



Università degli Studi di Salerno

Dipartimento di Informatica

Corso di Laurea in Informatica

Tesi di Laurea di I livello

Privacy Literacy: analisi ed implementazione

Relatrice

Ch.ma Prof.ssa

Delfina Malandrino

Candidata

Luisa Cauteruccio

Mat. 0512103478

Anno Accademico 2021-2022

Abstract

Nella società odierna tutto è diventato digitalizzato ed è semplice svolgere delle operazioni quotidiane attraverso semplici click: come ordinare la spesa, la cena, prenotare un viaggio, effettuare riunioni di lavoro a distanza di km, pulire la casa senza esserci effettivamente dentro ecc.. Svolgere queste azioni in questo maniera è diventata un'abitudine ormai intrinseca all'interno delle nostre vite e dispositivi come smartphone, tablet, dispositivi IoT e assistenti vocali sono ormai indispensabili nelle nostre giornate. Oltre i vantaggi che questi dispositivi offrono, sono anche in grado di raccogliere e archiviare dati di chi interagisce attivamente con loro ma anche dei soggetti che si trovano nello stesso ambiente. Risulta importante sapere utilizzare questi dispositivi in maniera responsabile in modo da poter usufruire dei vantaggi offerti e riuscire a proteggere le nostre informazioni in modo da evitare di subire attacchi alla privacy. Nel corso di sviluppo della tesi sono stati messi in evidenza i principali attacchi alla privacy mostrando la loro origine, le varie tipologie e le tecniche di attacco e le buone norme da conoscere ed utilizzare per evitare di subire un attacco alla privacy. Lo scopo di questa tesi è quello di sensibilizzare gli utenti sul tema della privacy con l'obiettivo

di insegnare l'importanza della privacy e della privacy dei dati online affinché siano in grado di tutelare i propri dati. Sono state svolte svariate indagini suddividendo gli utenti in varie categorie in base alla propria fascia d'età per conoscere quanto gli utenti siano alfabetizzati sul tema privacy. E' stato studiato il caso Instagram e la violazione degli account, uno dei furti d'identità più frequenti di questo periodo, mostrando le varie tecniche utilizzate per eseguire il "furto" e come recuperare il proprio account. Inoltre, sono stati evidenziati due tipologie di sistemi inerenti alla privacy: sistemi che tutelano la privacy degli utenti, come applicazioni VPN o browser più affidabili che non raccolgono i dati degli utenti bloccando tracker di terze parti; e sistemi che hanno come obiettivo quello di insegnare la privacy, purtroppo i sistemi dedicati all'insegnamento risultano ancora oggi pochi. Pertanto, si è pensato alla creazione di un sistema web che si occupi di insegnare la privacy ai propri utenti, attraverso tre sezioni principali: una sezione di studio all'interno della quale l'utente può apprendere le informazioni riguardanti la privacy; una sezione di test all'interno della quale l'utente può allenarsi; e una sezione di giochi all'interno della quale l'utente può imparare divertendosi. Il sistema presenta come prima funzionalità il "test principale", si tratta di un quiz formato da varie domande inerenti al tema privacy, alla fine del test, l'amministratore del sistema verrà a conoscenza del livello di preparazione dell'utente e l'utente potrà usufruire di tutti i vantaggi dell'applicazione al fine di imparare a conoscere l'importanza della privacy e di tutelare i propri dati.

Indice

1	Introduzione	1
2	La privacy	4
2.1	La privacy dei dati online	4
2.2	La privacy nella società attuale	6
2.2.1	Smartphone e sicurezza	8
2.2.2	Smart Assistant	9
2.2.3	Internet of things	10
2.3	Attacchi alla privacy	11
2.3.1	Malware	11
2.3.2	Phishing	19
2.3.3	Password forti e sicure	22
2.3.4	Attacchi sulle password compromesse	23
2.4	Leggi a tutela della privacy	26
2.4.1	Principi del GDPR	27
2.4.2	Protagonisti del GDPR	29
2.4.3	Conclusione - Dieci punti riassuntivi	36

3	Stato dell'Arte	38
3.1	Conoscenza e disinformazione sul tema della privacy nelle varie fasce di eta	38
3.1.1	Minori e privacy	38
3.1.2	Pre-adolescenti e adolescenti	39
3.1.3	Adolescenti	41
3.1.4	Adulti	44
3.2	Il caso Instagram e la violazione degli account	47
3.3	Sistemi esistenti che tutelano la privacy e sistemi che insegnano la privacy	50
3.3.1	Sistemi che proteggono i dati	50
3.3.2	Sistemi che insegnano la privacy	53
4	Progettazione del sistema	56
4.1	Ideazione del sistema	56
4.2	Progettazione	58
5	Il sistema "privacy for you"	70
5.1	Spring	70
5.2	Spring Boot	76
5.3	Implementazione del sistema	77
5.3.1	Infrastruttura	78
6	Conclusioni	89

Capitolo 1

Introduzione

Grazie al progresso tecnologico della nostra società possiamo considerare lo smartphone come un “fedele compagno” all’interno delle nostre vite, insieme a tutti gli altri dispositivi smart che utilizziamo giornalmente. Queste innovazioni sono state subito accettate e apprezzate dagli utenti per i vantaggi dei quali godono, come la facilità di svolgere operazioni quotidiane attraverso semplici click senza doversi “spostare” ma semplicemente collegandosi a un wi-fi o con la propria connessione dati. Questi dispositivi così utili ed efficaci in realtà sono in grado di raccogliere ed archiviare i dati che noi gli diamo in input, ma non solo, raccolgono dati, informazioni e abitudini anche quando chiacchieriamo tranquillamente con un amico, senza utilizzarli in maniera attiva. Pertanto, risulta importante tutelare i nostri dati, ma soprattutto conoscere quali dati vengono raccolti, essere a conoscenza che i nostri dati se non protetti adeguatamente possono subire degli attacchi e in che modo questi attacchi vengono effettuati, quali sono le situazioni a rischio che commette un utente per essere poi vittima di un attacco oppure

le informazioni fondamentali per riconoscere un determinato attacco in modo da evitarlo. Informare l'utente che esistono delle leggi che tutelano i nostri dati online già da tempo, infatti nel corso della tesi vengono mostrate le leggi che sono state emanate in precedenza per la tutela dei dati personali e le leggi che sono attualmente in vigore. Per riuscire a comprendere meglio il "problema" privacy è stato necessario conoscere la preparazione di un campione di utenti, suddivisi in base alle proprie fasce di età, ed è stato notato che il tema della privacy è tutt'ora poco conosciuto. Effettuare un report sugli attuali sistemi esistenti che si occupano della privacy, suddivisi in due categorie: sistemi esistenti che proteggono la privacy degli utenti e sistemi esistenti che insegnano la privacy, notando però che sono ancora pochi i sistemi dedicati all'insegnamento della privacy. Per risolvere questo problema ed ottemperare alla scarsa preparazione degli utenti sul tema della privacy e alla scarsa presenza sul mercato di sistemi che insegnano agli utenti a tutelare i propri dati, si è pensato di creare un sistema che ha come scopo principale proprio quello di preparare l'utente sul tema della privacy mostrando anche i rischi nei quali potrebbe incorrere, partendo proprio dalle lacune dell'utente sul tema. Infatti, il sistema presenta come prima funzionalità il "test principale" un quiz formato da varie domande tutte inerenti il tema della privacy, una volta effettuato il test, l'amministratore del sistema sarà in grado di conoscere le lacune dell'utente in modo da riuscire a colmarle attraverso tre sezioni principali, una sezione di studio all'interno della quale l'utente potrà apprendere gli argomenti, una sezione di test all'interno della quale l'utente potrà allenarsi e una sezione di giochi all'interno della quale l'utente potrà imparare giocando. L'intero sistema

è coordinato dalla figura di un amministratore che si occupa di gestire e controllare i comportamenti degli utenti e sottomettere a questi ultimi argomenti di studio e test in base alle loro esigenze, con l'obiettivo finale di migliorare la preparazione degli utenti sul tema della privacy.

Capitolo 2

La privacy

2.1 La privacy dei dati online

Il termine “privacy” viene definito dal Cambridge Dictionary come: “someone’s right to keep their personal matters and relationships secret” as well as “the right to be alone and do things without other people seeing or hearing you”. Le origini al diritto alla privacy risalgono ad un saggio di due giuristi statunitensi Samuel Warren e Louis Brandeis. La privacy viene definita come un diritto intoccabile, che protegge sia le proprietà materiali che immateriali. La rilevanza dell’aspetto immateriale della privacy venne affermata per la prima volta nel 1890, nell’articolo di revisione della legge “Il diritto alla privacy”. Infatti, secondo Warren e Brandeis la privacy è il diritto ad essere lasciati soli e il diritto alla riservatezza della propria sfera privata, a non subire intrusioni indesiderate nella propria vita intima. La privacy si definisce anche come: “Ability of individuals to control when, how, and to what extent their personal information is accessed” ossia la

capacità che hanno gli individui di controllare quando, come e in che misura le loro informazioni personali sono accessibili. Si tratta di un complesso di informazioni personali riservate, con lo scopo di salvaguardarle e tutelarle, impedendone quindi la divulgazione senza autorizzazione. Quando si fa riferimento al diritto alla privacy si intende il diritto a non essere soggetto a violazioni non autorizzate della privacy da parte del governo, delle società o degli individui, tale concetto appartiene alle leggi sulla privacy di molti paesi e, in alcuni casi, delle costituzioni. Inoltre è definito anche come il diritto alla riservatezza della propria vita privata e al controllo dei propri dati personali. Tale dichiarazione è presente all'interno de " il codice privacy", Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali, la cui finalità era quella di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato (con riferimento alla riservatezza), dell'identità personale e del diritto di protezione dei dati personali. I dati che vengono trattati nell'ambiente privacy sono:

- Dati personali o identificativi (definito anche nell'articolo 4 del GDPR): qualsiasi informazione riguardante una persona fisica identificata o identificabile: nome, numero di identificazione, dati relativi all'ubicazione, identificativo, indirizzo IP, marcatori personali (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza, traffico telefonico, immagini, dati di geolocalizzazione, dati genetici e biometrici.
- Dati genetici : dati personali relativi alle caratteristiche genetiche

ereditarie o acquisite di una persona fisica (informazioni univoche sulla fisiologia o sulla salute di tale persona fisica)

- Dati biometrici: dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica (immagine facciale o i dati dattiloscopici).
- Dati particolari di dati personali (ex-sensibili, presenti nell’articolo 9 del GDPR): dati personali che rilevino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, l’orientamento sessuale.
- Dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona, comprese le prestazioni di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute.

Esaminando tale elenco possiamo notare come molte di queste informazioni sono presenti sui nostri profili social, o sui siti di e-commerce che utilizziamo più spesso. Lo scopo di questa tesi è far conoscere quelli che sono i rischi di condividere troppo facilmente queste informazioni senza proteggerle, quindi insegnare “come” conservarle e proteggerle, evitare che vengano divulgate e in tal caso riuscire a riottenerle.

2.2 La privacy nella società attuale

I progressi ottenuti nell’ambito tecnologico di quest’epoca hanno dato vita a una società “digitalizzata” all’interno della quale risulta agevole svolgere delle operazioni quotidiane attraverso semplici “click” o comandi vocali,

grazie all'utilizzo di dispositivi come Alexa, creata da Amazon nel 2014 oppure Google Assistant di Google, Siri di Apple o Cortana di Microsoft che fanno parte della nostra quotidianità, nelle nostre case, auto, giochi ecc. . . Questi vantaggi apportati dal progresso tecnologico hanno permesso anche di aumentare la capacità di raccolta, archiviazione e condivisione di informazioni. Rendendo difficile per un individuo conoscere tutte le informazioni personali a cui altri potrebbero avere accesso. Le informazioni che sono maggiormente a rischio sono:

- Informazioni personali come: data di nascita, indirizzi di casa o ufficio, foto, contatti personali, messaggi, stato delle relazioni.
- Dati sulla localizzazione di un utente, la posizione geografica in cui un utente si trova in un determinato momento.
- Dati e misure biometriche, tramite l'utilizzo di sensori, come: battito cardiaco, ossigenazione del sangue, id del viso, impronte digitali.
- Dati tramite il comando vocale dei dispositivi IoT o semplicemente il microfono del nostro smartphone.

La condivisione di tali informazioni potrebbe portare dei rischi come:

- Identity theft o furto di identità.
- Profiling: record di dati sulla base del comportamento degli utenti.
- Stalking: tracciamento indesiderato sulla base dei dati raccolti in tempo reale.

- La rilevazione di dati sanitari potrebbe portare dei rischi sia in campo lavorativo o in casi di assegnazioni di assicurazioni e in alcune situazioni tramite queste informazioni gli utenti hanno subito anche delle discriminazioni.

2.2.1 Smartphone e sicurezza

Molto spesso capita di notare che il nostro smartphone possiede delle informazioni personali senza che l'utente le abbia inserite in maniera attiva attraverso qualche form o tramite l'utilizzo di qualche applicazione specifica. Questo perché i sensori degli smartphone e in particolar modo i microfoni sono attivi anche quando non stiamo utilizzare il nostro dispositivo. In questo modo vengono raccolte informazioni per fini terzi, come ad esempio per attività di marketing. L'utilizzo del microfono è richiesto tra le autorizzazioni di accesso al momento dell'installazione di un'applicazione, ma molto spesso gli utenti tendono ad accettare senza informarsi in maniera adeguata. Il garante privacy ha avviato un'indagine sulle app più scaricate dagli utenti e testando come queste acquisiscono dati attraverso i microfoni dei nostri dispositivi. “La prima linea di difesa è sempre la consapevolezza”, afferma il garante privacy dicendo che se gli utenti vogliono evitare di essere esposti ad eventuali ascolti indiscreti possono utilizzare delle semplici ma fondamentali accortezze.

1. Limitare il numero di app installate sullo smartphone, decidendo di installare solo quelle che considerano davvero utili. In quanto maggiori

sono le app installate sul nostro smartphone, maggiori saranno i dati che vengono raccolti, trattati e diffusi.

2. Le app richiedono il permesso di accedere a vari sensori e funzionalità e ai nostri dati, prima di accettare, si consiglia di valutare se queste informazioni servono ai fini dell'utilizzo dell'app che abbiamo scelto di utilizzare. Se in caso l'utente decide di accettare, si consiglia di leggere con attenzione l'informativa sul trattamento dei dati personali.
3. Anche quando l'utente ha concesso alle app l'autorizzazione per i sensori o il microfono può comunque sempre decidere di disattivare il permesso di utilizzo.

2.2.2 Smart Assistant

Altra grande novità del progresso tecnologico degli ultimi tempi è l'assistente digitale. Si tratta di un programma che interpreta il linguaggio naturale grazie all'utilizzo di algoritmi di intelligenza artificiale, pertanto è in grado di dialogare con gli umani e soddisfare le loro richieste. Gli assistenti digitali sono in grado di raccogliere e memorizzare una grande quantità di dati, non solo quelli di chi interagisce direttamente con il dispositivo sul quale è presente l'assistente digitale ma anche i dati delle persone che si trova nello stesso ambiente, come:

- Scelte, preferenze e abitudini
- Caratteristiche biometriche
- Geolocalizzazione

- Stati emotivi

Risulta quindi importante saper utilizzare questa tecnologia in modo informato e consapevole, per tutelare in maniera adeguata i nostri dati e di tutte le persone che entrano, volontariamente o meno, nel campo di azione di un'assistente digitale. Il garante privacy mostra dei consigli su come utilizzare al meglio lo smart assistant proteggendo i dati personali suggerendo di leggere attentamente l'informativa sui dati personali. Nel caso in cui per attivare l'assistente digitale o eventuali app di gestione di quest'ultimo è necessario registrarsi inserendo le nostre informazioni personali, consiglia di fornire solo quelle strettamente necessarie. Non utilizzare l'assistente digitale per memorizzare informazioni delicate come quelle relative alla nostra salute, password o numeri delle carte di credito. Disattivare l'assistente digitale quando non viene utilizzato. In quanto, se l'assistente è acceso ma non viene utilizzato entra in uno stato "passive listening", ascoltando lo stesso ciò che viene detto nell'ambiente circostante anche se non si interagisce personalmente con esso, tramite il microfono del dispositivo su cui è installato. Inoltre, si consiglia di cancellare periodicamente la cronologia del dispositivo.

2.2.3 Internet of things

Quando si fa riferimento all'IoT si tratta di oggetti smart thing. Uno smart thing è un oggetto fisico che è aumentato digitalmente grazie a sensori, attuatori, computazione e interfacce di comunicazione. Si tratta di una rete globale di oggetti interconnessi univocamente indirizzabili, basata su protocolli standard di comunicazione.

2.3 Attacchi alla privacy

Gli attacchi informatici, ma soprattutto gli attacchi alla privacy, consistono proprio nell'hackeraggio o possesso da parte di altre persone dei nostri dati personali, come indirizzi o numeri di carta di credito, foto, video ecc.. Esistono vari tipi di attacchi informatici relativi alla nostra privacy tra questi troviamo:

- Malware
- Phishing
- Attacchi sulle password compromesse
- Sql Injection Attack
- Cross-site Scripting (XSS)
- Denial of Service (Dos)
- Session Hijacking and Man-in-the-Middle Attacks

2.3.1 Malware

I malware sono i fenomeni più rilevante della parte oscura del web e degli attacchi alla privacy. Il termine “malware” deriva da malicious e software. Si tratta infatti di programmi realizzati per danneggiare i sistemi su cui vengono eseguiti o per sottrarre informazioni sensibili. Esistono 3 grandi categorie di malware:

- I virus: sono programmi realizzati per creare danni e successivamente propagarsi inserendosi all'interno di file.

- I worm: non hanno lo scopo di danneggiare il sistema direttamente, ma si auto replicano per saturare le risorse di sistema e di rete.
- I trojan horse malware nascosti all'interno di legittime applicazioni software che non godono di proprietà come la replicazione e la propagazione.

Oltre a questi ne esistono altri 2 tipi di malware che sono molto diffusi:

- Ransomware: impedisce l'accesso ad aree del proprio computer, che vengono bloccate e criptate. Per ottenere nuovamente l'accesso viene chiesto il pagamento di un riscatto.
- Backdoor: permette di accedere da remoto ad un pc e a tutte le sue funzioni, ottenendone parziale o completo possesso.

Esistono altri tipi di attacchi che fanno parte della famiglia dei malware:

- Adware: software indesiderati che visualizzano messaggi pubblicitari sullo schermo, spesso all'interno delle finestre del browser. Gli adware riescono a mascherarsi da componenti legittimi o nascondersi all'interno di un altro programma alla fine di provocarne con l'inganno l'installazione sul dispositivo.
- Spyware: una particolare tipologia di malware progettata per spiare le attività dell'utente sul computer, senza autorizzazione per poi comunicarle a chi ha sviluppato il codice malevolo.
- Rootkit: consentono agli hacker di ottenere i privilegi da amministratore sul sistema infetto. Vengono progettati per restare nascosti agli utenti, sia degli altri software e dal sistema operativo stesso.

- **Keylogger:** si tratta di codice malevolo che è in grado di registrare tutto ciò che la vittima digita sulla tastiera, inviando le informazioni rilevate agli hacker, in modo che quest'ultimi sono in grado di rubare informazioni sensibili.
- **Cryptominer:** noto anche come drive-by mining o cryptojacking, si tratta di una tecnica malware che prevede l'installazione di un trojan e consente agli hacker di utilizzare le risorse hardware della macchina infetta per “generare” criptovalute.
- **Exploit:** codice malevolo che sfrutta i bug e le vulnerabilità del sistema operativo o delle applicazioni consentendo agli hacker di prenderne il controllo remoto.

Un malware indipendentemente dalla sua tipologia presenta un ciclo di vita formato da varie fasi che sono:

- **Infezione:** il malware si introduce all'interno del sistema, superando eventuali barriere di sicurezza e si installa al suo interno. In seguito, modifica le impostazioni del sistema adattandole alle proprie necessità, la più importante quella di non essere rilevato.
- **Quiescenza:** il codice virale rimane residente in memoria, in attesa che si realizzi una determinata condizione, a seguito della quale si attiva (esecuzione delle azioni malevole e replicazione). Queste ultime possono essere ripetute più volte, quindi la fase si protrae fino ad una eventuale eliminazione da parte del codice stesso o di un software anti-malware.

- Replicazione e propagazione (solo per virus e worm): al determinarsi di certi eventi o condizioni, il malware si replica e seleziona i bersagli verso cui propagarsi, infettando altri sistemi.
- Azioni malevole: al verificarsi di certi eventi o condizioni, il codice virale esegue i propri compiti malevoli, come distruzione o furto dei dati del sistema. Se il sistema non viene compromesso definitivamente, il software ritorna nella fase di quiescenza.

I malware sono diffusi tipicamente tramite internet o mediante messaggi di posta elettronica, ma esistono numerosi altri metodi differenti utilizzati per diffondere e infettare i dispositivi:

- File dannosi allegati a email di phishing
- Collegamenti URL dannosi nel testo di un email
- Drive-by download
- Dispositivi USB infetti
- Intrusioni dirette nelle reti locali
- Vulnerabilità del sistema operativo o delle applicazioni installate sui dispositivi
- Applicazioni per dispositivi mobile scaricati da app store non ufficiali

Come riconoscere un malware

McAfee, azienda che si occupa della sicurezza informatica, ha pubblicato nel Novembre del 2021 un articolo nel quale enuncia i 5 sintomi che dovremmo

notare sul nostro dispositivo, se questo è stato infettato da un malware. Innanzitutto tale azienda mette subito in risalto l'instabilità del dispositivo infetto che stiamo utilizzando sia che si tratti di uno smartphone o un pc e anche la grande capacità del malware di non essere visibile e agire in background inviando informazioni sensibili a terze parti senza interrompere le altre funzioni. Pertanto, afferma che è molto importante prestare attenzione ai sintomi sotto descritti:

- Il dispositivo risulta caldo al tatto: se si scarica accidentalmente un malware, i componenti interni del dispositivo iniziano immediatamente a lavorare più intensamente per supportare il malware o il virus incorporato.
- Rallentamento: se il dispositivo che stiamo utilizzando è stato infettato da un malware, potremmo notare un rallentamento del caricamento di siti web, l'arresto anomalo di app o l'interruzione della carica della batteria. Le prestazioni complessive restano lente, nonostante i riavvii o l'eliminazione di file di grandi dimensioni.
- Aumento di popup casuali o nuove app: se il dispositivo che stiamo utilizzando è stato infettato tramite l'installazione di un'applicazione dannosa o un virus, potrebbero verificarsi degli aumenti di popup casuali e visualizzare un'applicazione che non è stata scaricata direttamente dall'utente proprietario.
- Link fraudolenti dai tuoi account: è frequente che il malware ottenga l'accesso all'elenco dei contatti e poi gli utilizzi per inviarli, in modo da

diffondersi e infettare altri dispositivi. La comunicazione può avvenire tramite email o attraverso gli account dei social media.

- Addebiti non autorizzati: potrebbe trattarsi di un app infetta che effettua acquisti a tuo nome o di un malware che ha carpito le informazioni personali per effettuare acquisti fraudolenti.

Come proteggere i nostri dispositivi

- Installare sempre gli aggiornamenti: assicurarsi di installare e mantenere aggiornate le funzionalità di sicurezza del nostro dispositivo. Gli aggiornamenti regolari forniscono le funzionalità di sicurezza sempre più recenti, alcune delle quali vengono sviluppate appositamente per contrastare attacchi specifici. Inoltre, è consigliato installare un software di sicurezza completo per bloccare malware e virus.
- Utilizzare password complesse e uniche: le password scelte per i nostri account o dispositivi devono essere lunghe almeno 8 caratteri, formate da lettere, numeri e simboli alfanumerici.
- Conoscere le app che sono installate sul nostro dispositivo: è fortemente consigliato scaricare le app solo da fonti affidabili evitando le app di terze parti. Prima di procedere all'installazione è bene informarsi leggendo le recensioni. La prassi migliore è quella di usare solo app presenti sull'app store o negli app store associati e verificati.
- Non cliccare link poco affidabili.

- Bloccare le impostazioni e limitare le autorizzazioni delle app: un ottimo modo per bloccare le minacce informatiche è rendere tutti gli account più privati possibili e limitare le autorizzazioni delle app, in modo da fornire personalmente le autorizzazioni alle app.
- Cancellare la cronologia di navigazione: controllare attentamente la cronologia del browser e i dati. Se si nota un link sospetto, bisogna eliminarlo, anche se è fortemente consigliato cancellare l'intera cronologia.

Come procedere se un dispositivo è infetto

- Installare un software di sicurezza che aiuta ad identificare il malware in modo da poter ripulire il dispositivo e proteggerlo in futuro.
- Eliminare le app che non sono state scaricate personalmente dall'utente, rimuovere i messaggi di testo rischiosi, cancellare la cronologia e svuotare la cache.
- Se la minaccia è fortemente invalidante è consigliato, ma in alcuni casi obbligatorio per il corretto funzionamento, ripristinare i dati di fabbrica.
- Una volta ripuliti i dispositivi cambiare le password.

Come rimuovere un malware

La rimozione dipende strettamente dal dispositivo che stiamo utilizzando, in base a quello ci sono passaggi differenti da seguire per la rimozione del malware:

- Da pc Windows: gli strumenti da utilizzare sono due, la sicurezza di windows e windows defender offline che permette di effettuare un'analisi del pc alla ricerca dei malware impiegando 15 minuti e poi il pc verrà riavviato. Dopo l'analisi è possibile visualizzare i risultati nella cronologia di protezione.
- Da Mac o Iphone: all'interno dei dispositivi è presente il supporto malware attraverso una pagina che mostra all'utente la protezione dai malware effettuata da macOS. La protezione verso i malware viene sviluppata attraverso 3 livelli di difesa che sono:
 - Impedire l'avvio e l'esecuzione di malware: App Store o Gatekeeper combinati con l'autorizzazione. Questo primo livello è progettato per inibire la distribuzione del malware e impedirne l'avvio anche una sola volta. Questo è l'obiettivo di App Store e Gatekeeper, insieme al processo di autorizzazione.
 - Il secondo livello si interessa di bloccare l'esecuzione del malware sui sistemi dei clienti: Gatekeeper, autorizzazione e XProtect. Questo livello di difesa successivo serve per garantire che nel caso in cui un malware compaia su un dispositivo Mac, questo deve essere subito identificato e bloccato sia per proteggere la diffusione e anche per proteggere gli altri dispositivi Mac collegati che potrebbero essere infettati.
 - Intervenire in caso di esecuzione di malware: XProtect. Se il malware non è stato bloccato in tempo bisogna utilizzare XProtect che elimina il malware che è andato in esecuzione.

- Da android: il supporto di Google mette a disposizione una guida su come rimuovere un malware o un software non sicuro. Google ci mostra quelli che possono essere 2 segnali che potrebbero annunciare la presenza di malware:

- Disconnessione dal proprio account
 - Segnali sospetti sul dispositivo che non scompaiono tipo pop-up
1. Il primo passaggio è assicurarsi che GoogleProtect sia attivo
 2. Poi bisogna verificare se ci sono aggiornamenti della sicurezza disponibili e del dispositivo Android
 3. Rimuovere le app non attendibili
 4. Eseguire un controllo di sicurezza

Se notiamo ancora qualcosa di strano sul nostro dispositivo, Google consiglia di ripristinare il dispositivo ai dati di fabbrica o contattare il produttore del dispositivo.

2.3.2 Phishing

Il phishing è un attacco informatico genere truffa telematica. L'obiettivo è quello di ottenere informazioni e dati personali degli utenti. È l'attacco più comune degli ultimi tempi. L'utente viene ingannato tramite la ricezione di messaggi e mail contenenti un messaggio allarmante ad esempio sui propri conti bancari, contenente un link attraverso il quale possiamo risolvere il problema. Il link riporta a un sito falso ma riprodotto molto bene. Il garante della privacy definisce chi effettua attacchi di tipo phishing come "i pescatori"

di dati. L'utente viene quindi adescato e compila il form. Il rischio in questo caso è duplice:

1. L'utente inserisci i propri dati che verranno poi utilizzati da terzi.
2. L'accesso al sito potrebbe infettare il dispositivo con malware e trojan horse.

Come riconoscere un attacco phishing e proteggersi

1. Controllare sempre il link e il mittente della mail prima di cliccare qualunque indirizzo, ancora meglio non cliccare sul link, ma copiarlo invece nella barra dove si inserisce l'indirizzo del browser.
2. Prima di cliccare su un qualunque link, bisogna verificare che l'indirizzo mostrato è davvero lo stesso indirizzo Internet al quale il link condurrà. Un controllo che può essere effettuato in modo semplice, passando il mouse sopra il link stesso.
3. Usare solo connessioni sicure, in particolar modo quando si accede a siti sensibili. Come precauzione minima, si consiglia di non sfruttare connessioni sconosciute né tantomeno i wi-fi pubblici, senza una password di protezione. Se vogliamo una maggiore sicurezza, abbiamo l'opportunità di installare VPN che possono cifrare il traffico, perché va ricordato sempre che in caso di utilizzo di una connessione non sicura, i cybercriminali possono reindirizzarci, senza essere visti, a pagine di phishing.

4. Controllare che la connessione sia HTTPS e verificare il nome del dominio all'apertura di una pagina. Questi fattori sono importanti soprattutto quando si usano siti che contengono informazioni sensibili, come pagine per l'online banking, i negozi online, i social media e via discorrendo.
5. Non condividere mai i propri dati sensibili con terze parti. Le compagnie ufficiali non chiedono mai informazioni del genere via email.

Se si è vittima di un attacco di phishing è consigliato rivolgersi alla polizia postale. Il garante privacy nel Novembre del 2020 ha pubblicato una guida sul phishing e su come proteggersi, affermando che “la prudenza non è mai troppa”, consigliando agli utenti di installare e mantenere aggiornato sui propri dispositivi un programma antivirus che protegga anche dal phishing. Inoltre, consiglia di controllare che siano adeguatamente attivate le impostazioni riguardanti le email spam che i gestori di posta elettronica hanno integrati al loro interno per proteggere i propri utenti da un attacco phishing. Il garante privacy afferma che è meglio non memorizzare dati personali e codici di accesso nel browser. Per proteggere i conti bancari, postali o le carte di credito consiglia di controllare spesso i movimenti sulle nostre carte e attivare sistemi di alert che avvisano ogni qualvolta viene effettuata un'operazione. Nel caso in cui si ha il dubbio di essere stato vittima si consiglia di contattare direttamente la banca o il gestore delle carte di credito, attraverso i canali di comunicazione ufficiali. Inoltre, ricorda che utenze come banca o poste non contattano in questo modo i proprio clienti. Per quanto riguarda

gli acquisti online, il garante privacy consiglia l'utilizzo di carte di credito prepagate o altri sistemi di pagamento che evitano la condivisione dei dati.

2.3.3 Password forti e sicure

Navigando in rete è possibile trovare varie guide che mostrano quali sono i requisiti per creare una password che sia forte e sicura:

- Lunghezza: utilizzare almeno 8 caratteri, ma sono fortemente consigliate password formate da 12 caratteri.
- Tipi di caratteri da utilizzare:
 - Numeri da 0-9
 - Lettere 52 tipi: 26 caratteri maiuscoli e 26 minuscoli
 - Caratteri speciali presenti sulla tastiera 33
- Mista: combinare quanto è più possibile i tipi di caratteri sopra descritti.
- Senza senso: evitare nomi, o parti di parole che sono facili da trovare facilmente anche in un semplice dizionario
- Non utilizzare sequenze o caratteri ripetuti
- Non utilizzare parole scritte al contrario
- Non utilizzare informazioni personali e familiari: nomi, date importanti, numero di patente ecc. . .
- Cambiare la password periodicamente

2.3.4 Attacchi sulle password compromesse

Quasi ogni giorno si registrano data breach cioè violazione dei dati di servizi web. Il “dark web” è colmo di database che custodiscono password rubate con lo scopo di ricavarne denaro. La figura protagonista è definita cyber crime che mette in vendita le password rubate, vendendole a chi poi le userà per compiere altri attacchi alla sicurezza. Questa categoria di attacco informatico può essere schematizzata in 4 fasi che sono:

1. Password reuse: riutilizzo delle stesse password in servizi differenti
2. Credential stuffing: riempimento delle credenziali
3. Account takeover: acquisizione dell’account
4. Furto d’identità

Password reuse

Il “password reuse” è la tendenza ad utilizzare la stessa password per diversi servizi online. Molte volte gli utenti tendono ad agire in questo modo perché è più semplice ricordare una sola password anziché tante e diverse. Utilizzare sempre la stessa password per più siti o per tutti è uno degli errori più gravi che un utente possa commettere, in quanto un hacker violando i server di un sito può “rubare” tutte le password e se queste vengono utilizzate per più siti allora sono a rischio anche le altre informazioni che abbiamo inserito negli altri siti. Per evitare che situazioni di questo tipo si ripresentino, si consiglia l’uso di un gestore password, la creazione e l’utilizzo di una password forte e sicura.

Credential stuffing

La fase due è quella del “credential stuffing” ossia riempimento delle credenziali, ed è una delle forme di attacco più diffuse in campo di cyber security. Fa parte della famiglia degli attacchi “brute force” sfruttando la poca attenzione alle credenziali degli utenti registrati sui sistemi. In cui si cerca di accedere ad un sito o servizio web usando credenziali di accesso rubate. Si tratta di un attacco portato a termine senza aggredire direttamente l'applicazione web a cui il malintenzionato accede. Vengono rubate le credenziali di accesso degli utenti iscritti ad un altro sito Web. Così un hacker può sfruttare username e password per accedere. La tecnica solitamente utilizzata è:

- Creare un archivio di username e password raccolte all'interno della rete, se non se ne dispone già di uno.
- Creare uno script (formato JSON) per accedere all'archivio oppure utilizzare un tool che permette in modo automatizzato di recuperare le credenziali rubate.
- Lanciare lo script sperando che una parte degli utenti non abbia cambiato la propria password oppure che si usi la stessa per diversi account, portando così ad un furto di identità.

Account takeover e furto di identità

Account takeover o ATO è letteralmente “acquisizione dell'account”. Una volta ottenuto l'account come sopra descritto, lo scopo dell'hacker è quello di ottenere un profitto modificando i dettagli dell'account, attraverso ope-

razioni tramite l'account stesso, compiendo quindi un furto di identità ed utilizzandolo come esca per avere l'accesso ad altri account.

Password Spray

Questo tipo di attacco colpisce utenti sconosciuti con il tentativo di superare le comuni misure di prevenzione contro gli attacchi ATO. In questo caso si utilizza un attacco bot su siti web selezionati per eseguire più tentativi di accesso utilizzando nomi utente comuni o noti. Se l'accesso non riesce e verranno effettuati altri tentativi fallimentari, verrà attivato un blocco.

SQL Injection

Si tratta di una tecnica di attacco sfruttata dagli hacker per attaccare le applicazioni web-based e i siti web.

Cross- site Scripting (XSS)

Si tratta di un tipo di vulnerabilità dei siti web che consente a chi lancia l'attacco di utilizzare script dannosi in pagine web e app, al fine di installare malware sui browser web degli utenti.

Denial of Service (Dos)

L'obiettivo di questo attacco è quello di ingolfare le risorse di un sistema informatico che fornisce un determinato servizio ai computer connessi. In una scala più ampia troviamo il DDoS che è Distributed denial of Service che consiste nel tempestare di richieste un sito fino a “distruggerlo” e renderlo

irraggiungibile. Risulta fra gli attacchi che colpiscono un'impresa ogni cinque minuti.

Session Hijacking and Man-in-the-Middle Attacks

Un tipo di attacco che consiste nel dirottamento di sessione che inganna l'utente al fine di installare malware sul suo sistema informatico. Di solito si usa un link.

2.4 Leggi a tutela della privacy

Una delle prime leggi sulla privacy in Italia è la legge 675 dal titolo “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”, in Italia venne approvata nel 1996 e nel 1999 venne affiancato il DPR 318 che conteneva le misure minime da applicare per garantire la sicurezza dei dati personali trattati dalle persone fisiche o giuridiche. Nel 2003 la legge 675 fu sostituita dal Decreto Legislativo 196: “Codice in materia di protezione dei dati personali” o anche detto “codice privacy”. Nel 2016 fu approvato il GDPR (General Data Protection Regulation). È il regolamento del 2016/679 del parlamento europeo. Questa normativa ha prevalenza su quella nazionale, essendo un regolamento europeo, quindi se una normativa italiana è in contrasto con il GDPR allora non ha valore. Per questo è stato modificato il decreto legislativo 196/2003 con il Decreto Legislativo 101/2018 nelle sezioni in cui era in contrapposizione con il GDPR. La normativa richiede che ogni paese deve istituire un DPA (Data protection Authority). In Italia questa autorità è attiva dal 1996 e ha il nome di Garante privacy che ha

l'autorità di emanare provvedimenti ossia normative supplementari, sentenze e linee guida. Dal 2018 è attivo il "Comitato dei garanti europei" che ha il compito di armonizzare gli interventi in ambito europeo emanando, ad esempio linee guida relative a specifici trattamenti. All'interno del GDPR viene definito anche il concetto di dato personale (Art 4, paragrafo 1) definito come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". Nell'articolo 4 viene esplicitato anche l'ID online (indirizzo IP, nickname) che è considerato un dato personale e quindi deve essere acquisito e trattato come un dato personale.

2.4.1 Principi del GDPR

I dati personali devono rispettare alcuni principi, che vengono presentati nell'articolo 5 del GDPR:

- Principio di liceità, correttezza e trasparenza: un trattamento è lecito e corretto se l'interessato ne è informato correttamente e se ricorrono specifiche condizioni, ossia le basi giuridiche stabilite dal GDPR negli articolo 6,9 e 10. Non sempre è possibile informare l'interessato, si tratta di situazioni particolari in questi casi vanno seguite informazioni specifiche.
- Principio di limitazione della finalità: Principio richiamato dal GDPR, art 5 comma 1 lettera b. Il titolare del trattamento prima di avviare un trattamento e raccogliere dati personali, deve determinare quali sono le finalità per cui vuole utilizzare quei dati. L'interessato deve quindi essere informato delle finalità. Il titolare può trattare i dati

esclusivamente per le finalità indicate nell'informativa. Nel caso in cui il titolare intenda successivamente trattare i dati per ulteriori e diverse finalità deve informarne l'interessato e nel caso raccoglierne il consenso.

- Principio di minimizzazione dei dati Principio richiamato dal GDPR, art 5 comma 1, lettera c. Devono essere acquisiti solo i dati necessari per conseguire le finalità per cui sono richiesti. Ad esempio, i siti web di e-commerce che chiedono agli utenti dati non pertinenti come sesso, età e professione vengono meno all'applicazione di tale principio.
- Principio di esattezza Principio richiamato dal GDPR, art 5 comma 1, lettera d. I dati devono essere esatti ed aggiornati.
- Principio di limitazione della contestazione (e diritto all'oblio) Principio richiamato dal GDPR, art 5, comma 1, lettera e: i dati non devono essere conservati più del tempo necessario alle finalità per cui sono stati raccolti. È possibile stabilire i tempi di conservazione se questi sono stabiliti dalla normativa. In Italia i dati amministrativi vanno conservati per 5 o 10 anni, dopo questo periodo vanno cancellati.
- Principio di integrità e riservatezza Principio richiamato dal GDPR, art 5, comma 1, lettera f. Devono essere attuate adeguate misure di sicurezza per evitare che i dati personali siano accessibili a persone non autorizzate e quindi trattati illecitamente, persi o distrutti. Le misure di sicurezza non devono essere solo tecniche ma anche organizzative.
- Principio di responsabilizzazione(Accountability) Principio richiamato dal GDPR, art 5, comma 2. Il titolare del trattamento dei dati per-

sonali è responsabile del rispetto dei principi sopra citati. Il GDPR esprime questo principio affermando che “il titolare è competente per il rispetto della correttezza e trasparenza dei dati e deve essere in grado di provarlo”.

2.4.2 Protagonisti del GDPR

I dati sono trattati da soggetti come:

- Titolare o controller
- Contitolare o joint controller
- Responsabile o processor
- Designato (ex responsabile interno)
- Responsabile della protezione dei dati (DPO)
- Autorizzato (ex incaricato)
- Amministratore di sistema

È importante osservare che la normativa privacy non si applica alle persone fisiche che trattano dati personali per scopi esclusivamente personali o domestici. Va applicato a professionisti o persone giuridiche. Si intende per “interessato”, la persona fisica a cui si riferiscono i dati personali. L’articolo 28 del GDPR richiede che il rapporto tra titolare e il responsabile venga formalizzato da un accordo scritto. Il GDPR si occupa non solo della protezione dei dati delle persone in generale, ma c’è anche una sezione apposita per il trattamento dei dati dei minori. Il GDPR stabilisce che per i servizi

informatici è necessario il consenso del titolare della responsabilità genitoriale per i minori di 16 anni. In Italia con il decreto legislativo del 196/2003, la soglia è stata abbassata a 14 anni. Con l'aumento di strumenti come MICROSOFT 365 e G-Suite di Google, il GDPR vieta il trasferimento di dati in paese extra-UE se non nei casi regolamentati. Prima di usare i dati, il titolare o il responsabile deve verificarne la provenienza. Se i dati stessi sono forniti dall'interessato non ci sono problemi. Discorso diverso per le imprese come campagne di marketing o per ricerche di mercato. In questo caso prima di utilizzare i dati bisogna assicurarsi di avere il consenso. All'interno dell'articolo 9 troviamo anche la definizione di dati ex- sensibili. Nell'articolo 10 vengono definiti anche i dati giudiziari che sono quelli relative alle condanne penali e ai reati o connesse a misure di sicurezza. Quando si usa il termine trattamento in inglese processing si intende qualsiasi operazione o insieme di operazioni applicate ai dati personali. Tali operazioni possono essere compiute con sistemi informatici o meno. Si fa riferimento anche ai dati personali anche quelli in formato cartaceo come le fotografie, i filmati e anche le registrazioni audio. Tali operazioni includono la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione. I dati vengono manipolati e quindi trattati per una ragione specifica, tale ragione viene individuata con il termine finalità.

Autorità di controllo (DPA) e garante privacy

L'articolo 51 del GDPR riporta "Ogni stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento". Tali autorità sono l' Autorità di controllo o Data Protection Authority. In Italia tale autorità è il Garante per la protezione dei dati personali. L'autorità di controllo si occupa di compiti come:

- Trattare i reclami degli interessati ed eventualmente emanare sanzioni ai titolari e ai responsabili.
- Svolgere indagini sull'ottemperanza alla normativa privacy e emanare le relative sanzioni.
- Emettere provvedimenti e le linee guida per l'applicazione della normativa privacy.

Le autorità di controllo devono coordinarsi tra loro per assicurare la coerenza di interpretazione nel Comitato Europeo per la protezione dei dati.

Titolare

Il titolare è quell'entità che determina la finalità e i mezzi del trattamento di dati personali o che è designato dalla normativa vigente. Il titolare del trattamento è l'entità nel suo complesso e non il legale rappresentante della stessa. Alcuni esempi di titolari sono:

- Società di autonoleggio per aziende che, una volta ricevuti i dati dalle aziende, contattano direttamente le persone che usufruiscono dei benefit.

- Fondi sociali integrativi che, una volta ricevuti i dati dalle aziende su indicazioni degli interessati contattano direttamente gli interessati stessi.
- Organismi di certificazione.
- Società di assicurazione del personale dipendente, in quanto le organizzazioni che vi ricorrono sono obbligate a farlo e non possono essere esse stesse società di assicurazione.
- Medici competenti delle organizzazione.
- INPS e INAIL che ricevono dei dipendenti delle organizzazioni.

Un titolare può comunicare i dati personali ad un altro titolare. Se il titolare non ha sede nell'Unione Europea deve indicare un rappresentante.

Contitolare

Un titolare può determinare le finalità e i mezzi del trattamento dei dati insieme ad un'altra entità che tratta a sua volta i dati per autonome finalità e prende il nome di contitolare. L'articolo 26 del GDPR richiede che venga redatto un accordo tra contitolari nel quale vengono indicate le rispettive responsabilità, le modalità in cui gli interessati possono esercitare i propri diritti e i canali di comunicazione.

Responsabile

È definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

I responsabili vanno selezionati, bisogna contrattualizzare il rapporto e in fine chiuso.

Amministratore del sistema

La normativa italiana prevede che siano identificati degli Amministratori di sistema (AdS), si tratta solo di persone fisiche, si tratta di figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati.

Registro dei trattamenti

Il GDPR richiede di redigere e mantenere un registro delle attività di trattamento. I campi obbligatori del registro sono definiti dall'art 30 del GDPR:

- I dati dell'organizzazione che tiene il registro e se previsti del titolare del rappresentante dell'organizzazione e del DPO.
- Nel caso di responsabili del trattamento, i riferimenti dei titolari del trattamento e, se previsto, del rappresentante del titolare del trattamento.
- La finalità del trattamento o, nel caso dei responsabili, i trattamenti effettuati per conto dei titolari
- Le categorie degli interessati e dei dati personali trattati.
- I destinatari a cui i dati personali sono stati o saranno comunicati.

- I termini di cancellazione delle diverse categorie di dati.
- I trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale, e in casi particolare le garanzie ritenute adeguate per il trasferimento.
- Se possibile, una descrizione delle misure di sicurezza.

Il consenso

Per trattare i dati, bisogna avere il consenso dell'interessato che si può ottenere:

- Per iscritto sui moduli cartacei
- In formato digitale
- Verbalmente

Il GDPR richiede che il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali. Questo è facile da dimostrare, se il consenso è stato ottenuto attraverso moduli cartacei e informatici, risulta invece più complesso nel caso di un consenso ottenuto verbalmente. Quando il consenso è raccolto via modulo informatico, non deve essere marcata in via predefinite l'opzione acconsento al trattamento. In gergo tecnico, l'approccio deve essere di tipo opt-in ossia l'interessato per fornire il proprio consenso deve attivarsi. Un ragionamento simile vale per il consenso sull'uso dei cookie.

I cookie

I cookie Quasi tutti i siti web raccolgono dati degli utenti riferiti alla navigazione nel sito stesso. Questo serve per analizzare le preferenze e le abitudini di navigazione. Possono essere raccolti dati di insieme per valutare le prestazioni del sito e le aree di maggiore interesse o relativi al singolo interessato per successive azioni di marketing diretto, solitamente attraverso pubblicità mirate visibili in altri siti visitati dall'interessato. Per trattare i dati a scopo pubblicitario è necessario il consenso dell'interessato. Molti siti presentano un banner che scompare solo dopo aver fornito o negato il consenso. Oggi molti siti presentano un cookie wall che non permette neanche la navigazione fino a quando l'interessato non ha cliccato su “accetta” o “rifiuta”. Per i cookie il testo di riferimento è la direttiva 2009/136 CE del 25 Novembre 2009 che è stata recepita in Italia con il Decreto Legislativo 69 del 2012. La questione cookie è trattata in modo più completo da:

- Provvedimento del Garante “Individuazione delle modalità semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie” dell’8 Maggio 2014
- “Guidelines 05/2020 on consent under Regulation 2016/679” dell’EDPB del 4 Maggio 2020.

Backup

Il GDPR si esprime anche a riguardo del backup, definendolo come una copia dei dati che andrebbe conservata in luoghi distanti da dove sono conservati i dati originali. Pertanto afferma che il backup dei sistemi informatici vanno

conservati in un data center diverso da quello dove si trovano i server e le copie dei documenti cartacei. Va inoltre, stabilita la periodicità dell'operazione di copie e il tempo di conservazione delle copie. L'accesso ai dati dei backup deve essere gestito applicando gli stessi criteri dell'accesso ai dati primari.

Malware

Per quanto riguarda i malware, il GDPR afferma che vanno installati dei sistemi antivirus sui pc, server e server email, che vanno aggiornati periodicamente. La soluzione più corretta dal punto di vista della sicurezza prevede che siano attivati gli aggiornamenti automatici.

2.4.3 Conclusione - Dieci punti riassuntivi

In conclusione il GDPR si può riassumere in 10 punti chiave che sono:

- Trattamento lecito equo e trasparente
- Limitazione di scopo dati e archiviazione
- I diritti degli interessati
- Il consenso
- Violazione dei dati personali
- Privacy by design
- La valutazione dell'impatto sulla protezione dei dati
- Trasferimento dei dati

- Il responsabile della protezione dei dati
- Consapevolezza e formazione

Capitolo 3

Stato dell'Arte

3.1 Conoscenza e disinformazione sul tema della privacy nelle varie fasce di età

3.1.1 Minori e privacy

Il garante privacy ha messo a disposizione degli utenti un vademecum sui rischi ai quali sono soggetti le informazioni dei minori che navigano sul web, mettendo in evidenza che un minore che utilizza strumenti connessi alla rete potrebbe rivelare inconsapevolmente agli sconosciuti informazioni su dove abita, sulle sue abitudini o sui percorsi che compie di solito. Potrebbe diffondere dati dal dispositivo che sta utilizzando, o consentire tramite un uso poco responsabile, benché sconosciuto, ai cybercriminali di accedere a dati utilizzati per scopi illeciti. I minori devono essere accompagnati, afferma il garante privacy evidenziando che è buona abitudine non far utilizzare le nuove tecnologie ai bambini da soli, e regolare le impostazioni privacy

dei dispositivi e di eventuali servizi se usati da minori. Risulta importante attivare il “parent control” che permette di monitorare l’uso di un dispositivo elettronico da parte di un minore:

- Impostando blocchi e filtri per determinate funzioni
- Creare una lista di parole che il minore non può cercare e trovare sui motori di ricerca
- Limitare l’uso del dispositivo solo in determinate ore

Il GDPR prevede che i sistemi elettronici siano progettati e configurati per ridurre al minimo la raccolta e il trattamento dei dati personali attraverso la privacy by design e la privacy by default, concetti espressi all’interno della legge stessa. Dopo aver messo in evidenza i rischi che gli utenti possono incontrare non tutelando i propri dati, è stata svolta un’indagine su un campione di persone che sono state suddivise in base alle varie fasce di età per conoscere il loro grado di preparazione sul tema. Le fasce di età sono:

- Pre-adolescenti: ragazzi frequentanti classi come la seconda e la terza media
- Adolescenti: ragazzi frequentanti classi del liceo
- Adulti

3.1.2 Pre-adolescenti e adolescenti

Tramite lo studio di un documento di ricerca svolto all’università di Bergamo dalla ricercatrice Alice Ponzi nel 2012 su un campione di 1402 studenti delle

scuole superiori di Bergamo e provincia e 456 studenti che frequentano classi di seconda e terza media è emerso che:

- 89.7 percento degli studenti possiede un proprio smartphone
- 89.9 percento degli studenti utilizza WhatsApp per comunicare
- 82.3 percento degli studenti usa Facebook dallo smartphone, il rimanente è sempre connesso.
- 55.6 percento degli studenti usa Instagram

Questo studio è stato effettuato su studenti di età compresa tra i 12 e i 18 anni. Le legge sulla privacy sia GDPR che il codice privacy italiano vietano a persone al di sotto di 13 anni di iscriversi a un social network pertanto una fetta degli utenti del campione non dovrebbe possedere un proprio account. Infatti dalla ricerca emerge che:

- 85 percento degli studenti conosce qualcuno che è iscritto ad un social network senza aver compiuto 13 anni.
- 55.6 percento degli studenti conosce qualcuno che è iscritto con un'identità diversa dalla sua.
- 15.2 percento degli studenti è stata rubata l'identità online.

Altro tema presente nel progetto di ricerca è quello del cyberbullismo:

- 80.3 percento degli studenti è a conoscenza dell'esistenza del cyberbullismo
- 39.2 percento degli studenti conosce qualcuno che ne è stato vittima

Sì, con connessione dati (3G/4G)	88.6%
Sì, mi connetto quando c'è il WiFi (non ho la connessione dati)	9.4%
No, ho un cellulare che non si può connettere a Internet	1.5%
No, non ho un cellulare	0.4%

Figura 3.1: Sei in possesso di un cellulare con una connessione a Internet?

- 10.8 percento degli studenti è stato vittima di cyberbullismo

3.1.3 Adolescenti

In questo caso lo studio è stato effettuato utilizzando una ricerca svolta dall'università di Bergamo nel 2015. I dati sono stati raccolti utilizzando come strumento un questionario che è stato sottoposto a studenti delle scuole secondarie di secondo grado di Bergamo e provincia con lo scopo di indagare modi, luogo e tempi dell'uso delle comunicazioni telematiche, in 18 istituti superiori per un totale di 1370 studenti. Il questionario, implementato attraverso i moduli di Google Drive, era composto da 52 domande, più 5 domande di profilazione personale poste in fondo al questionario per far lavorare i rispondenti da subito con domande impegnative e soltanto alla fine con quelle che richiedono meno concentrazione. Il questionario era anonimo. Il questionario è stato compilato da maschi per il 48.4 percento e da femmine per il 51.6 percento. Le domande e le tematiche presenti all'interno del questionario riguardano argomenti come il possesso di cellulari e l'uso, in relazione ai servizi di comunicazione utilizzati dai rispondenti per comunicare con genitori e o amici, inoltre sono presenti anche domande sul bullismo e sul cyberbullismo. Alcuni dei dati che sono stati ricavati dal questionario sono:

All'interno del questionario viene anche richiesto agli studenti di rispon-

	Parlando al telefono	Con SMS	Con servizi di messaggistica come WhatsApp	Con social networks	Con e-mail
Mai	1.7%	11.3%	23.6%	79.5%	82.9%
Raramente	18.5%	21.9%	11.4%	12.7%	11.4%
Più volte al mese	12.3%	15.4%	9.0%	1.9%	3.1%
Più volte alla settimana	28.1%	23.7%	20.4%	2.7%	1.6%
Tutti i giorni (o quasi)	26.1%	18.2%	18.8%	1.7%	0.8%
Più volte al giorno	13.3%	9.4%	16.8%	1.4%	0.2%

Figura 3.2: Frequenza d'uso dichiarata di servizi di comunicazione tra rispondenti e genitori

	Parlando al telefono	Con SMS	Con servizi di messaggistica come WhatsApp	Con social networks	Con e-mail
Mai	3.3%	8.1%	2.4%	24.1%	70.8%
Raramente	18.1%	19.1%	0.8%	17.7%	20.9%
Più volte al mese	17.2%	11.2%	0.4%	10.5%	3.7%
Più volte alla settimana	27.8%	17.5%	2.9%	15.6%	2.9%
Tutti i giorni (o quasi)	18.5%	16.6%	13.9%	12.3%	0.8%
Più volte al giorno	15.1%	27.5%	79.7%	19.8%	0.8%

Figura 3.3: Frequenza d'uso dichiarata di servizi di comunicazione tra rispondenti e amici

	Ask.fm	Facebook	Facebook Messenger	Instagram	Snapchat	Twitter	WhatsApp
Mai	63.7%	18.6%	28.7%	29.9%	77.9%	78.6%	2.5%
Ogni tanto	15.0%	15.7%	28.2%	8.9%	7.9%	12.2%	1.3%
Spesso	6.4%	16.3%	20.7%	14.0%	5.2%	5.1%	3.2%
Tutti i giorni	9.0%	49.3%	22.4%	47.2%	9.0%	4.1%	93.0%

Figura 3.4: Frequenza d'uso per alcuni servizi telematici

Su tutto il campione	Prendere accordi per incontrare persone conosciute in Internet	Inviare fotografie a persone conosciute in Internet	Pubblicare/spedire immagini intime	Vedere fotografie/video intime
Mai	68.9%	57.7%	83.6%	68.7%
Ogni tanto	21.2%	20.1%	10.7%	19.3%
Spesso	6.4%	14.3%	3.4%	7.9%
Tutti i giorni	3.5%	8.0%	2.3%	4.0%

Figura 3.5: Con quale frequenza ti capita di...

	Per niente	Poco	Abbastanza	Molto
TOTALE	3.9%	16.2%	62.1%	17.7%
Femmine	3.8%	16.5%	64.4%	15.3%
Maschi	4.1%	15.8%	59.7%	20.4%
I	7.4%	19.4%	59.4%	13.8%
II	3.8%	15.3%	58.7%	22.2%
III	5.3%	17.3%	59.9%	17.6%
IV	1.2%	13.1%	71.4%	14.3%
V	0.5%	14.9%	63.1%	21.6%

Figura 3.6: Competenza degli studenti
Competenza degli studenti in merito all'uso dei social
e la divulgazione di dati personali

dere a domande in merito a quelle che pensano essere le proprie competenze. Da queste domande e relative risposte è emerso che i ragazzi manifestano indubbie abilità di uso della rete, non però supportate da adeguata conoscenza degli strumenti, dei contesti, dei linguaggi, dei protocolli di comunicazione, pertanto non si può affermare una vera competenza e consapevolezza dei mezzi, sia per quanto riguarda lo sfruttare le opportunità che i mezzi offrono sia per i rischi connessi al loro utilizzo. Come possiamo notare le risposte 'si' e 'no' sono bilanciate. Tramite una combinazione lineare delle risposte sono stati individuati 3 gruppi:

- Competenti: 137 studenti
- Incompetenti: 479
- Una posizione intermedia

I due gruppi estremi sono stati usati per indagare il legame tra competenza percepita ed esposizione ai rischi della rete, andando a incrociare i dati con quelli relativi ai comportamenti a rischio. L'analisi statistica così incrociata

ha mostrato che gli utenti che si sentono competenti sono quelli più esposti ai rischi. Infatti sono anche quelli che più frequentemente inviano fotografie a persone conosciute in internet, pubblicano o spediscono immagini intime, inoltrano video senza autorizzazione. Per testare le competenze tecnologiche si è deciso di inserire due domande riferite alla dimestichezza con il PC e alla familiarità con la sintassi degli indirizzi URL. Anche queste mostrano la discrepanza tra conoscenza e percezione delle proprie competenze. Sono stati individuati 4 profili:

- Lo studente competente
- Lo studente incompetente
- Lo pseudo-competente
- Lo pseudo-incompetente

Questi 4 profili mostrano che la competenza percepita diversa da quella reale conduce a maggiore esposizione ai rischi.

3.1.4 Adulti

Per quanto riguarda il rapporto tra gli adulti e la rete è stata consultata la Rivista italiana di Educazione familiare all'interno della quale la figura degli adulti viene intesa anche come genitori. I dati di tale ricerca suggeriscono che, i media digitali sono incorporati nella routine quotidiana della maggior parte delle persone. Il lavoro presentato all'interno della rivista si basa su un'intervista effettuata su 302 genitori italiani tramite un survey online, su

temi inerenti la genitorialità e le nuove tecnologie. Le attività svolte in rete, vengono suddivise in:

- Attività di comunicazione
- Attività culturali o ludiche
- Attività legate al commercio elettronico e ai servizi bancari online.

Il sondaggio online è stato somministrato via Google Drive a cui ha preso parte un campione di 302 genitori. Il questionario è formato da 36 domande escluse quelle anagrafiche prevalentemente a risposta chiusa con alcune domande a risposta aperta. Il campione era costituito da:

- Madri per l'85
- Soggetti che vivono in coppia 86
- Soggetti lavorativamente attivi 89
- Soggetti con laurea 70
- Soggetti con diploma di scuola superiore 27,5
- 48 per cento tra i 41 e 50 anni
- 38,7 per cento tra i 30 e il 40 anni
- 12,3 per cento tra i 51 e 60 anni
- Nord Italia 67,6 per cento
- Centro 23 per cento

- Sud 8,7 percento

Per quanto riguarda l'adozione dei dispositivi per navigare in rete, i dati ISTAT dimostrano che fino ai 34 anni la propensione degli utenti è quella di combinare pc e cellulare. Dopo i 34 anni, è stato notato che la scelta dell'uso del device dipende dal genere: gli uomini prediligono l'uso di dispositivi multipli ma principalmente l'uso esclusivo del pc. Le donne prediligono l'uso esclusivo del cellulare. L'uso di instant messaging rimane elevato anche nelle classi di età successive fino a 65 anni. Anche i social network risultano via via meno diffusi a partire da 45 anni. Per quanto riguarda l'uso delle piattaforme, la più utilizzata è Facebook che viene prevalentemente usata come mezzo per aggiornarsi sulle notizie di attualità, commentare status, foto, notizie interagire con i propri contatti e pubblicare materiale. Per quanto riguarda l'instant messaging quella più usata è WhatsApp per il 95 percento seguita da FacebookMessenger nel 65La maggior parte dei rispondenti riporta di utilizzare la rete giornalmente per svolgere le seguenti attività:

- Fare ricerche 85 percento
- Collegarsi a Facebook o altri tipi di social 74 percento
- Chattare usando WhatsApp 97 percento

Importante nella situazione genitoriale il tema della condivisione di materiale fotografico sui propri figli dal quale è emerso che:

- Il 55 percento pubblica almeno una volta una foto di un figlio sui social media

- Solo il 12 per cento consulta i figli prima della pubblicazione, le differenze notate su questo dato riguardano il grado di preparazione e i titoli di studio dei genitori. I genitori con un titolo di studio più elevato, tendono a pubblicare meno foto dei figli.

Da queste informazioni è possibile notare che l'impreparazione sul tema della privacy in rete è presente in tutte le fasce di età sopra analizzate. Pertanto non è possibile definire una specifica fascia d'età in quanto la possibilità di subire un attacco legato alla privacy oppure di non essere a conoscenza di come i nostri dati viaggiano all'interno del web, può accadere a qualsiasi soggetto indipendentemente dalla sua età anagrafica. Pertanto, il range di età a cui si rivolge la nostra applicazione è molto vasto.

3.2 Il caso Instagram e la violazione degli account

Instagram è uno dei social più utilizzati attualmente per la condivisione di foto e video che hanno cambiato il mondo della comunicazione.

Si tratta di un servizio di rete sociale statunitense che permette agli utenti principalmente di scattare foto e pubblicarle via internet. La prima versione è stata lanciata nel 2010 ed era disponibile solamente su iOS, nel 2012 è stata resa disponibile anche per Android. Instagram ha ottenuto subito un grande popolarità. Dopo il suo lancio nel 2010 ha guadagnato 1 milione di utenti registrati in soli due mesi, 10 milioni in un anno e 1 miliardo di utenti nel 2019. Instagram ha creato un nuovo modo di comunicare, non solo tramite le foto ma anche tramite gli hashtag, parole chiavi che sono state introdotte per aiutare gli utenti a scoprire le foto degli altri sulla piattaforma. Ad

oggi gli hashtag sono utilizzati per creare “tendenza”. Nel 2013 Instagram ha lanciato i direct, una funzionalità che consente agli utenti di interagire fra di loro tramite l’invio di messaggi. Nel 2016 sono state introdotte le storie che consentono agli utenti di scattare foto visibili solo per 24 ore. Questo tipo di funzionalità era alla base di Snapchat infatti all’inizio questa innovazione ricevette molte critiche. La popolarità di Instagram ha portato alla creazione di una varietà di servizi di terze parti progettati per integrarsi con esso, compresi i servizi per la creazione di contenuti da pubblicare sul servizio e la generazione di contenuti da foto di Instagram. Negli ultimi mesi, gli utenti iscritti sulla piattaforma hanno subito dei furti di identità. Esistono due tecniche per ottenere gli account degli utenti. La prima si avvia con la ricezione di un messaggio in direct da un mittente sconosciuto o un semplice conoscente con la richiesta di aiuto per un problema sul proprio account affermando che lo stesso instagram ha suggerito il nostro account per risolvere il problema. In direct l’adescatore invia delle indicazioni da seguire fino a portare la vittima al cambio della email legato al proprio account, a quel punto l’account passa nella mani dell’adescatore. L’altra tecnica è quella della ricezione di un messaggio in direct da un conoscente che chiede qualcosa in cambio tramite un link, ad esempio votare una foto per un contest, cliccando tale link l’utente vittima può visualizzare un form che chiede di effettuare l’accesso dall’esterno, così facendo il cyber crime ottiene le credenziali di accesso e se ne impossessa. Oppure nei casi più recenti nel momento stesso in cui l’utente vittima clicca sul link, il controllo del suo account passa automaticamente all’cybercrime, e l’utente non è più in grado di accedervi. L’assistenza fornita da Instagram aiuta i suoi utenti

che sono stati “derubati” a riottenere il proprio account. Fornendo due metodi per recuperare l’account: Nel primo caso, nel tentativo di accedere al proprio account nel momento in cui questo è stato già ottenuto e le credenziali sono state cambiate, Instagram propone all’utente la possibilità di accedere attraverso l’utilizzo di una ulteriore applicazione come Google Authenticator, Authy, 1Password; oppure tramite codice di backup forniti da Instagram nel momento in cui si crea l’account. Risulta utile e responsabile conservare questi codici, ma in caso l’utente non ne è più impossesso si possono recuperare effettuando una richiesta a Instagram stesso che richiede all’utente di inviare una foto contenente il proprio volto e un foglio con scritto l’username e il nome dell’utente, dopo questa verifica Instagram invia il codice di backup che permette all’utente di accedere nuovamente al proprio account e cambiare le credenziali. Nel secondo caso, dopo vari tentativi ad accedere al proprio profilo, Instagram va in aiuto dell’utente chiedendo se avesse perso il possesso dell’account. In questa procedura standard offerta da Instagram, l’applicazione pone all’utente una serie di domande e alla fine chiede di inviare un video tramite l’applicazione mostrando il volto da varie angolazioni per controllare che il volto nel video sia effettivamente quello delle foto presenti all’interno del profilo che si vuole recuperare ed entro 48 ore l’utente riceverà una risposta, contenente un link per recuperare il profilo.

3.3 Sistemi esistenti che tutelano la privacy e sistemi che insegnano la privacy

All'interno degli store dei nostri smartphone o navigando in rete è possibile conoscere e scaricare molte applicazioni o sistemi dedicati alla privacy. Durante il corso della tesi, sono stati raccolti i maggiori sistemi o applicazioni inerenti alla privacy che sono stati suddivisi in due categorie, distinguendo:

- Sistemi che proteggono i dati personali sul web
- Sistemi che insegnano come proteggere e tenere sicuri i nostri dati personali

3.3.1 Sistemi che proteggono i dati

Tra i sistemi che proteggono i dati troviamo molte applicazioni VPN, siti web ma soprattutto browser che proteggono i dati degli utenti che li utilizzando, bloccando tracker di terze parti, in modo da non manipolare i dati per vari scopi, come le pubblicità mirate.

- Disconnect.me Sistema parzialmente open source che serve per bloccare i tracker di terze parti. È stata rilasciata sia come estensione del browser che app mobile. Presenta 3 tipi diversi di servizi: adblocker, firewall, VPN. Utilizza la crittografia e VPN per rendere le informazioni sicure. È stata creata da due ex collaboratori di Google pertanto il suo ingresso nel mercato non è stato inizialmente molto semplice.
- Jumbo Jumbo è stata lanciata ad Aprile 2019 solo per IOS ma gli sviluppatori hanno assicurato che sarà presto disponibile una versione

anche per Android. È pensata come assistente personale che deve gestire le esigenze di data protection dell'utente, compresa la rimozione di contenuti obsoleti da varie piattaforme. Presente 4 principali servizi di protezione: sicurezza, gestione delle impronte digitali, monitoraggio e personalizzazione delle profilazioni, monitoraggio dei tag e della visibilità dei contenuti. Prevede tre profili di diverso rigore: basso, medio e alto a cui corrispondono diversi settaggi predefiniti delle impostazioni presenti nei social coinvolti. È un app piuttosto pesante e limitante per il sistema su cui viene installata dalla battery drain, il consumo di memoria interna e l'utilizzo della rete.

- Bouncer Si tratta di un gestore dei permessi richiesti dalle applicazioni installate sui dispositivi. Il permesso viene rilasciato solo in caso di necessità, infatti di default i permessi sono tutti negati, l'utente può però personalizzare queste impostazioni. L'app Bouncer è a pagamento
- Tor Browser TOR acronimo di THE ONION ROUTER ha come icona una cipolla che rappresenta l'incapsulamento dei dati in vari livelli di crittografia. Si basa su Mozilla Firefox. La sua capacità è quella di assicurare l'anonimato della navigazione web. Meno chiara è la funzione che svolge quando si protegge l'anonimato di chi gestisce uno specifico sito e la sua vicinanza al Dark Web. Tor è disponibile su Google Play.
- IoT Assistant È l'app più recente nell'ambito della tutela della privacy, il suo intento è quello di informare gli utenti su quali tecnologie IoT sono intorno a noi e le informazioni che raccolgono. È concepita come una soluzione soprattutto per gli stessi proprietari dei dispositivi IoT.

- Duck Duck Go Si tratta di un motore di ricerca dedicato principalmente alla protezione dei dati e la privacy degli utenti. Non archivia i dati e le informazioni degli utenti, permette le navigazioni private, non tenendo traccia degli indirizzi IP anche se li rileva. La sicurezza offerta è di alto livello anche grazie all'uso della crittografia. Purtroppo sono ancora pochi i risultati ottenuti nel momento di una ricerca, ma risultano molto precisi.
- Vivaldi Si tratta di un browser web freeware multiplatforma, risulta veloce privato e sicuro. Vivaldi non monitora il comportamento degli utenti e blocca i tracker di terze parti. Pertanto, le informazioni private degli utenti restano sempre al sicuro. Non sono presenti estensioni in quanto quest'ultime rallentano il browser stesso e mettono a rischio i dati degli utenti. Vivaldi usa una serie di strumenti opzionali: bonus che non occupano risorse e non “rubano” dati.
- Brave Browser open-source multiplatforma specializzato nella protezione della privacy, basato sul progetto Chromium. Blocca i tracker di terze parti e gli annunci fastidiosi su tutti i siti web che un utente visita. L'assenza di annunci e tracker fastidiosi porta un caricamento più veloce delle pagine web e una maggiore durata della batteria del dispositivo e persino un risparmio di dati.
- Qwant Motore di ricerca europeo lanciato nel 2013, viene definito come “il motore di ricerca che non sa niente di te” infatti non c'è tracciamento delle ricerche, nessun archivio di dati personali e pubblicità mirate.

Presenta delle pubblicità che servono per finanziare la piattaforma che sono uguali per tutti gli utenti e non sono influenzate dalle ricerche.

Inoltre, esistono un sacco di programmi VPN acronimo di Virtual Private Network ossia “rete privata virtuale”, quindi delle app che offrono un servizio per proteggere la connessione internet e la privacy online.

3.3.2 Sistemi che insegnano la privacy

Per quanto riguarda i sistemi dediti all’insegnamento della privacy purtroppo ad oggi risultano solo cinque, riportati di seguito:

- Space Shelter: creato da Google nel 2021 si tratta di un gioco il cui compito principale è quello di insegnare agli utenti a rendere più sicuri i propri dati online. Il gioco è ambientato in una navicella, Il soggetto è un avatar che è un’astronauta e si può scegliere fra 4 avatar. Il gioco inizia con un piccolo quiz, per capire le conoscenze dell’utente che sta iniziando il gioco. Superato il test ci viene chiesta di inserire una password partendo da una parola semplice di almeno 8 caratteri e aggiungendo, caratteri maiuscoli, numeri e simboli alfanumerici all’interno della parola stessa, lo scopo quindi è quello di insegnare a creare delle password forti e sicure e presentando agli utenti l’utilizzo del gestore delle password e l’importanza dell’autenticazione a due fattori. Una volta fatto questo la navicella è pronta a muoversi nello spazio ed evitare gli attacchi muovendosi con le frecce, se non riusciamo a schivarli allora dobbiamo rispondere a delle domande. Superati gli attacchi, c’è un ultimo test complessivo da rispondere e poi il gioco termina.

- Quanto ne sai di privacy?: Questo serious game creato dall'associazione dei consumatori francese UFC-Que Choisir è stato utilizzato da CIE per diffondere la conoscenza della Legge GDPR. Il gioco, disponibile gratuitamente, inizia con l'annuncio del matrimonio di due amici. Starà al giocatore organizzare l'evento a tempo di record, affrontando una serie di sfide che ruotano intorno alla privacy, come tutelarla e come non infrangerla. Organizzare la luna di miele a sorpresa senza far sapere nulla alla futura moglie, cercare di nascosto su pc o tramite i suoi amici foto di lei da proiettare al matrimonio, "ripulire" il proprio profilo social per evitare crisi prematrimoniali o il ritorno improvviso di una ex. Attraverso queste situazioni particolari e divertenti, il Serious Game punta a far comprendere al giocatore l'importanza della privacy e del rispetto dei dati personali.
- Datak-II privacy game: è un serious game che nasce per sensibilizzare le persone sul tema della privacy e della protezione dei propri dati, infatti può essere definito anche come privacy game. Si tratta di un'esperienza didattica gratuita che viene erogata in modo divertente. Il ruolo ricoperto dall'utente che gioca è l'assistente del sindaco, responsabile della protezione dei dati della città di Data Ville. La meccanica di gioco è molto semplice e si limita a qualche click su elementi della scena o rispondendo a delle domande. In base alle risposte il gioco procede in maniera diversa.
- Interland: Si tratta di un gioco interattivo lanciato da Google nel 2020 che fa parte del progetto "Vivi internet, al meglio". Tale gioco

si rivolge a bambini dai 6 ai 13 anni con lo scopo di insegnare delle lezioni fondamentali relative alla sicurezza sul web. Il gioco comprende 4 esperienze di gioco: insegnare a custodire le proprie informazioni in rete, valorizzare le positive vibes sul web e la loro importanza, prestare attenzione a cosa si condivide sul web e infine il phishing.

- Cyber Chronix : Un gioco mobile del Centro Comune di Ricerca della commissione europea che si concentra sul regolamento europeo sulla protezione dei dati ingenerale. I giocatori vengono portati su un pianeta futuristico a diversi anni luce dalla terra. L'obiettivo è quello di aiutare il proprio personaggio a partecipare ad una festa, superando diversi ostacoli legati alla protezione dei dati. Il gioco è rivolto a un pubblico giovanile ma i contenuti e l'esperienza di gioco possono risultare interessanti e divertenti anche per gli adulti. Il gioco è disponibile in inglese, francese e italiano. Attualmente è disponibile solo la versione per Android.

Capitolo 4

Progettazione del sistema

4.1 Ideazione del sistema

La soluzione proposta è un sistema “privacy for you” che ha come scopo quello di insegnare agli utenti l’importanza della privacy e di tutelare i proprio dati online e come proteggerli in una maniera divertente e allo stesso tempo accattivante in modo da non risultare noiosa e far appassionare l’utente che utilizza il sistema. Il sistema prevede 3 sezioni principali, tutte dedita all’insegnamento della privacy: una sezione test, una sezione giochi e una di studio. La prima funzionalità del sistema proposta all’utente è quella di “test principale”, funzionalità che permette all’utente di svolgere un quiz generico che contiene varie domande sul tema privacy una volta effettuato il test principale, l’amministratore visualizzerà il punteggio svolto dall’utente e l’utente potrà accedere alle altre sezioni del sistema. All’interno della sezione test l’utente potrà esercitarsi sugli argomenti riguardati la privacy come ad esempio “malware”, “phishing”, “attacchi legati alle password” ecc..

All'interno della sezione "studio" l'utente potrà apprendere le informazioni necessarie sulla privacy e su come tutelare i propri dati evitando i rischi, erogate attraverso testi descrittivi, immagini o video interattivi. All'interno della sezione "giochi", l'utente potrà apprendere divertendosi. Il sistema prevede che l'utente sia registrato sulla piattaforma, una volta effettuata la registrazione e il relativo login ogni volta che sarà richiesto l'utente potrà usufruire del sistema stesso. Inoltre, è presente una sezione "profilo" dedicata all'utente all'interno della quale lui può visualizzare il suo profilo, modificare la propria password se lo desidera oppure eliminare il proprio profilo dalla piattaforma. Il sistema viene gestito da un amministratore che si occupa di gestire gli utenti, per i quali può controllare tutti gli utenti presenti sulla piattaforma con i relativi dati e il relativo punteggio. Pertanto, il sistema può essere utile all'interno delle scuole per conoscere il grado di preparazione sul tema della privacy degli studenti. Inoltre, l'amministratore potrebbe decidere di eliminare un utente all'interno del sistema se il suo comportamento non risulta adeguato alle regole del sistema stesso. Per la sezione test, l'amministratore ha il compito di visualizzare i test presenti sulla piattaforma e aggiungere eliminare o modificare una o più domande relative ad un test. Può inoltre decidere di modificare l'intero test o eliminarlo. Per la sezione studio, l'amministratore può prendere decisioni in merito alla visualizzazione dei casi di studio, pubblicazione di un nuovo argomento di studio, modifica ed eliminazione di uno o più argomenti di studio. Per la sezione giochi, l'amministratore può prendere decisioni in merito alla visualizzazione dei giochi presenti sulla piattaforma, pubblicazione di un nuovo gioco, modifica ed eliminazione di uno o più giochi. Il sistema è stato

progettato interamente, per ogni sezione sono stati definiti scenari, casi d'uso sequence diagram, diagramma della classi, activity diagram e statechart diagram. Sono state definite due sezioni una per gestire la registrazione e una per l'accesso e in più le sezioni legate alle funzionalità del sistema: test, giochi, studio, una gestione per l'utente e una per l'amministratore. Il sistema risulta implementato e funzionante per quanto riguarda la gestione dell'utente, dell'amministratore e la funzionalità di test principale.

4.2 Progettazione

Il sistema è stato progettato interamente, prevedendo varie gestioni per registrazione, accesso, account, utenti, test, giochi, studio e amministratore.

Gestione utente

L'utente è il protagonista del sistema per usufruire della piattaforma deve registrarsi compilando un form all'interno del quale sono richieste informazioni quali: email, password, nome, cognome e data di nascita. Queste informazioni permettono all'utente di essere descritto e riconosciuto dall'amministratore all'interno della piattaforma. Le informazioni di email e password sono richieste quando l'utente, una volta registrato, deve effettuare il login. L'utente sulla piattaforma può effettuare il test principale, visualizzare il suo profilo, modificare le informazioni riguardanti o decidere di eliminarlo

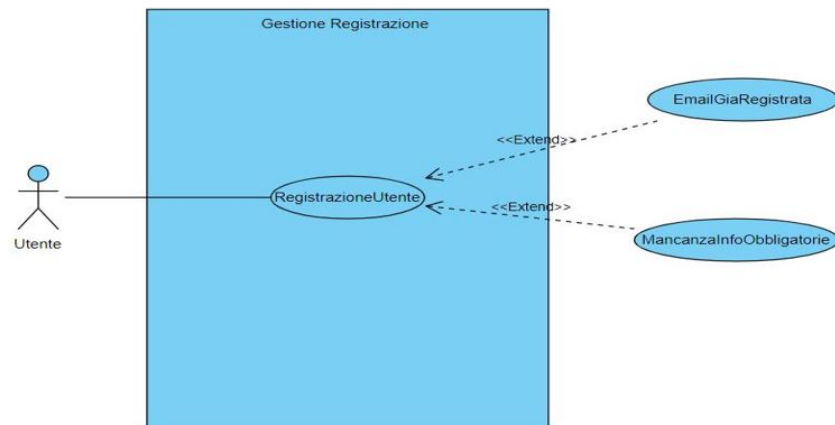


Figura 4.1: Use case gestione registrazione

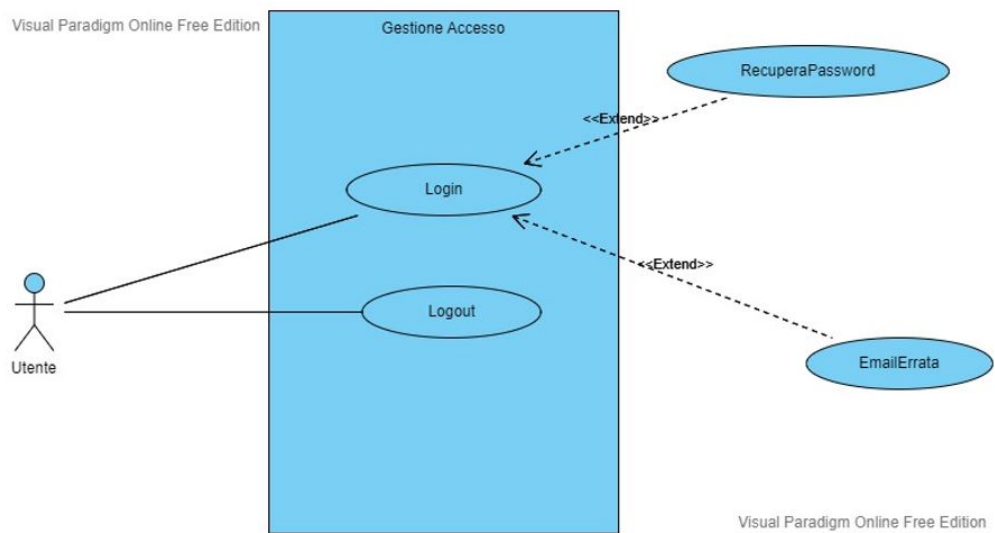


Figura 4.2: Use case gestione accesso

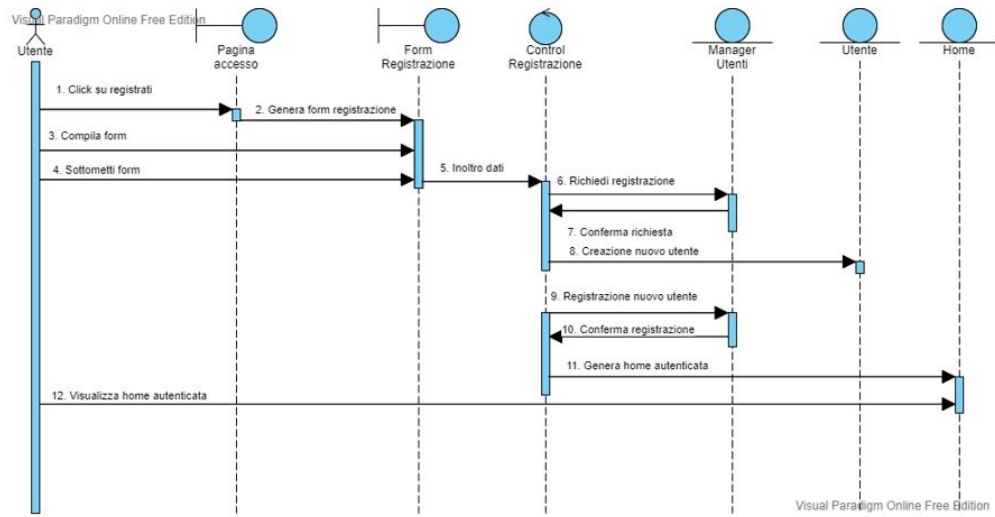


Figura 4.3: Sequence gestione registrazione

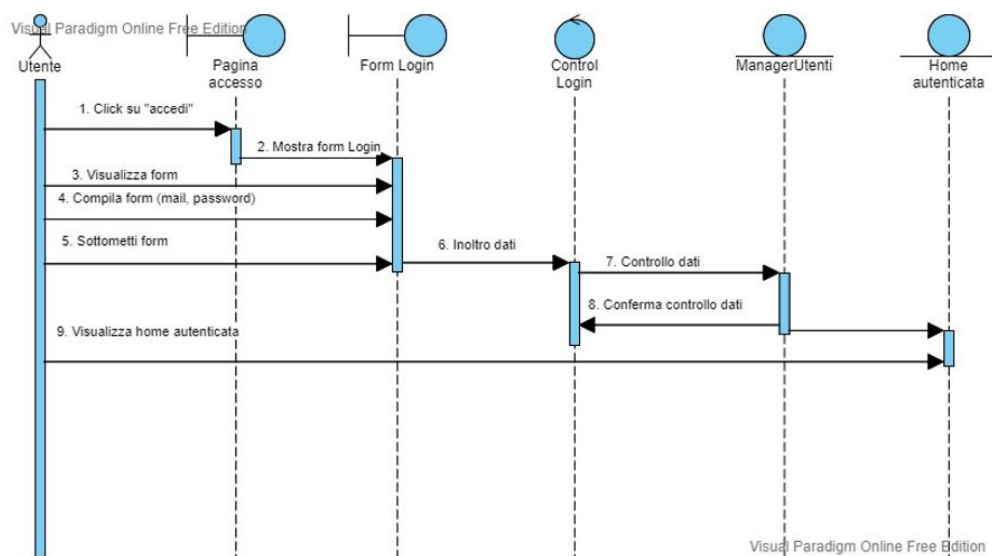


Figura 4.4: Sequence login

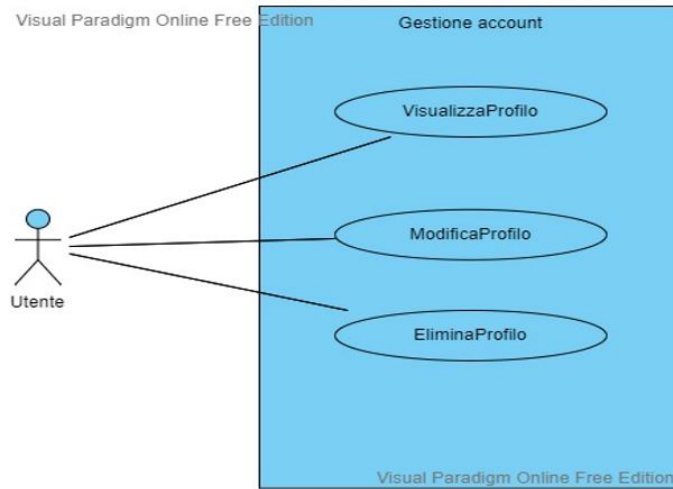


Figura 4.5: Use case gestione account

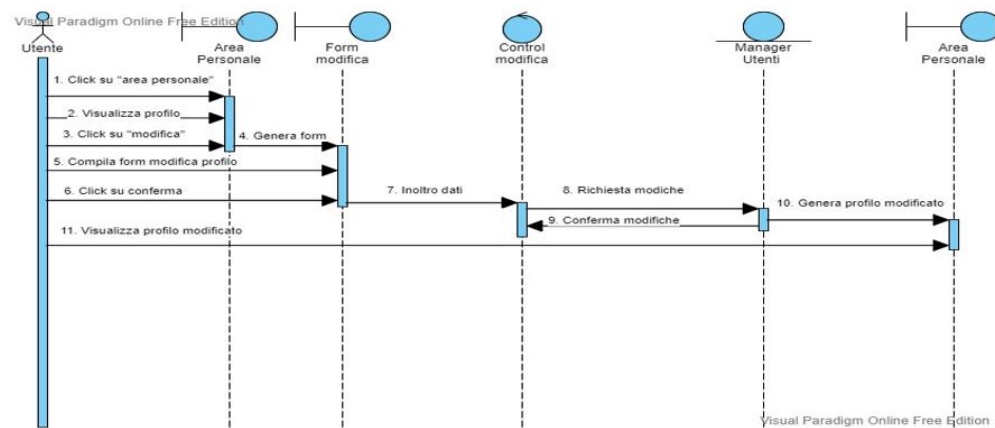


Figura 4.6: Sequence diagram utente modifica profilo

Gestione test

La sezione test è la sezione nella quale l'utente può effettuare un test principale formato da varie domande tutte inerenti alla privacy. Per effettuare il test, l'utente deve essere registrato ed aver effettuato il login. Dopo aver risposto alle domande del questionario, verrà calcolato il punteggio ottenuto e da quello il livello di preparazione dell'utente, che sarà visibile dall'amministratore all'interno della sezione utenti e nella sezione profilo dell'utente. Inoltre sono stati progettati dei test di allenamento, dei quiz formati da domande che si riferiscono tutte ad uno stesso argomento, una volta effettuato il test, l'utente riceverà un punteggio che determina la sua preparazione sull'argomento di riferimento.

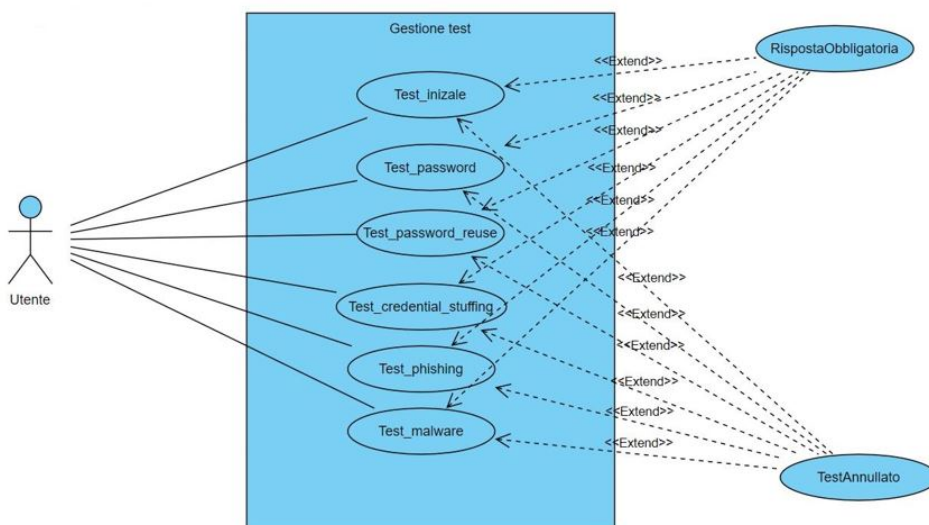


Figura 4.7: Use case gestione test

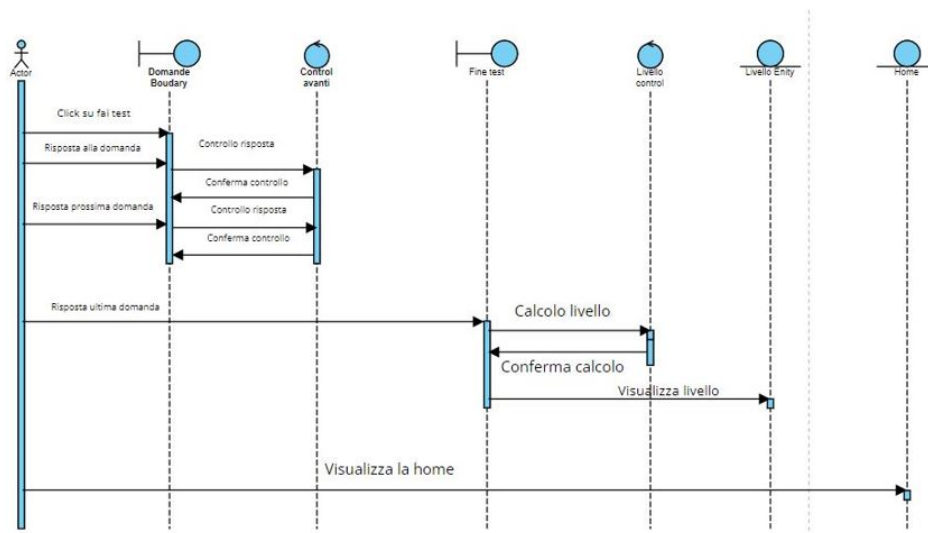


Figura 4.8: Sequence diagram test principale

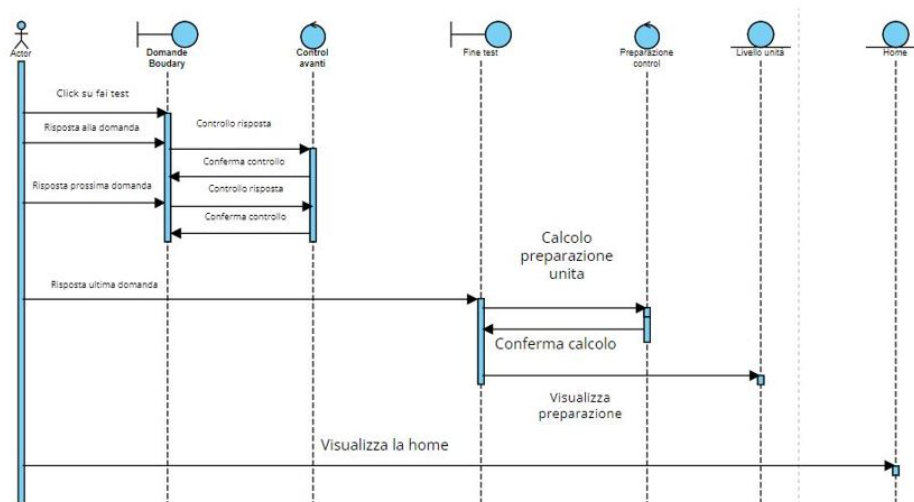


Figura 4.9: Sequence diagram test principale

Gestione giochi

All'interno della sezione giochi è possibile apprendere e conoscere importanti argomenti sulla privacy tramite dei serious game. Tale sezione è stata progettata considerando un gioco per ogni singolo attacco o altro argomento legato alla privacy.

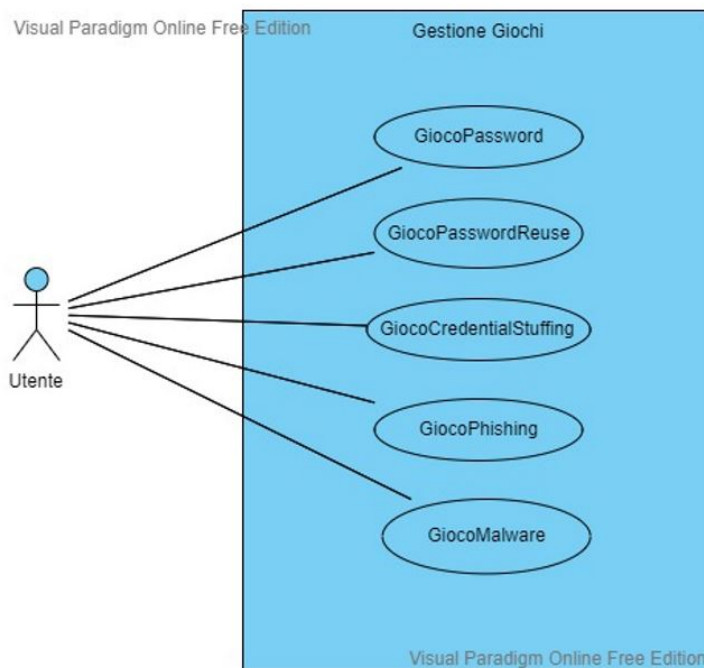


Figura 4.10: Use case gestione giochi

Gestione studio

Per la sezione studio è stato pensato uno studio per ogni tipo di attacco, un argomento di studio è descritto all'interno della piattaforma tramite id dello studio, titolo e una descrizione. Successivamente, verranno implementati uno

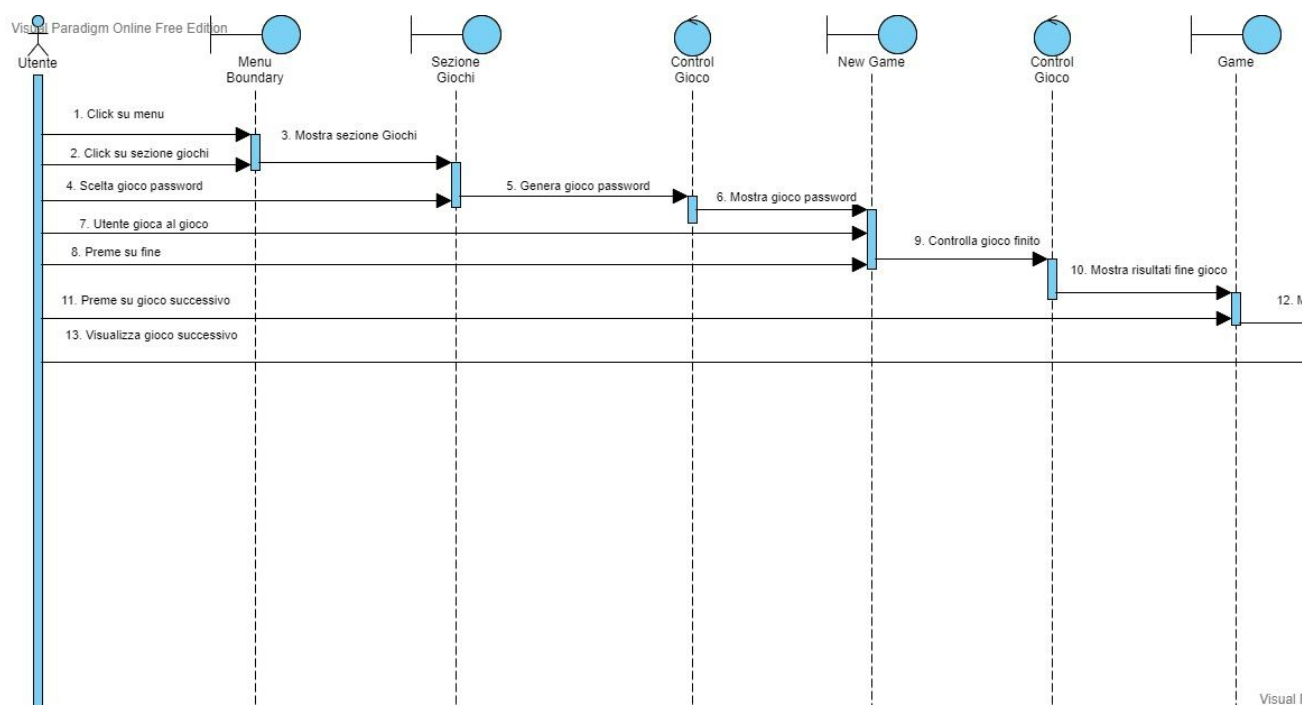


Figura 4.11: Sequence diagram per gioco password

o più casi di studio, per apprendere informazioni sulla privacy attraverso video, immagini o lezioni descrittive.

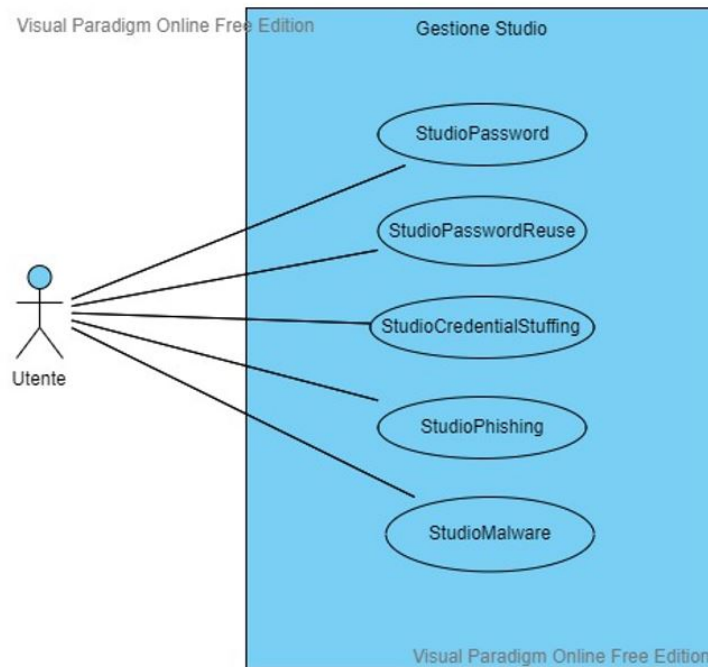


Figura 4.12: Caso d'uso gestione studio

Gestione amministratore

L'amministratore è la figura che si occupa di gestire l'intero sistema. Infatti si occupa di coordinare gli utenti, i test, gli studi e i giochi. Permettendo per ognuno di questi oggetti operazioni come: inserimento o pubblicazione, modifica ed eliminazione.

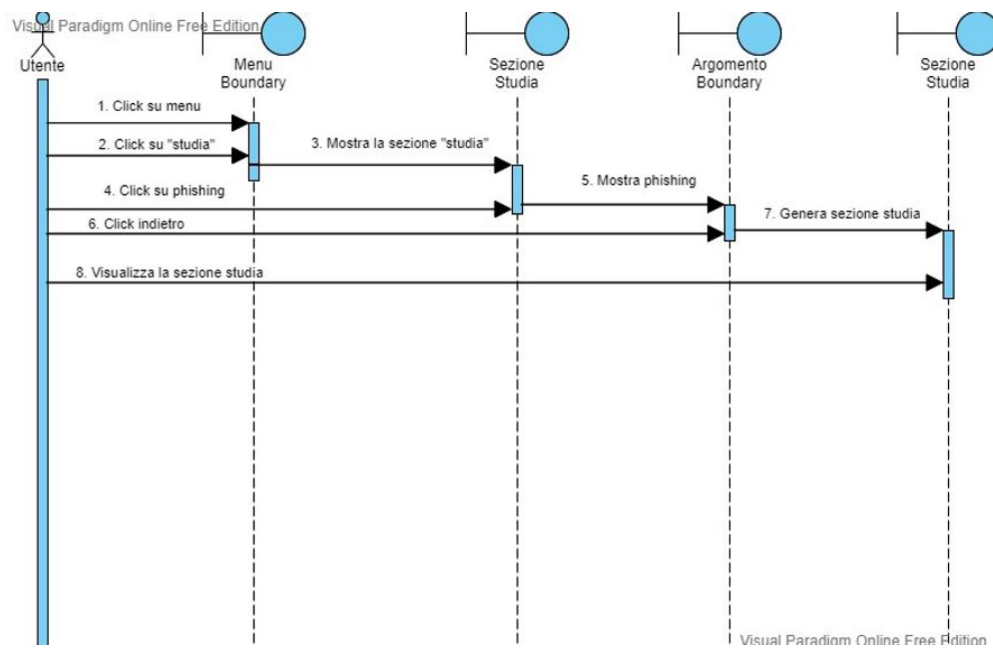


Figura 4.13: Sequence diagram per un caso di studio

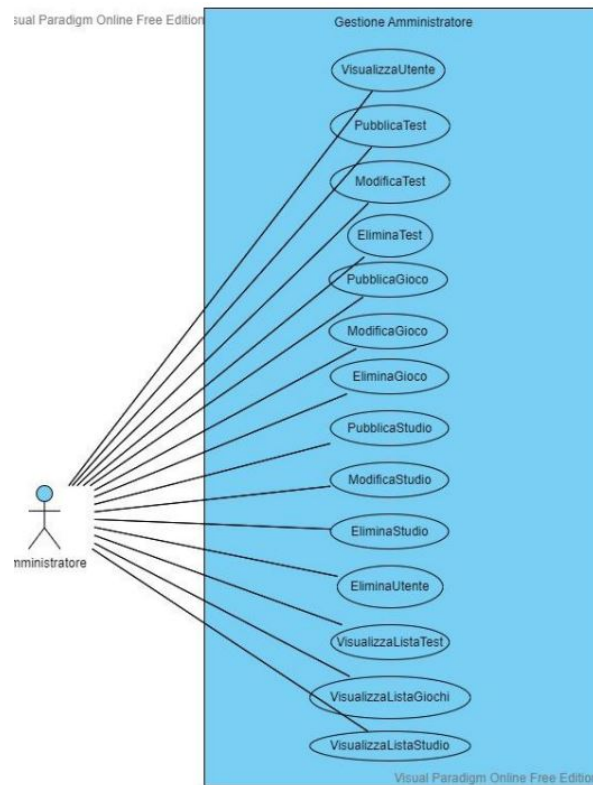


Figura 4.14: Use case gestione amministratore

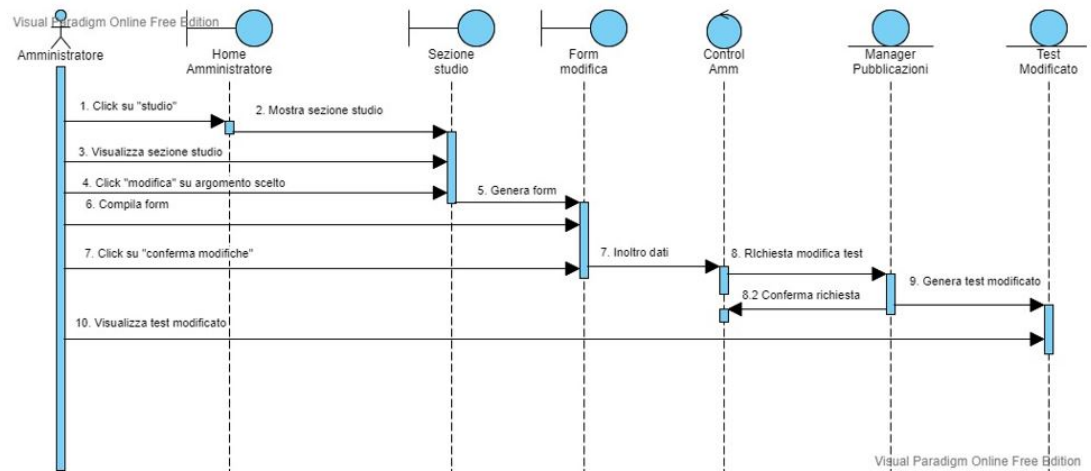


Figura 4.15: Sequence diagram amministratore modifica argomento di studio

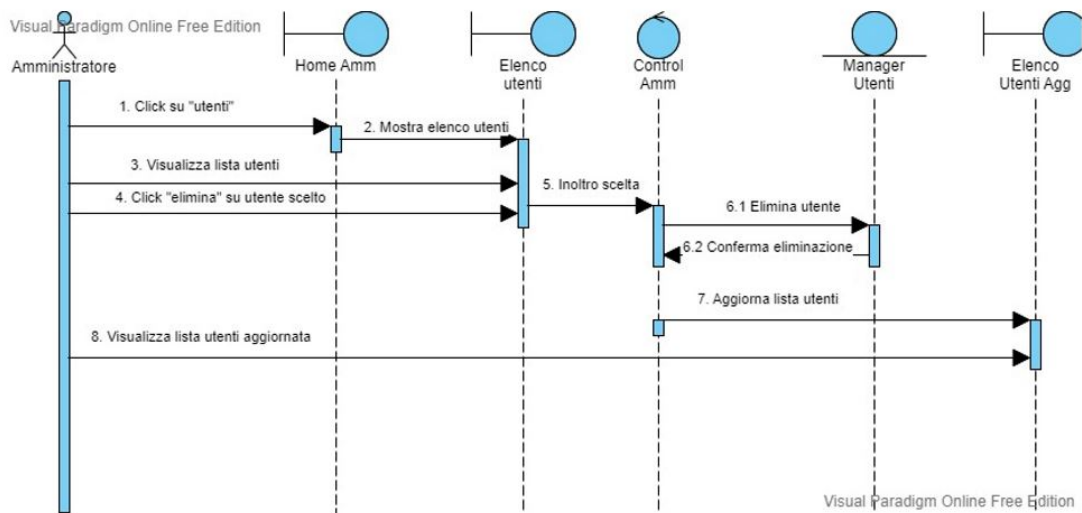


Figura 4.16: Sequence diagram amministratore elimina utente

Capitolo 5

Il sistema "privacy for you"

5.1 Spring

Spring è un framework open source nato come alternativa alla complessità nello sviluppo di applicazioni enterprise. La prima versione è stata rilasciata da Rod Johnson nel 2000. Nel 2004 la prima versione di Spring venne distribuita grazie al lavoro di un piccolo gruppo di sviluppatori che nell'anno precedente avevano pubblicato il progetto Sourceforge. Nel 2013 la società che aveva sviluppato Spring, cioè la SpringSource venne acquisita da Pivotal. Successivamente nel 2019 Pivotal è stata acquisita da Vmware. Spring è diventato così popolare perché ha permesso la diffusione di tecniche come:

- L'inversion of control : è un principio di progettazione mediante il quale il controllo degli oggetti o porzione di codice viene trasferito al container o al framework.
- La programmazione orientata agli aspetti – AOP

Queste due tecniche erano presenti già in Java EE, infatti possiamo affermare che Spring è complementare a Java EE, anche se Spring non utilizza le specifiche di Java EE ma si integra con alcune di esse come le Servlet API, WebSocket API, JSON Binding API, Bean Validation, JPA e JMS. Spring supporta anche altre due specifiche che lo sviluppatore può utilizzare al posto dei meccanismi forniti da Spring che sono:

- La dependency Injection: è un design pattern utilizzato per implementare l'IoC, che consente la creazione e l'associazione degli oggetti fuori dalla classe che li utilizza.
- Common Annotations

Le caratteristiche che hanno reso Spring il principale framework di Java sono:

- Spring è flessibile: l'ecosistema Spring è ricco di estensioni e librerie sviluppate da altri che aiutano nella realizzazione di numerosissime applicazioni. Prima di sviluppare una certa funzionalità bisogna verificare se esiste una libreria o un'estensione che la implementa, accelerando quindi lo sviluppo dell'applicazione.
- Spring aumenta la produttività: la disponibilità di estensioni e librerie di terze sono fattori che aumentano notevolmente la produttività
- Spring è veloce: il termine veloce può essere inteso in due sensi.
 - Le applicazioni sono più veloci nell'avvio e nell'arresto rispetto ad un'applicazione web JEE. Spring supporta il modello di programmazione reattivo, in grado di aumentare l'efficienza delle applicazioni.

- Grazie a Spring Boot, la produttività degli sviluppatori aumenta notevolmente, consentendo di creare applicazioni più rapidamente rispetto ad altri framework.
- Spring è sicuro: tutte le vulnerabilità segnalate vengono testate in maniera approfondita, consentendo un rapido rilascio di aggiornamenti che risolvono eventuali criticità. Spring mette a disposizione Spring Security, un framework che fornisce autenticazione, autorizzazione e altre funzionalità di sicurezza per le applicazioni enterprise e può essere integrato nelle applicazioni per gestire queste funzionalità critiche.

Spring è stato sempre definito come un framework leggero da utilizzare per lo sviluppo di applicazioni Java. Per leggero si intende che è necessario apportare poche o nessuna modifica al codice della nostra applicazione per usufruire dei vantaggi delle componenti core di Spring. L'ecosistema di Spring è costituito da tanti moduli, ognuno dei quali assolve a determinate funzioni. Per poter utilizzare una funzione è sufficiente importare nell'applicazione il modulo che la implementa. La modularità di Spring è uno dei fattori chiave del suo successo. Un modulo è un file JAR che contiene una serie di classi ed interfacce che definiscono ed implementano le funzionalità del modulo. Ecco come sono suddivisi i moduli di Spring:

- spring-core: è il modulo principale che ogni applicazione Spring deve includere e contiene tutte le classi condivise dagli altri moduli Spring.
- spring-aop: è il modulo che contiene le classi necessarie per utilizzare le funzionalità AOP di Spring. Questo modulo va importato anche se è necessario utilizzare altre funzionalità in Spring che utilizzano AOP.

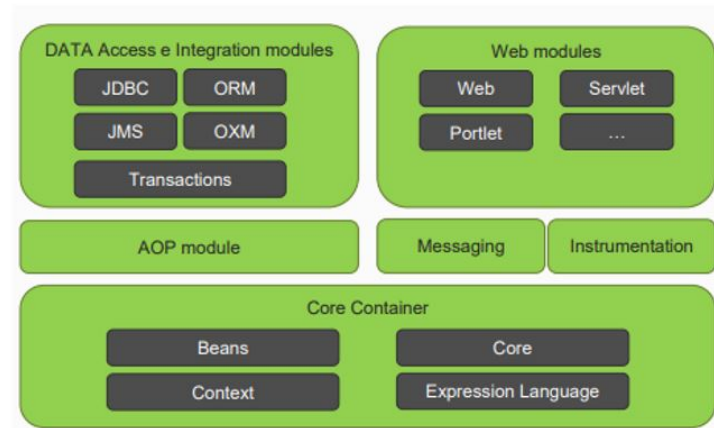


Figura 5.1: Moduli di Spring

- spring-beans : modulo che contiene le classi per gestire i bean Spring
- spring-context: il modulo contiene le classi che forniscono molte estensioni al modulo core. Il modulo contiene anche le classi per l'integrazione degli EJB, JNDI e JMX. Il modulo contiene inoltre le classi per la comunicazione remota, per l'integrazione con i linguaggi di scripting dinamici.
- spring-jdbc: il modulo contiene le classi per il supporto JDBC ed è necessario per le applicazioni che richiedono l'accesso al database.
- spring-orm: il modulo estende le funzionalità del modulo spring-jdbc implementando il supporto ai più diffusi strumenti ORM
- spring-web: contiene le classi principali per l'utilizzo di Spring nelle applicazioni Web, tra cui le classi per gestire l'upload di file, elaborare la query string ecc..

- `spring-webflux`: modulo che contiene le classi necessarie per implementare applicazioni web con `spring Web Reactive`
- `spring-webmvc`: il modulo contiene le classi per utilizzare il framework MVC di Spring.

Per definire un modulo da utilizzare nella nostra applicazione ci sono due modi: manualmente, che è la strada più complicata o tramite un Dependency Management tool tipo Maven o Gradle. Se non viene utilizzato uno strumento di gestione delle dipendenze, bisogna includere manualmente tutti i moduli che dobbiamo utilizzare ed anche quelli necessari perché utilizzati da moduli importanti. Con Maven, tutte le librerie di terze parti richieste verranno incluse automaticamente. Spring implementa l'Inversion of control utilizzando il pattern Dependency Injection per gestire le dipendenze, utilizzando i moduli `spring-core` `spring-beans` e `spring-context`. La componente Spring che crea le istanze e configura gli oggetti prende nome di IoC container. Gli oggetti creati da IoC Container prendono il nome di beans e vengono configurate attraverso file metadati, Java Annotation o codice Java. Il modulo `spring-context` basato su `spring-beans` contiene l'interfaccia `ApplicationContext` che eredita le funzionalità di `BeanFactory` e ne aggiunge altre come: supporto per l'internalizzazione, propagazione di eventi, caricamento di risorse e supporto JEE. Spring presenta all'interno del suo framework Spring Web MVC un framework per lo sviluppo di applicazioni web, costruito sull'API Servlet. Il modello sui cui si basa Spring MVC è il pattern architetturale MVC. Il nome del pattern deriva da Model, componente che modella i dati ricevuti dall'utente; View, la componente che

visualizza le informazioni all'utente; Controller, la componente che gestisce il reindirizzamento delle URL chiamate dall'utente verso le view. Spring MVC consente il mapping di metodi e classi Java con determinati URL, supporta la gestione di differenti tipologie di informazioni restituite al client, consente la realizzazione di applicazioni internazionalizzate e la realizzazione di temi grafici per personalizzare l'esperienza dell'utente. All'interno del framework Spring troviamo Spring Data, sezione che si occupa di fornire gli strumenti necessari per l'accesso ai dati. Spring data contiene diversi moduli, specifici per un dato database e per una specifica tecnologia di accesso ai dati. Spring supporta pienamente l'integrazione con Java Persistence API. Supportando nativamente Hibernate per la gestione delle risorse, le implementazioni DAO e la gestione delle transazioni. Questo supporto è effettuato tramite delle funzionalità IoC che semplificano la configurazione dei vari componenti. Spring Data ha un potente meccanismo per la gestione dei metodi di accesso al database in lettura e scrittura. Questo livello di astrazione è implementato attraverso una serie di strumenti che consentono di automatizzare la creazione dei metodi di gestione dei dati. Esistono due elementi alla base di questo processo:

- Repository: svolge il ruolo di marker e serve per identificare le interfacce delegate alla gestione dell'accesso ai dati
- CrudRepository che definisce le principali operazioni CRUD

5.2 Spring Boot

Spring Boot è un progetto Spring che ha come obiettivo quello di rendere più semplice lo sviluppo e l'esecuzione di applicazioni Spring. Si tratta di un popolare framework open source di livello enterprise per la creazione di applicazioni autonome che vengono eseguite sulla Java Virtual Machine. Un'applicazione Spring richiede generalmente una serie di configurazioni, Spring Boot semplifica lo sviluppo di applicazioni effettuando una configurazione automatica dei componenti utilizzati. Infatti, la grande differenza fra Spring e Spring Boot è che le applicazioni sviluppate con Spring Boot richiedono pochissima configurazione Spring. Spring Boot semplifica lo sviluppo delle applicazioni perché effettua una configurazione automatica, infatti un'applicazione Spring Boot richiede, di solito una configurazione minima. Spring Boot utilizza un approccio "opinionated" ossia convenzionale basato su opinioni e convenzioni proprie. Con Spring Boot si possono realizzare applicazioni Java che possono essere avviate utilizzando il comando `java-jar`, applicazioni web tradizionali distribuite sotto forma di `war`. Spring Boot consente anche di fare l'embedding di Servlet Container nel caso di sviluppo di una applicazione web. Alcune caratteristiche principali di Spring Boot sono

- Starter dependencies: configurazione automatica delle librerie e delle dipendenze dell'applicazione. Spring Boot semplifica la gestione delle dipendenze fornendo e supportando un insieme curato di dipendenze starter. Una dipendenza starter è una dipendenza la cui inclusione implica automaticamente l'inclusione delle sue dipendenze transitive.

- Configurazione automatica di bean e componenti e delle relazioni tra esse: con Spring Boot la configurazione di un'applicazione web è molto semplice, non è necessario nessun altro file in più per configurare il sistema.
- Actuator: per ispezionare un'applicazione Spring Boot in esecuzione: Spring Boot Actuator fornisce un insieme di caratteristiche aggiuntive per il monitoraggio e la gestione delle applicazioni, fornisce inoltre meccanismi di ispezione per analizzare la configurazione dei bean in esecuzione. Tutto sotto forma di risorse e operazioni REST.

5.3 Implementazione del sistema

“Privacy for you” è una piattaforma web che si occupa di insegnare la privacy ai propri utenti attraverso lezioni, quiz e giochi. Presenta una home all'interno della quale si può subito intuire lo scopo del sistema. L'intero sistema inizia ponendo all'utente una semplice domanda “Quanto ne sai di privacy?” invogliando l'utente a eseguire il primo quiz, il “test principale” che darà come risultato un punteggio iniziale e un relativo livello di preparazione dell'utente. Per usufruire dei vantaggi apportati dal sistema l'utente deve registrarsi sulla piattaforma, inserendo i propri dati quali: email, password, nome, cognome e data di nascita. Una volta registratosi sulla piattaforma l'utente dovrà effettuare il login ogni volta che vorrà usufruire del sistema. L'utente può visualizzare i suoi dati inseriti al momento della registrazione nella sezione “Profilo”, all'interno della quale può modificare la propria password o decidere di eliminare il suo profilo. L'utente effettua il test

principale, premendo sul pulsante fai il test presenta nella home. Il test è formato da varie domande, tutte inerenti al tema privacy, ogni domanda deve essere risposta. Una volta risposte tutte le domande e aver inviato il test, l'utente visualizzerà una schermata che lo informa di aver effettuato il test. L'amministratore potrà controllare nella sua sezione utenti il punteggio ottenuto dall'utente e il suo livello di preparazione. L'utente può visualizzare tali informazioni all'interno del suo profilo. L'amministratore si occupa di gestire l'intero sistema e ha una sua home dedicata, all'interno della quale può gestire tutte gli oggetti del sistema: gli utenti, il test principale, le domande del test, gli argomenti di studio e i giochi.

5.3.1 Infrastruttura

L'intero sistema è stato implementato secondo il pattern architetturale Model-View-Controller. Per quanto riguarda le view, queste sono state create utilizzando HTML e CSS grazie al template engine Thymeleaf. Durante la fase di elaborazione della tesi lo sviluppo è stato concentrato sulla parte back-end. I model e i control sono stati implementati con SpringBoot, il database è stato gestito con MariaDB un sistema di gestione di database relazione open source. La prima versione è stata rilasciata nel 2009, nato da una fork di MySQL. (Infrastruttura del sistema presente a pag 87)



Figura 5.2: Home

Figura 5.3: Form di registrazione

Form nel quale l'utente può effettuare la registrazione sulla piattaforma inserendo i propri dati personali


AMMINISTRATORE ACCEDI

PRIVACY FOR YOU
PROMUOVI E PROTEGGI I TUOI DATI

ESCI

HOME PAGE TEST GIOCHI STUDIO PROFILO

Login Form



Email

Inserisci email

Password

Inserisci Password

Accedi

☒ Ricordami

Se non hai un account

Registrati

Figura 5.4: Form per effettuare il login
Form che permette all'utente di effettuare il login

AMMINISTRATORE ACCEDI

PRIVACY FOR YOU
PROMUOVI E PROTEGGI I TUOI DATI

ESCI

HOME PAGE TEST GIOCHI STUDIO PROFILO

Il mio profilo

Ecco i tuoi dati personali

Email	Password	Nome	Cognome	Data	Punteggio	Livello
luisa@gmail.com	luisa	luisa	cauteruccio	31 Dicembre 1996	10	alto

Modifica


Elimina

Ritorna alla home

Figura 5.5: Profilo dell'utente
Profilo nel quale l'utente può visualizzare i suoi dati e le informazioni riguardanti il test principale il punteggio e il livello di preparazione

AMMINISTRATORE

ACCEDI



ESCI

HOMEPAGE

TEST

GIOCHI

STUDIO

PROFILI

Test Principale

Rispondi alle domande per completare il test principale

0

A quale categoria di dati fanno parte le informazioni come nome, cognome, data di nascita, codice fiscale?

☐ personali
 ☐ genetico
 ☐ biometrico

1

Quali sono i caratteri da utilizzare per una password forte e sicura?

☐ lettere
 ☐ numeri
 ☐ entrambi

2

Quanto deve essere lunga una password forte e sicura?

☐ 10 caratteri
 ☐ Massimo 5
 ☐ Non importa la lunghezza

3

Quale e' la password più utilizzata, anche se scorretta?

☐ 1234
 ☐ Password
 ☐ 8h0urtezz@

4

Quale dei seguenti dati è più utile come password?

☐ Informazioni personali
 ☐ Una parola mista formata da simboli come lettere numeri e simboli affiancati
 ☐ Il nome del tuo cane

5

Cosa significa 2FA?

☐ Due nuove applicazioni
 ☐ Autenticazione a due fattori
 ☐ Due file eseguibili

6

Quale è il modo migliore per proteggere i propri dati quando si utilizza un dispositivo fuori casa?

☐ Accedere al wi-fi pubblico
 ☐ Usare una VPN gratuita
 ☐ Utilizzare la connessione dati del proprio gestore di telefonia

7

Il phishing è

☐ Un attacco informatico
 ☐ Un tipo di virus
 ☐ Un video game divertente

8

Quale strumento giuridico protegge la privacy delle informazioni degli utenti in rete?

☐ Il codice civile
 ☐ Il garante privacy
 ☐ L'antivirus installato sul proprio pc

9

Un trojan horse è

☐ Un virus
 ☐ Un antivirus
 ☐ Un software che velocizza il nostro pc

Invia

Figura 5.6: Test principale
 Test principale che comprende le domande alle quali l'utente deve rispondere per conoscere il suo livello



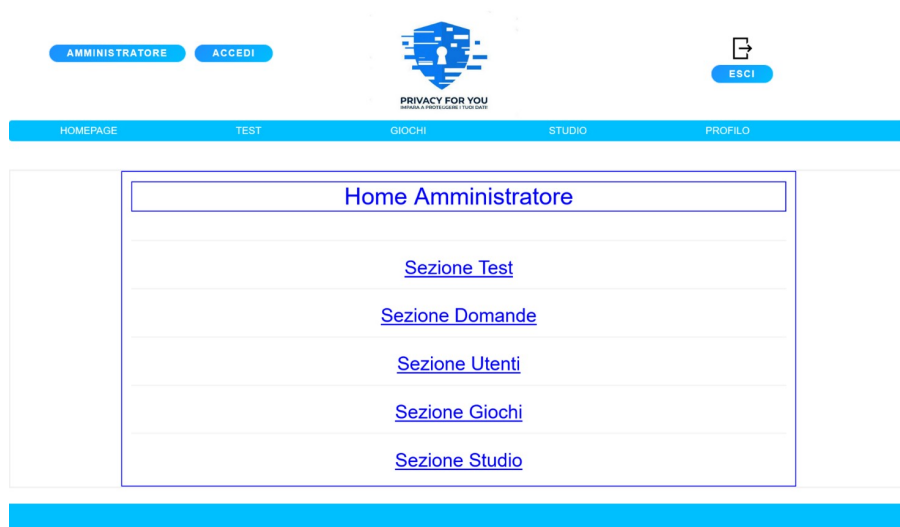
Sezione Utenti

Tutti gli utenti presenti sulla piattaforma

Email	Password	Nome	Cognome	Data	Punteggio	Livello
admin	admin	admin	admin	amministratore	0	Nessun test
lu	lu	lu	lu	lu	6	medio
lui	lu	lu	lu	lu	0	Nessun test
luisa	lu	lu	lu	lu	10	alto
luisa@gmail.com	luisa	luisa	cauteruccio	31 Dicembre 1996	10	alto

[Elimina utente](#)
[Ritorno alla home](#)

Figura 5.7: Sezione utenti amministratore
 Nella sezione utenti, anche l'amministratore può conoscere il livello di preparazione di un utente



Home Amministratore

[Sezione Test](#)

[Sezione Domande](#)

[Sezione Utenti](#)


[Sezione Giochi](#)

[Sezione Studio](#)

Figura 5.8: Home amministratore

AMMINISTRATORE

ACCEDI



PRIVACY FOR YOU

ESCI

HOME PAGE

TEST

GIOCHI

STUDIO

PROFILO

Sezione Domande

Tutti le domande presenti sulla piattaforma

IdDomanda	Testo	Risposta1	Risposta2	Risposta3	Risposta Corretta	IdTest
0	A quale categoria di dati fanno parte le informazioni come nome, cognome, data di nascita, codice fiscale?	personali	genetici	biometrici	personali	TP
1	Quali sono i caratteri da utilizzare per una password forte e sicura?	lettere	numeri	entrambe	entrambe	TP
2	Quanto deve essere lunga una password forte e sicura?	10caratteri	Massimo 5	Non importa la lunghezza	10caratteri	TP
3	Quale e' la password piu utilizzata, anche se scorretta?	1234	Password	SlouRezz@	1234	TP
4	Quale dei seguenti dati è più utile come password?	Informazioni personali	Una parola mista formata da simboli come lettere numeri e simboli alfanumeri	Il nome del tuo cane	Una parola mista formata da simboli come lettere numeri e simboli alfanumeri	TP
5	Cosa significa 2FA?	Due nuove applicazioni	Autenticazione a due fattori	Due file eseguibili	Autenticazione a due fattori	TP
6	Quale è il modo migliore per proteggere i propri dati quando si utilizza un dispositivo fuori casa?	Accedere al wi-fi pubblico	Usare una VPN gratuita	Utilizzare la connessione dati del proprio gestore di telefonia	Utilizzare la connessione dati del proprio gestore di telefonia	TP
7	Il phishing è	Un attacco informatico	Un tipo di virus	Un video game divertente	Un	TP
8	Quale strumento giuridico protegge la privacy delle informazioni degli utenti in rete?	Il codice civile	Il garante privacy	L'antivirus installato sul proprio pc	Il garante privacy	TP
9	Un trojan house è	un virus	Un antivirus	Un software che velocizza il nostro pc	un	TP
55	Domanda	Modificata	da form	form	form	T001
66	Domanda 1	Acqua	Sale	Luisa	Luisa	T001
77	Domanda 1	Acqua	Sale	Luisa	Luisa	T001
88	Domanda 1	Acqua	Sale	Luisa	Luisa	T001

Aggiungi domanda

Modifica domanda

Elimina domanda

Ritorno alla home

Figura 5.9: Sezione domande amministratore
Sezione nella quale l'amministratore può inserire una domanda,modificarla o eliminarla

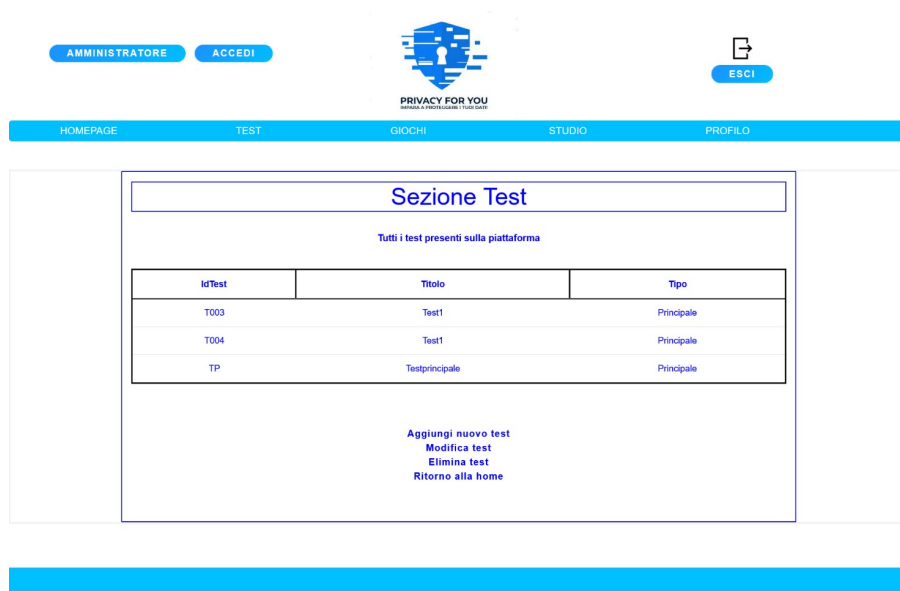


Figura 5.10: Sezione test amministratore
Sezione nella quale l'amministratore può inserire un test, modificarlo o eliminarlo



Figura 5.11: Sezione giochi amministratore
Sezione nella quale l'amministratore può inserire un gioco, modificarlo o eliminarlo



Figura 5.12: Sezione giochi amministratore
Sezione nella quale l'amministratore può inserire un nuovo argomento di studio, modificarlo o eliminarlo

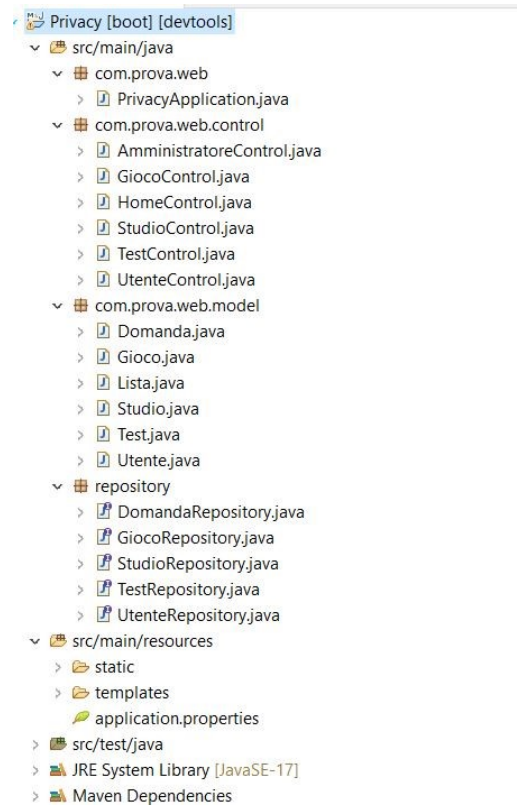


Figura 5.13: Infrastruttura del sistema

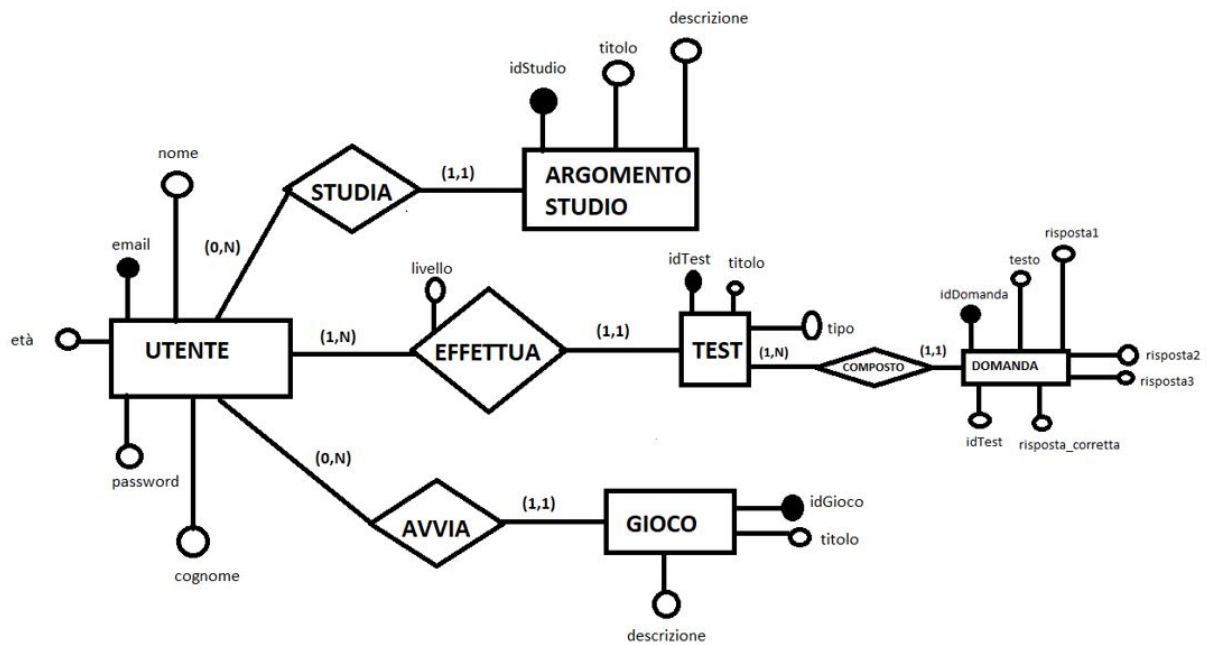


Figura 5.14: Schema relazionale del database

privacy_learning	112,0 KiB
domanda	16,0 KiB
gioco	16,0 KiB
studio	16,0 KiB
test	32,0 KiB
utente	32,0 KiB

Figura 5.15: Tabelle del database all'interno di MariaDB

Capitolo 6

Conclusioni

Il sistema sviluppato ha come obiettivo quello di sensibilizzare gli utenti sul tema della privacy. Il sistema è stato progettato interamente, a livello implementativo risulta ad oggi completo e funzionante la gestione degli utenti, la gestione dell'amministratore e la funzionalità di test principale, funzionalità che permette di sottoporre gli utenti a un test composto da varie domande sul tema della privacy al fine di conoscere in base al punteggio ottenuto un livello di preparazione. Pertanto, il sistema potrà già essere utilizzato all'interno delle scuole come strumento di verifica per conoscere la preparazione degli studenti sul tema della privacy. Le domande inserite all'interno del test principale possono essere modificate dall'amministratore in modo da poter offrire domande adeguate rispetto al grado scolastico e alla classe di riferimento all'interno del quale il test viene svolto. I prossimi passi saranno: quello di utilizzare i risultati ottenuti dal test principale, al fine di implementare le altre funzionalità, migliorare il front-end attualmente offerto dalla prima versione del sistema e creare dei test di usabilità e scalabilità.

Bibliografia

- [1] Anatomia del malware M. Mezzalama, A. Lioy, H. Metwalley ,2013
- [2] Spazi ibridi tra la rete e la piazza: l'evoluzione della comunicazione degli adolescenti ai tempi dello smartphone, Marco Lazzari (2015)
- [3] Spazi ibridi tra la rete e la piazza: l'uso di Internet tra gli studenti delle scuole medie, Marco Lazzari (2015)
- [4] Adolescenti e comunicazione online: la ricerca, Alice Ponzoni, Università degli studi di Bergamo 2014
- [5] I media digitali come strumenti per “esercitare e performare” la genitorialità, Rivista Italiana di Educazione Familiare 2019
- [6] APProva di privacy, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9475065>
- [7] Smartphone:spegni il microfono accendi la privacy,<https://www.garanteprivacy.it/temi/smartphone/microfoni>
- [8] Assistenti digitali i consigli del garante per un uso a prova di privacy, <https://www.garanteprivacy.it/temi/assistenti-digitali>

- [9] I suggerimenti del garante per proteggersi dal phishing, <https://www.garanteprivacy.it/temi/cybersecurity/phishing>
- [10] Minori e le nuove tecnologie: consigli ai grandi per un utilizzo sicuro da parte dei piccoli, <https://www.garanteprivacy.it/temi/minori>
- [11] Malware cosa sono, come riconoscerli e come rimuoverli, www.cybersecurity360.it
- [12] Password compromesse: come scoprire se i nostri account sono ancora sicuri, www.cybersecurity360.it
- [13] App a tutela della privacy: quali sono e come funzionano, www.cybersecurity360.it
- [14] Account Instagram hackerato: come è possibile e come difendersi, www.cybersecurity360.it
- [15] Attacchi credential stuffing: cosa sono e come difendersi dal furto di identità, www.cybersecurity360.it
- [16] Vivaldi, www.vivaldi.com
- [17] Duck Duck Go, <https://duckduckgo.com/>
- [18] Space Shelter, https://spaceshelter.withgoogle.com/intl/it_it/
- [19] Interland, https://beinternetawesome.withgoogle.com/it_it/interland

- [20] Spring e Spring Boot, <https://www.udemy.com/course/spring-e-spring-boot-la-guida-completa/learn/lecture/11693880#overview>
- [21] Quanto ne sai di privacy, <https://www.cie-europa.com/serious-game>
- [22] Datak, <https://www.datak.ch/#/start>
- [23] Il GDPR e come attuarlo: un piccolo libro sulla privacy, Agosto 2020