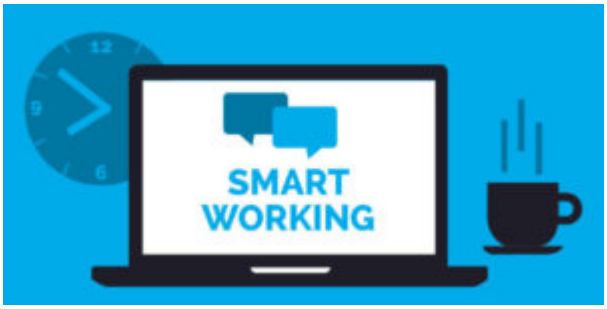
Privacy e protezione dati nello smart working



di PAOLO MANCINELLI-

Negli ultimi anni si è intensificato molto lo smart-working, ovvero il lavoro da remoto. L'utilizzo dello smart-working ha comportato una riduzione dei costi ed un aumento della produttività , ma soprattutto ha dato una maggiore spinta verso un miglioramento della qualità di vita dei dipendenti, creando quel flusso di attività correlate tra vita lavorativa e vita privata; il cosiddetto work life balance. Al contrario lo smart-working, attraverso l'utilizzo di un molteplice flusso di dati in diverse piattaforme comporta sempre dei rischi, soprattutto l'aumento di attacchi informatici che possono comportare una violazione di dati. Per questo occorre, anzi diventa necessario fortificare le strategie di privacy attraverso procedure e software. Seguire questi 5 semplici passi per effettuare uno screening sul proprio stato di protezione:

1. Valutare il rischio e identificare i punti "deboli" , esaminando l'infrastruttura tecnologica, rete , dispositivi e software utilizzati.

• Utilizzo dispositivi personali – (da una parte riduce i costi ma dall'altra comporta un maggiore rischio per i dati);

• Utilizzo di reti non protette, molto spesso criptate;

• Maggiore attenzione e controllo su Phishing, Malware, Password deboli;

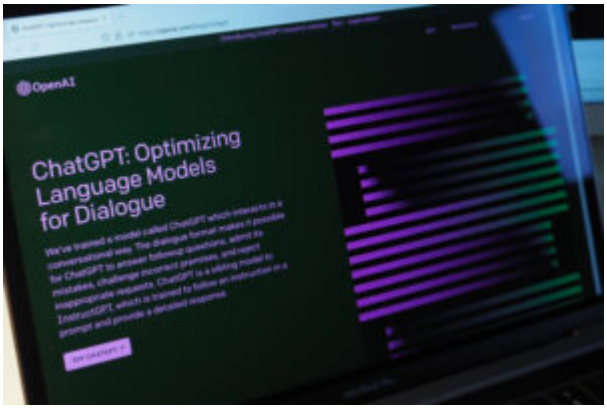
2. Definire una policy comprendente di privacy e protezione

dati
Definire una policy è il passo principale per definire un percorso di protezione d’informazioni sensibili e per creare quella che in gergo si chiama una metrica efficacie. Per la protezione dei dati e la loro gestione possiamo sfruttare i vantaggi della business analytics . La policy sulla privacy e la protezione dei dati devono in primo luogo definire le modalità di gestione dei dati sensibili definendo la loro raccolta, archiviazione e condivisione. Un primo step per la policy è quella di applicare un controllo degli accessi , ovvero definire chi ha accesso ai dati e i casi in cui può farlo; quest’ultimi avranno un’autenticazione a due fattori e password forti. Un ulteriore punto di forza della privacy e protezione dei dati, che devono essere indicate , sono le clausole di conservazione dei dati, che permettono di definire il tempo di conservazione dei dati , quando eliminarli o eliminarli definitivamente;.
3. Come difendersi dalle cyber minacce lavorando da remoto
• Rete privata virtuale o VPN , attraverso di essa i dati vengono cifrati e quindi non viene data possibilità agi hacker di intercettare dati e informazioni sensibili;
• Attacchi DDoS , per evitarli i consigli di utilizzare un servizio basato su icloud , servizio progettato per rilevare e bloccare il traffico dannoso. Può essere rafforzato attraverso firewall, limitazione di velocità e l’utilizzo di rete di distribuzione di contenuti;
• Costante aggiornamento del software di protezione antivirus e malware;
• Utilizzare l’autenticazione a due fattori (password e token di sicurezza);

4. Programmi id formazione per il remote working
Molte persone, scegliendo il lavoro da casa dovranno essere formate, e per questo dovranno essere definiti dei programmi di formazione, tramite i quali, tutta la forza lavoro in “smart” resterà costantemente aggiornata
5. Strategia: aggiornamento e monitoraggio

I cyber criminali, riescono sempre a trovare tutte le falle dei nostri sistemi, per questo è importante un aggiornamento costante sulle misure di sicurezza. Un sistema di protezione e privacy dei dati all'avanguardia e sotto controllo, aiuta ad identificare sia la vulnerabilità sia il momento in cui bisogna rafforzare il livello di protezione. A tal fine può essere condotto ad un audit interno per verificare tutte le strategie aziendali di protezione e privacy , policy e procedure e tecnologie.
In conclusione dobbiamo sempre tenere presente che la sicurezza informatica è un processo continuo, un processo che richiede un costante controllo per far si che tutto si eseguito in modo efficace attraverso un monitoraggio continuo e costanti aggiornamenti.

ChatGPT torna di nuovo disponibile in Italia



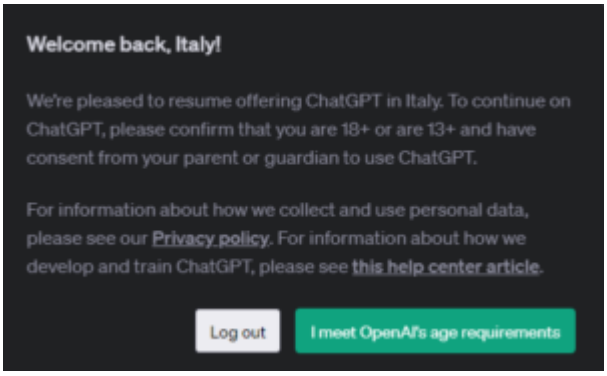
di GIUSEPPE INTAGLIATA –

Il chatbot Chat GPT è tornato operativo oggi in Italia dopo un periodo di stop determinato dal Garante della Privacy. La società proprietaria del chatbot, OpenAI, ha infatti accettato di adeguarsi alla normativa europea sulla privacy e di

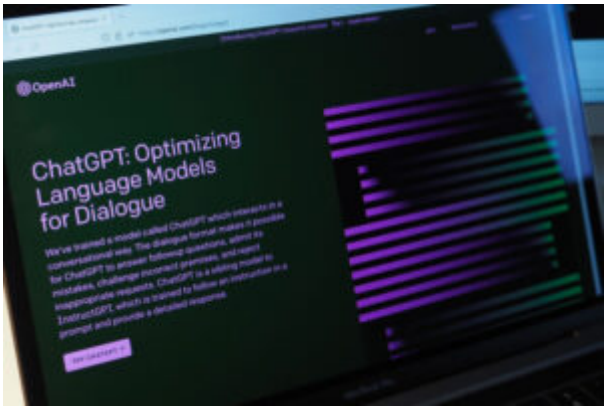
soddisfare le richieste del Garante italiano. Tra queste richieste c’è quella di garantire la possibilità per gli interessati, anche non utenti, di richiedere la rettifica dei dati personali generati in modo errato dal servizio o la loro cancellazione.

La settimana scorsa, OpenAI aveva già permesso a tutti gli utenti mondiali di escludere le proprie conversazioni dal training dell’algoritmo. Ora, Chat GPT dovrà anche consentire agli interessati non utenti di esercitare il diritto di opposizione in modo semplice e accessibile rispetto al trattamento dei loro dati personali utilizzati per l’esercizio degli algoritmi. Inoltre, OpenAI dovrà riconoscere lo stesso diritto agli utenti, qualora individuino il legittimo interesse come base giuridica del trattamento. Infine, OpenAI dovrà promuovere una campagna pubblicitaria per far conoscere a tutti, anche ai non utenti, la possibilità di escludersi dal chatbot.

Il Garante della Privacy ha anche affrontato un’altra questione importante riguardante la verifica dell’età dei minori. In particolare, ha ordinato di implementare entro il 30 settembre 2023 un sistema di verifica dell’età degli utenti, in grado di escludere l’accesso agli utenti sotto i 13 anni e ai minorenni non autorizzati dai genitori.



Come continuare ad utilizzare ChatGPT in Italia nonostante il blocco (legale)



di GIUSEPPE INTAGLIATA –

Il servizio di intelligenza artificiale **ChatGPT**, sviluppato da **OpenAI**, è stato bloccato in Italia a causa di problemi relativi alla privacy degli utenti. La decisione è stata presa dal Garante per la protezione dei dati personali e della privacy e ha avuto effetto immediato nel nostro paese. Sebbene la vicenda susciti molte controversie, molti si chiedono se sia ancora possibile utilizzare il servizio in Italia. La risposta è sì, a patto di utilizzare diversi "trucchi" che ora vi spiegherò:

Una valida soluzione può essere l'utilizzo di una **VPN** (Virtual Private Network) che permetta di aggirare il blocco. Senza una VPN, il portale restituisce un messaggio che certifica l'impossibilità di usare il servizio e su Bing Chat (da poco integrata in Windows 11 con ChatGPT) vengono visualizzati solo risultati di ricerca correlati al posto della finestra di chat dell'AI.

Per utilizzare una VPN, è necessario installarne una e impostare un paese diverso dall'Italia per la localizzazione. Questo passaggio permette di simulare la presenza al di fuori

dei confini italiani e di accedere nuovamente alla schermata iniziale del chatbot senza errori o blocchi.

Tra le varie disponibili, è possibile utilizzare Opera GX, un browser solitamente utilizzato per i videogiochi che include una VPN gratuita e illimitata. Una volta installato, è possibile abilitare la VPN andando nelle impostazioni del browser e attivando l'opzione "VPN" nella sezione "Privacy e sicurezza". Selezionando un paese diverso dall'Italia, sarà possibile utilizzare ChatGPT come sempre. Esistono anche numerose VPN per smartphone anche se bisogna stare attenti soprattutto leggendo le recensioni che siano affidabili.

Essendo ChatGPT un progetto **open-source**, ovvero il codice sorgente può essere accessibile e modificato da qualsiasi utente che abbia competenze in merito, esistono altri applicativi di questo tipo anche scaricabili direttamente dallo store del telefono cercando ad esempio "chat gpt ai". La maggior parte, però, richiedono una registrazione a pagamento dopo un numero di messaggi mandati all'intelligenza artificiale. E' stato, però, recentemente sviluppato un sito dedicato proprio all'uso del bot in Italia, gratuito e senza bisogno di registrazioni. Si chiama "PizzaGPT", dal nome può sembrare poco affidabile o una truffa ma posso assicurare che funziona correttamente (provato diverse volte) in quanto utilizza il codice sorgente di ChatGPT ma rendendolo accessibile anche dall'Italia in linea con le norme sulla privacy.

Con questi metodi sarà, quindi, possibile continuare a utilizzare ChatGPT legalmente in Italia nonostante il blocco.

Privacy e Cybersecurity: Stato dell’arte, sistemi di difesa e resilienza. Il 4 aprile l’Inps ospita la V Conferenza Nazionale

ROMA – Il prossimo 4 aprile, dalle ore 9.00 si terrà a Palazzo Wedekind, in piazza Colonna a Roma, la V Conferenza Nazionale “Privacy e Cybersecurity: stato dell’arte, sistemi di difesa e resilienza” organizzata dall’Università degli Studi di Roma Tor Vergata ed un partenariato di società pubbliche o private, con il patrocinio dell’INPS.

Si discuterà delle attuali soluzioni di difesa per la cybersecurity, in prospettiva istituzionale, tecnologica e umana, al fine di prospettare linee di sviluppo auspicabili per il presente e futuro.

L’evento sarà aperto da Orazio Schillaci, Rettore dell’Università degli Studi di Roma “Tor Vergata”, da Pasquale Tridico, Presidente INPS, dall’on. Angelo Tofalo, già Sottosegretario di Stato alla Difesa e da Roberto Baldoni, Direttore generale dell’Agenzia nazionale per la cybersicurezza.

La conferenza, moderata da Elisabetta Zuanelli, Coordinatore del Partenariato per il Piano di formazione in Cybersecurity,

Cyberthreate e Privacy ed Esperto ONU di Intelligenza artificiale, si articolerà intorno a quattro tavole rotonde:
“La Cybersecurity nei sistemi di difesa: reti, DNS, sistemi operativi, applicativi. Stato dell’arte, strumenti e tecniche”;
“I destinatari fruitori delle soluzioni e delle tecnologie della sicurezza”;
“I fornitori di servizi digitali: reti di telecomunicazione, DNS, sistemi operativi, cloud, e applicativi”;
“I fornitori di soluzioni e tecnologie di difesa”.
Interverranno specialisti della sicurezza informatica e cyber insieme ad alcuni player istituzionali e aziendali più impegnati in tema di cybersecurity, al fine di approfondire le misure per una strategia nazionale e operativa, individuare risposte generali e di sistema nella digitalizzazione innovativa, favorire una prospettiva comune nelle soluzioni per sistemi di difesa integrati.
L’evento sarà accessibile anche in streaming al seguente link: Cybersecurity: stato dell’arte, sistemi di difesa e resilienza”
Il link con accesso diretto sarà pubblicato anche sui seguenti siti: www.cybersecurityprivacy.it e www.ai4a.eu.

Che cos’è Signal e perchè se ne parla

di GIUSEPPE INTAGLIATA –

VITERBO – E’ da qualche giorno che agli utenti che utilizzano WhatsApp appare un messaggio che richiede di confermare le nuove condizioni d’utilizzo per poter continuare ad utilizzare il servizio entro il mese di Maggio. Proprio a causa di queste nuove condizioni che modificano la maniera con cui vengono trattati i dati personali, molti utenti hanno deciso di passare ad altre applicazioni per la messaggistica instantanea. Tra queste quella che ha raggiunto il maggior numero di nuovi utenti è **Signal**.

Signal, proprio come WhatsApp, consente di scambiare messaggi di testo, foto, video, audio e consente di creare gruppi o effettuare chiamate o videochiamate. Tutto questo utilizzando la **rete wifi** o la **connessione dati** del telefono. La vera differenza tra queste due applicazioni è che Signal utilizza un sistema di crittografia più profondo rispetto a WhatsApp. Questo sistema (chiamato X3DH), permette di mantenere privata la comunicazione tra due utenti. Inoltre Signal raccoglie molti **meno metadati**, ovvero informazioni sulla data di ricezione o invio di un messaggio o di una foto, di una chiamata o dell’ultimo accesso.

Se volete provare Signal, vi basterà scaricarla e installarla cercandola sullo **store** (Google Play per Android e App Store

per iPhone). Una volta aperta inserite il vostro numero di telefono e riceverete un codice di conferma per il numero. Una volta inserito il codice potete scegliere il nome da visualizzare nell’applicazione e un’immagine profilo. Apparentemente è molto simile a WhatsApp e, con lo **stesso numero**, potete utilizzare **entrambe** le applicazioni.