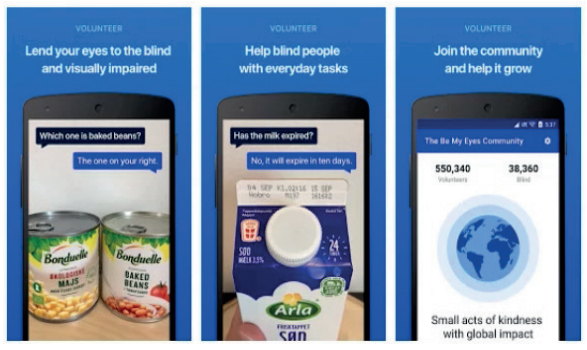
Con l'app «Be My Eyes» si prestano gli occhi a chi non vede

«Be My Eyes» è un'applicazione per smartphone gratuita, nata inizialmente per mettere in contatto le persone non vedenti con dei volontari (circa 6,3 milioni) pronti ad aiutarli da remoto per ogni richiesta. Recentemente è stata integrata con un nuovo generatore dinamico di image-to-text alimentato da GPT-4 (un chatbot di intelligenza artificiale) di OpenAi, un'organizzazione, senza scopo di lucro, di ricerca sull'intelligenza artificiale avente lo scopo di promuovere e sviluppare un'intelligenza artificiale di tipo friendly AI per il benessere dell'umanità. Questo nuovo aggiornamento dell'applicazione viene presentato da Lucy Edwards, una ragazza inglese non vedente, sul suo profilo Instagram. In un reel



pubblicato, la ragazza mostra di trovarsi in palestra e di aver bisogno di sapere dove sono posizionati i tapis roulant, scatta quindi una foto e «Be My Eyes» le indica come arrivare al macchinario libero più vicino. Questo assistente virtuale può essere ancora più specifico e dettagliato, come in un altro esempio che Edwards mostra: lo usa su un catalogo di abbigliamento ed il programma le descrive precisamente i vestiti indossati dalle modelle e tutte le altre informazioni richieste.
In caso lo strumento non fosse in grado di rispondere correttamente ad una domanda, offrirà automaticamente la possibilità di collegare l'utente ad un volontario disponibile per l'assistenza
Attualmente questa funzione è in fase di test per il feedback da parte di alcuni utenti dell'applicazione; in caso di maggioranza di feedback positivi, nei prossimi mesi, il Virtual Volunteer verrà reso disponibile a più persone non vedenti. «Speriamo di applicare questa tecnologia per fornire alle persone potenti strumenti e funzionalità per arricchire la loro esperienza di assistente virtuale in modi sorprendenti e complessi che non avremmo mai pensato sarebbero stati possibili», scrive il team di Be My Eyes sul sito ufficiale.

Anna SBARDELLATI

APOSTOLATO DIGITALE

condividere codici di salvezza

AUMENTANO I RIFIUTI TECNOLOGICI – LA VULNERABILITÀ È LEGATA ALLA SICUREZZA

Le 5 regole che allungano la vita dei Pc

Accanto all'acquisto di device di qualunque tipo è previsto un aggiornamento periodico del software che corregge i bug e ci protegge dalle vulnerabilità. Un giorno, però, gli aggiornamenti smettono di arrivare e scatta la necessità di acquistare un nuovo dispositivo. Parliamo di obsolescenza tecnologica (quello stato di cose per cui il nostro device diventa inutilizzabile in sicurezza, lato software e hardware), peggio ancora quando è programmata (quando cioè le case produttrici peggiorerebbero di proposito le prestazioni dei dispositivi più vecchi per spingere gli utenti a comprare quelli nuovi). Lo scorso Rapporto Annuale del Centro di Coordinamento Raee rivela che la produzione dei rifiuti tecnologici del solo 2022 ha superato le 361 mila tonnellate. Sebbene si tratti di una leggera riduzione rispetto all'anno precedente, sono ancora molte le apparecchiature da smaltire ed è in continua diminuzione il tempo di durata dei dispositivi elettronici.

Dunque, come far sopravvivere i nostri dispositivi all'obsolescenza tecnologica? Superati i termini per l'aggiornamento si diventa più vulnerabili a bug e attacchi informatici. È possibile quindi continuare ad utilizzare i nostri dispositivi in sicurezza? Sì, con alcuni accorgimenti in più. Ecco cinque buone prassi per mantenere alto il livello di sicurezza.
1) Aggiorna periodicamente il tuo browser. Rimanere al passo con gli aggiornamenti del browser offrirà una certa protezione da siti web dannosi. Società di browser affidabili come Mozilla aggiornano le loro app per funzionare su computer che hanno più di 10 anni.
2) Evita comportamenti a rischio. Non aprire messaggi o fare clic su collegamenti provenienti da mittenti sconosciuti e utilizza solo app offerte da marchi affidabili. I dispositivi Android sono più suscettibili ai malware rispetto ai telefoni Apple, in parte perché possono essere configurati per installare app da app store non autorizzati. Inoltre, molti produttori smettono di supportare i dispositivi Android dopo solo due anni. Che fare? I proprietari di dispositivi Android obsoleti possono aggiungere un livello di protezione installando un'applicazione che permette l'identificazione dei malware.
3) Proteggi i tuoi account online. Configura i tuoi account online con l'autenticazione a due fattori. Questa pratica genera un codice univoco tramite un'app o un messaggio di testo ogni volta che accedi a un sito: può aiutare a prevenire l'accesso inappropriato al tuo account in caso di furto della password. 4) Installa un sistema operativo diverso. Esistono passaggi più avanzati che possono mantenere un dispositivo funzionante e sicuro oltre la sua vita supportata. Uno prevede la sostituzione del sistema software del produttore con un'alternativa. L'installazione di un sistema operativo diverso richiede alcune conoscenze tecniche, ma una miriade di risorse e tutorial online offrono istruzioni dettagliate per l'aggiunta ad esempio di Linux, un sistema operativo open source noto per la solida sicurezza.
5) Lato smartphone. I possessori di smartphone hanno certo meno scelte. Per Android, c'è LineageOS, un sistema operativo Mobile open source, che ha ricevuto recensioni positive per la sua solida sicurezza. I dispositivi mobili Apple obsoleti, invece, non possono essere facilmente modificati per installare un sistema operativo alternativo. In effetti, gli esperti di sicurezza sconsigliano il "jailbreak" o l'iniezione di software non autorizzato, perché può indebolire la sicurezza del dispositivo Apple.
L'obsolescenza tecnologica però non riguarda solo il software, ma anche l'hardware e a volte il nostro device proprio non ce la fa più a svolgere le funzioni per cui è stato progettato. Cosa possiamo fare quando, ad esempio, la batteria si scarica spesso e costi, sforzi e rischi si sommano, rendendo inutilizzabile il nostro dispositivo? La soluzione potrebbe essere disattivare la connessione Internet di un apparecchio datato per utilizzarlo, in sicurezza, per attività leggere come riprodurre musica. Se non è connesso alla rete, non importa che non sia aggiornato.

A.G.

Notizie digitali
Digital News Report 2022

IL 14 GIUGNO – CON 499 VOTI A FAVORE

Parlamento europeo, sì all'AI Act

Lo scorso 14 giugno 2023, il Parlamento europeo ha dato il suo benestare adottando con 499 voti a favore, 28 contrari e 93 astenuti, l'AI Act e cioè il Regolamento sull'Intelligenza artificiale, tanto atteso.
Ora inizia la fase conclusiva tra colloqui e ultimi giri di tavolo con i governi della Ue per giungere al testo definitivo e, quindi alla sua pubblicazione in Gazzetta Ufficiale europea che si auspica tra la fine di quest'anno (2023) e l'inizio del prossimo (2024).

La ratio di fondo, senza entrare troppo nel merito del final draft, è quella di garantire che l'AI sia sviluppata e adoperata in modo conforme ai diritti dell'Unione.
Ad esempio, nello specifico tra gli altri l'AI Act intende «promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile e garantire un livello elevato di protezione della salute, della sicurezza, dei diritti fondamentali, della democrazia e dello Stato di diritto, nonché dell'ambiente, dagli effetti nocivi dei sistemi di intelligenza artificiale nell'Unione, sostenendo nel contempo l'innovazione e migliorando il funzionamento del mercato interno».
Ecco, la necessità che la normativa segua il cd risk based approach ovvero un approccio basato sul rischio stabilendo obblighi per fornitori/operatori dei sistemi di AI, a seconda del livello di rischio possibili e generabili. Da qui, i sistemi di AI aventi un livello di rischio non accettabile in relazione alla sicurezza delle persone dovranno essere tassativamente vietati.
Ma non è tutto, gli europarlamentari hanno voluto, tra gli altri, ampliare l'elenco inclusivo dei divieti sugli usi intrusivi e discriminatori dell'AI (sistemi di identificazione biometrica remota, sistemi di polizia predittiva riconoscimento delle emozioni, estrazione di dati). Il tutto per evitare che l'AI cagioni danni significativi per la salute, la sicurezza, i diritti fondamentali delle persone.
Circa i sistemi di AI generativa (ChatGPT) introdotti nell'ultimissima versione grazie ad alcuni emendamenti apportati, occorre che rispettino i requisiti di trasparenza.
In generale, se da un lato l'AI Act intende stimolare l'innovazione nel campo delle tecnologie emergenti sostenendo in particolare le PMI, con sgravi grazie alla messa a disposizione di licenze open-source; dall'altro vuole rafforzare «il diritto dei cittadini di presentare reclami sui sistemi di IA e di ricevere spiegazioni sulle decisioni basate su sistemi di IA ad alto rischio con un impatto significativo sui loro diritti fondamentali».
La strada tracciata è quella giusta, per quanto prevedibili siano ulteriori sforzi per «rendere l'ambiente dell'AI amichevole e funzionale ai bisogni di tutti e non solo a quelli di pochi», come sostengono alcuni autorevoli commentatori. Ma innegabili sono i benefici, specie se riconducibili ad un uso consapevole dell'AI.
Tuttavia, una domanda conclusiva sorge spontanea: quanto l'AI quale tecnologia all'avanguardia, sarà al «servizio dell'umanità» anziché uno strumento pericoloso che rischia l'appiattimento del pensiero umano? Ma di questo ne abbiamo già scritto.

Chiara PONTI