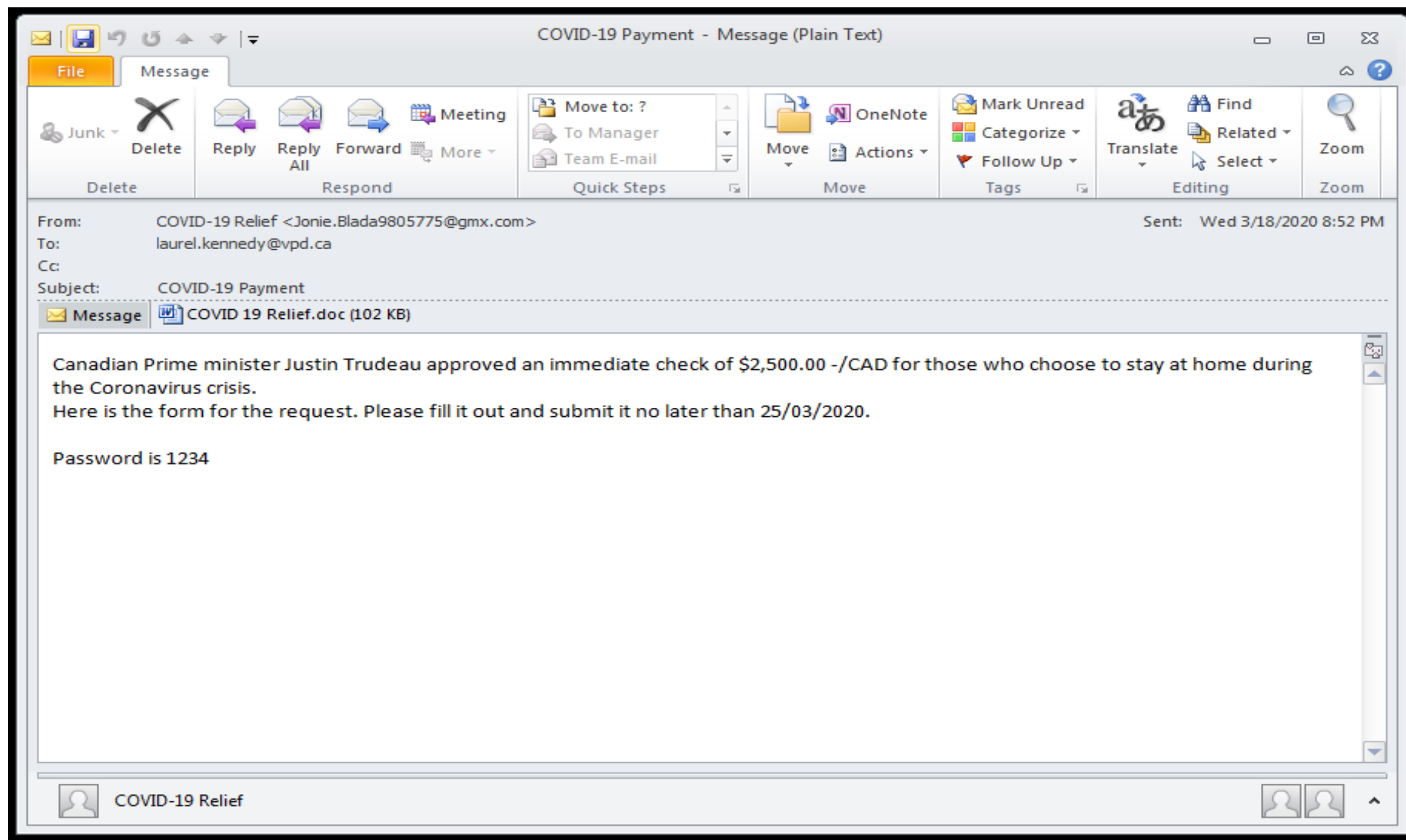
Le principali minacce sono il Phishing, ransomware o spyware, trojan (nascoso nel codice dell'allegato)

Allegati

04

ALLEGATI

Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza



Social Engineering

05

SOCIAL ENGINEERING

Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

Prendere tempo, fare molte domande al richiedente sulla sua identità e non divulgare informazioni sensibili. In casi eclatanti fare denuncia alla Polizia Postale

è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili



Viene usato dai criminali informatici per carpire informazioni con la finalità di frode o ricatto

Il rischio di condividere informazioni sensibili è molto alto. Fare molta attenzione alle richieste e al mittente per evitare di essere ingannati

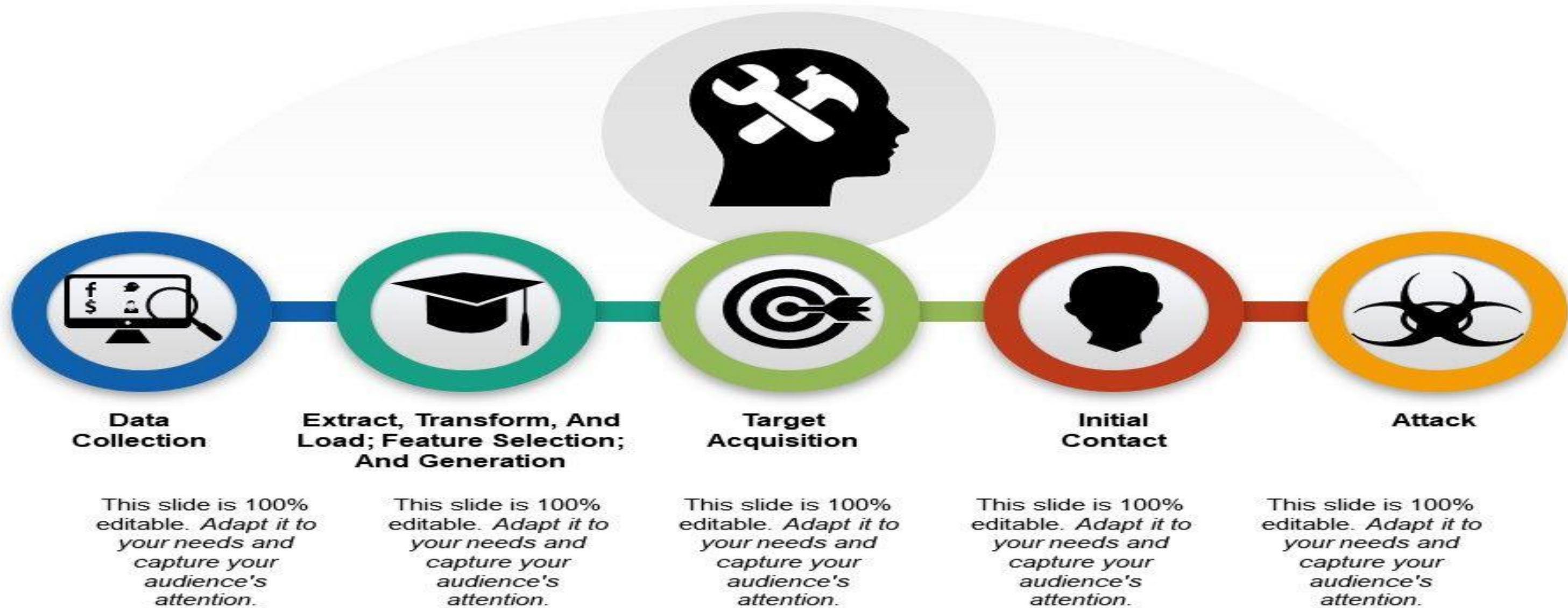
Social Engineering

05

SOCIAL ENGINEERING

Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

Social Engineering With Five Steps Include Data...



VPN

06

VPN

Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili

Va utilizzata principalmente quando si lavora in modalità smartworking o si vuole accedere al proprio Server in modalità sicura

E' una tecnologia che permette di collegare due punti/postazioni in maniera sicura



Rende la comunicazione tra due punti (ie. PC dello studio e PC di casa) sicura e crittografata evitando l'accesso a terzi

L'utilizzo di questa tecnologia abbatte notevolmente il rischio di un attacco e rende il lavoro in modalità smartworking ancora più sicuro

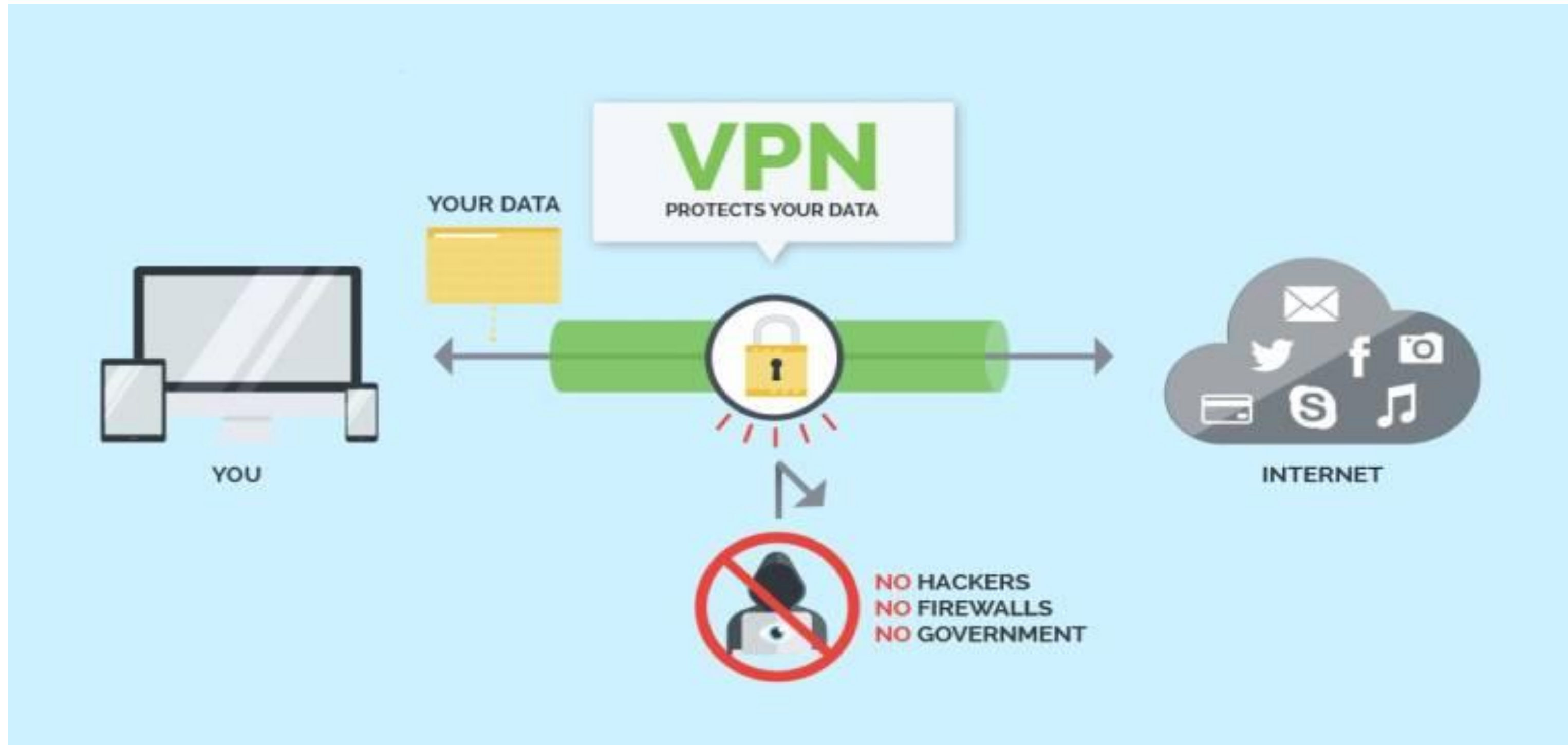
Previene l'accesso di terzi e di malware (se entrambi i punti sono protetti)

VPN

06

VPN

Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili



Condivisione

07

CONDIVISIONE

Non usare strumenti di condivisione dati pubblici (es. Wetransfer) ma cloud privati (es. Google Cloud, Azure, DropBox), proteggendo i dati con password robuste

Nel caso di condivisione di file nel cloud è sempre buona norma proteggerli con una password (ie ZIP file) o se possibile crittografarli

E' un tecnica usata principalmente per lo scambio di file di grandi dimensioni



Scambiare file di grandi dimensioni (ie video, foto, CAD, etc) attraverso canali non convenzionali come la posta elettronica

Il sistemi non convezionali come WeTrasfer conservano i dati su server pubblici esposti a minacce sul web senza specifici apparti ti protezione, pertanto il rischio di accesso a dati riservati o progetti è alto. L'uso di cloud privati garantisce da parte dell'operatore un livello minimo di sicurezza perimetrale

La condivisione sicura su cloud privati (ie . Google, Azure, Dropbox, etc), previene la minaccia di accesso da parte di terzi in caso di data breach

Crittografia

08

CRITTOGRAFIA

Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili

Quando si vuole condividere un'informazione altamente sensibile (ie. un progetto di un cliente). In questo caso usare almeno una crittografia a 128 bit

Condividere dati sensibili senza «offuscamento» ha un elevato rischio di data leak che può sfociare in caso di leak in una frode o ricatto



metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo

Rendere non leggibile il dato a terzi evitando l'accesso non autorizzato

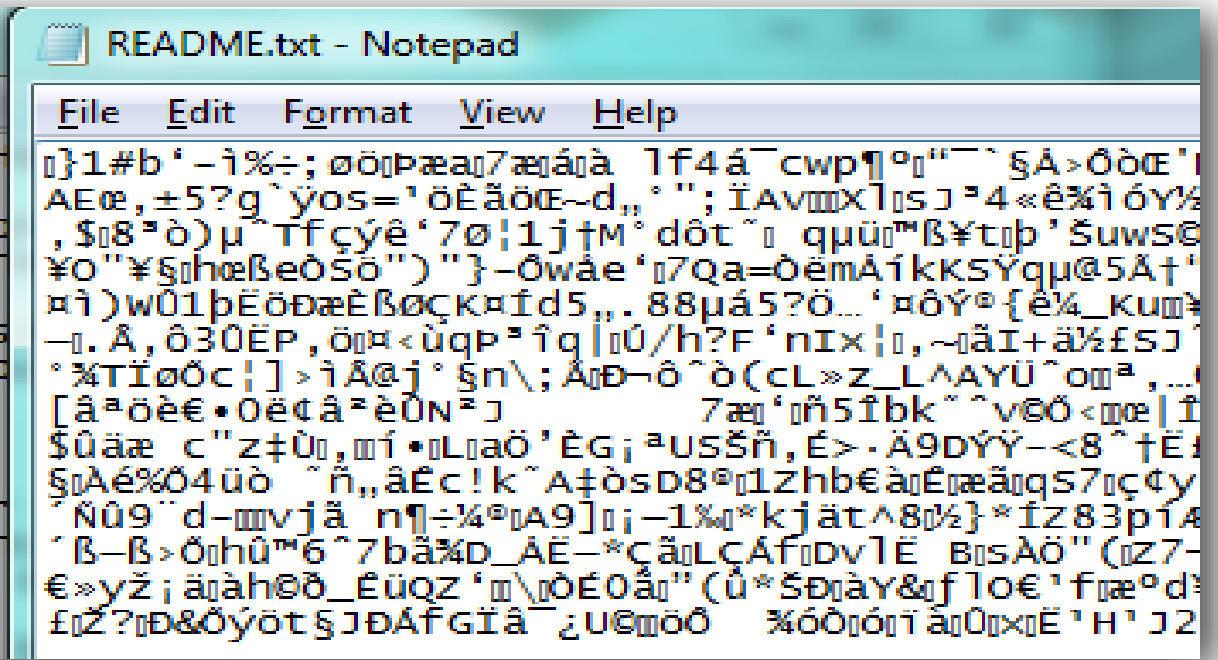
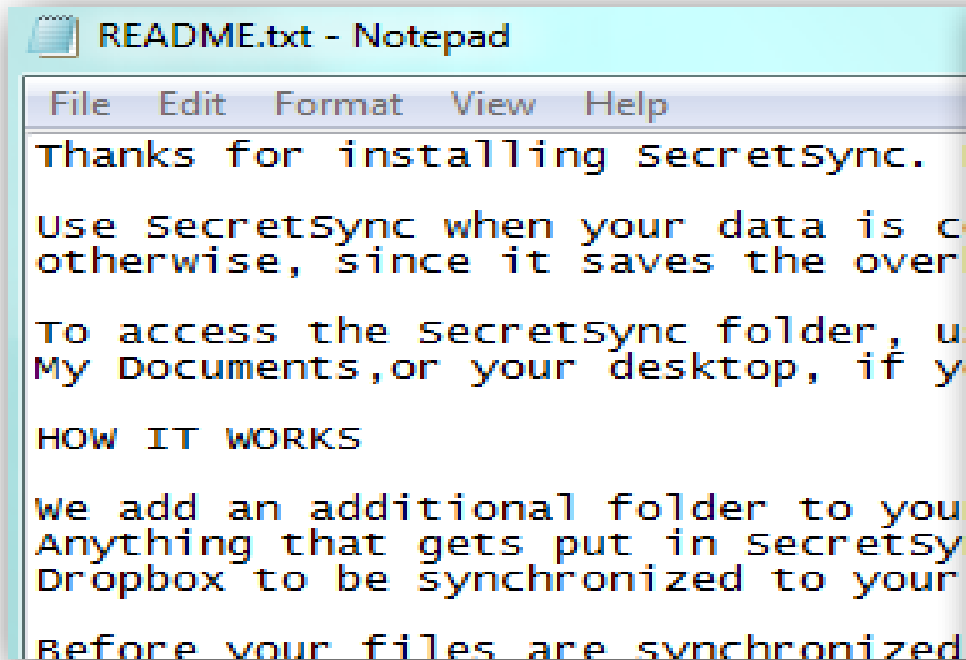
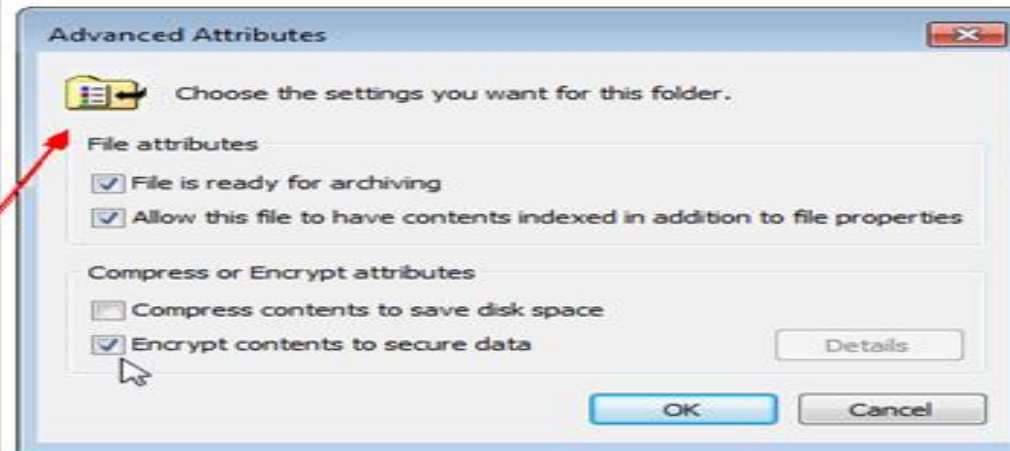
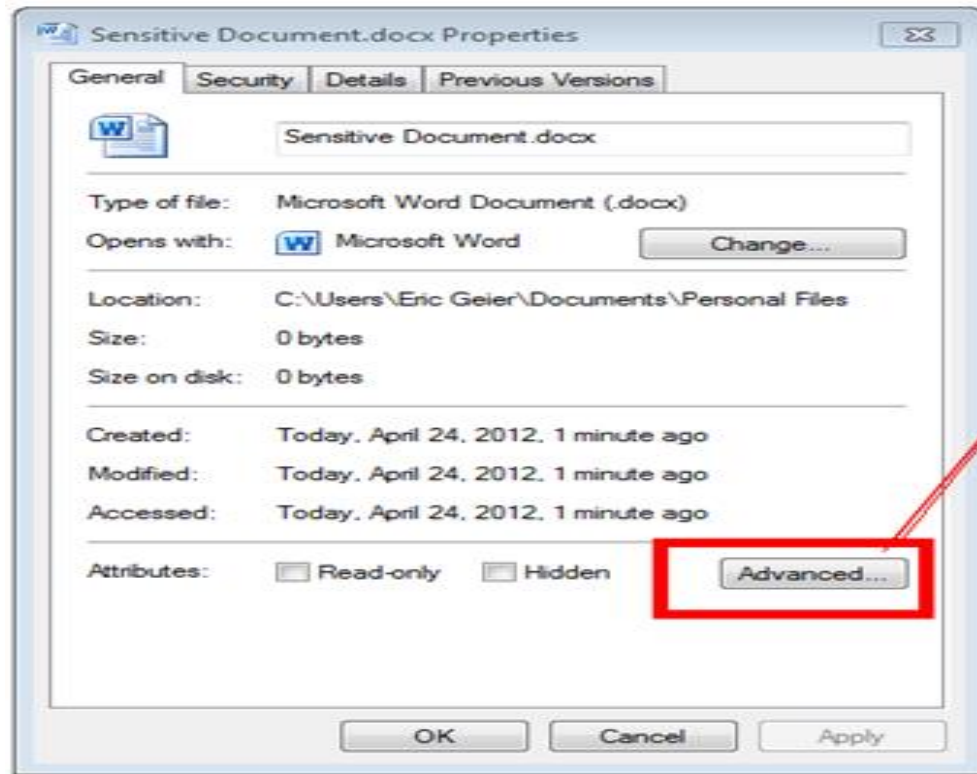
Attacchi principalmente di malware, ma anche insider threat e cyberspionaggio

Crittografia

08

CRITTOGRAFIA

Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili



Procedure

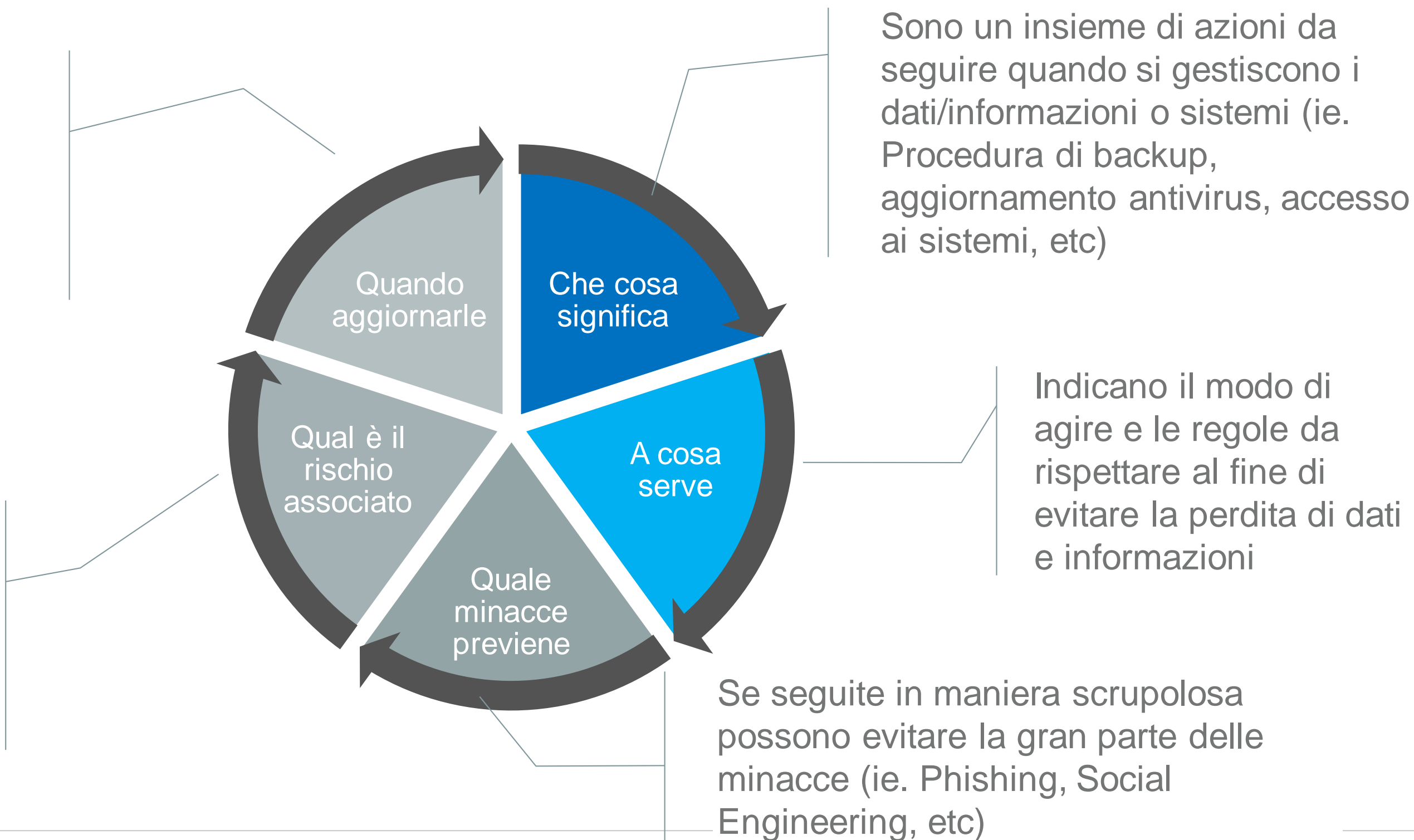
09

PROCEDURE

Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

Vanno rivisionate almeno una volta l'anno. Tramite dei piani di Audit a cui va seguito un piano di Remediation

Seguirle diminuisce il rischio di perdita dei dati ed aumenta il valore del Brand. ie. GDPR, ISO27001 , etc



Accessi

10

ACCESSI

Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

Configurando opportuni sistemi di protezione perimetrale come Firewall o IDS. Tracciando tramite i LOG di accesso le operazioni effettuate dagli utenti

Sono delle tecniche utilizzate per l'identificazione di accessi anomali

Se si identificano accessi da parte di soggetti non autorizzati il rischio di data leak associato è molto alto. Lo stesso vale in caso di attacco dall'esterno

Principalmente a identificare e prevenire accessi anomali da parte di soggetti ad aree non pertinenti o attacchi esterni



Insider Threat e malware, Ddos, etc

Accessi

10

ACCESSI

Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

The screenshot shows the Windows Event Log Explorer interface. The left pane displays the 'Computers Tree' with 'TORNADO (local)' selected. The right pane shows a list of 110 events, with the 'Security' log selected. The table below represents the data shown in the event list.

Type	Date	Time	Event	Source	Category	User	Computer	Description
Audit Success	13.05.2008	0:33:40	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:33:47	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:46	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:35	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:26	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	12:05:08	576	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Speci
Audit Success	12.05.2008	12:05:08	528	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Succe
Audit Success	12.05.2008	12:05:08	552	Security	Logon/Logoff	\SYSTEM	TORNADO	Logon
Audit Success	12.05.2008	12:05:08	680	Security	Account Logon	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	12:04:59	540	Security	Logon/Logoff	NT AUTHORITY\ANONYM	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	576	Security	Logon/Logoff	NT AUTHORITY\LOCAL S	TORNADO	Speci
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	NT AUTHORITY\LOCAL S	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	576	Security	Logon/Logoff	NT AUTHORITY\NETWO	TORNADO	Speci
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	NT AUTHORITY\NETWO	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	\SYSTEM	TORNADO	Succe
Audit Success	12.05.2008	12:03:36	513	SECURITY	System Event	N/A	TORNADO	Windc
Audit Success	12.05.2008	12:03:34	538	Security	Logon/Logoff	TORNADO\Michael	TORNADO	User L
Audit Success	12.05.2008	12:03:29	551	Security	Logon/Logoff	TORNADO\Michael	TORNADO	User i
Audit Success	12.05.2008	11:53:38	576	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Speci
Audit Success	12.05.2008	11:53:38	528	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Succe

The description pane for the selected event shows the following details:

Logon attempt using explicit credentials:
Logged on user:
User Name: Michael
Domain: TORNADO
Logon ID: (0x0,0x20E14)
Logon GUID: -
User whose credentials were used:
Target User Name: Administrator
Target Domain: TORNADO
Target Logon GUID: -
Target Server Name: mike-mobile.FSPRO.internal

Conclusioni

Esistono diversi rischi e minacce nel mondo dell'IT, ognuna della quali ha un impatto sull'operatività e sui dati diversa.

Oltre ai 10 elementi e regole da seguire per un corretto uso in sicurezza dei nostri dati, ne **esiste una 11esima, legata alla possibilità di sottoscrivere un contratto assicurativo in caso di data breach o attacco informatico**. Dove però la responsabilità primaria ricade sempre nel Titolare del dato stesso.

Non esiste un livello di sicurezza massimo, ma il tutto si basa sulla consapevolezza del singolo rispetto alla percezione del rischio.

L'Human Factor è l'elemento essenziale da considerare nonché l'elemento più debole della catena.
