Volontariato in tempo di Covid la miniguida sulle iniziative on line

Il volontariato non si è fermato durante la pandemia. Numerosi esempi hanno dimostrato l'impegno dei volontari che, per garantire la continuità dei servizi e mantenere il distanziamento fisico, hanno cercato nuovi modi per rimanere vicini ai più fragili e rispondere ai loro bisogni. Non appena sono state pubblicate le prime limitazioni dovute all'emergenza Covid-19, è stato necessario trovare delle soluzioni alternative al fine di ridurre i rischi per la salute di operatori e destinatari. A facilitare tutto questo sono state le tecnologie digitali; grazie ad esse è stato possibile raccogliere, contenere, dirottare le motivazioni dei volontari e stimolare sia lo sviluppo di nuove modalità di servizio, sia la progettazione di nuovi interventi. Per comprendere meglio una parte di questo cambiamento la Fondazione Sodalitas, in collaborazione con imprese e organizzazioni no profit, ha svolto un'analisi sull'esperienza virtuale del Volontariato d'Impresa, cioè quell'insieme di azioni che un'impresa promuove a favore della comunità attraverso il coinvolgimento dei propri dipendenti durante l'orario di lavoro, ma nel ruolo di volontari. A partire da questa analisi, la fondazione ha realizzato la «Miniguida sul Volontariato d'Impresa Virtuale» che mostra sia le criticità del servizio virtuale, sia le opportunità offerte dagli strumenti digitali: raggiungere nuovi e più numerosi destinatari, ampliare la gamma dei servizi, favorire la condivisione di competenze, garantire maggiore accessibilità e flessibilità. La miniguida è uno strumento utile per chi intende sviluppare progetti ed iniziative online, ma anche un'occasione per riflettere sui processi di trasformazione che coinvolgono il mondo del volontariato. È ancora troppo presto per dire quale volto quest'ultimo avrà dopo la pandemia, per ora possiamo solo osservare che nella solidarietà siamo più capaci di adattarci ai nuovi scenari, segno che l'ostacolo del «si è sempre fatto così»non è poi così insormontabile.

Ivan ANDREIS

APOSTOLATO DIGITALE

condividere codici di salvezza

Il web è già umano, ma serve una nuova visione

Ancor precedente al problema: «Come umanizzare il web?», è la domanda: «Cosa significa umanizzare il web?». Qui si creano varie e confusionarie sovrapposizioni: custodirne il protagonista - ma cosa significa custodirlo? Porre delle sanzioni? Dei limiti? Utilizzare lo strumento diversamente? Mostrarne le potenzialità positive? Emerge allora il reale problema: non è possibile umanizzare qualcosa se prima non si possiede un'idea sul chi sia l'umano. Il rischio è quello di cadere in retoriche richieste di umanizzazione, di tutele e di custodie senza sapere chi sia colui che utilizza il web. E, non sapendolo, davanti alla potenza espressiva del web, si corre anche il rischio di elevarlo a criterio semantico alla luce del quale interpretare l'essere umano. Intrattenimento, comunicazione, umorismo, pornografia, spaccio di droga e di armi, giochi, gratificazione, lavoro, memorie condivise, foto autoreferenziali, attacchi informatici, comunità, confidenze, conferenze, dibattiti, litigi, lotte etniche, terrorismo, evangelizzazione, commercio; tutto questo non parla già dell'essere umano? La questione allora va capovolta: non chiedersi come il web possa essere umanizzato, ma quanto il web, con le sue logiche e i suoi algoritmi, esaurisca il senso dell'essere umano. Lo esaurisce? Evidentemente no. Manca allora una riflessione capace di ri-significare il ruolo dell'umano nella contemporaneità in relazione alle sue creazioni tecniche, compreso il web ma non solo il web; una riflessione in grado di dire chi sono, oggi, l'uomo e la donna. Ma per farlo è necessario un criterio di riferimento che li superi, che vada oltre, non che li descriva. Il web non ha alcun bisogno di essere umanizzato: è «umano, troppo umano» già così com'è proprio perché è l'essere umano che lo ha creato e che, per suo mezzo, esprime se stesso - al massimo necessita di una regolamentazione per scongiurarne gli effetti negativi. Il web oggi ha bisogno di essere ricollocato e ri-pensato alla luce di una nuova visione dell'essere umano. Ma questa visione, al momento, manca: deve essere concepita o riscoperta.

Luca PREZIOSI

Etica e Intelligenza artificiale

Etica dell'Intelligenza Artificiale o Etica Umana? Voce ai ragazzi. Evento organizzato dall'Associazione Italiana per l'Intelligenza Artificiale.

ANALISI – ANCHE DA CASA DOBBIAMO GUARDARCI DA TRUFFE ON LINE DI OGNI GENERE

Cyber criminali, pericolo sottovalutato

Mai come in questo periodo in cui stiamo vivendo un «salto quantico» nell'evoluzione tecnologica e nel processo di digitalizzazione di tutti i settori della nostra società, siamo esposti al cyber crime: attività criminali – a scopo di profitto – volte a colpire o utilizzare per scopi malevoli un computer, una rete di computer o un dispositivo connesso alla rete. Dalle frodi informatiche, al furto d'identità o furto di dati finanziari, o aziendali, ma anche cyber-estorsioni o cyberspionaggio.
La maggior parte dei crimini informatici (anche se non tutti), viene commessa da hacker per realizzare profitti illeciti. Si tratta sia di individui singoli, sia di organizzazioni, alcune delle quali altamente specializzate.
Spam, phishing, malware, botnet, una ridda di termini dal significato spesso oscuro, di fronte ai quali ci sentiamo impreparati ed indifesi.
Da comuni cittadini, siamo esposti al phishing - una frode informatica realizzata attraverso l'invio di e-mail contraffatte, finalizzata all'acquisizione illegale di dati riservati, oppure volta ad indurci al download di un file oppure al collegamento a un sito web infetto e infestante.
Anche da casa dobbiamo guardarci da truffe online di ogni genere. Questo vale per i più vecchi come per i più giovani. Secondo una ricerca della Lloyds Bank, i giovani tra i 18 e i 34 anni sono preda delle frodi online più di qualsiasi altra fascia d'età, sebbene «nativi digitali».
La pandemia poi è stata una manna per i criminali cibernetici che ne hanno approfittato per colpire consumatori ed organizzazioni di tutti i settori, anche politiche o commerciali. Gli attacchi di phishing e malware collegati al Covid-19 sono passati da meno di 5.000 a settimana registrati a febbraio, a oltre 200.000 a settimana a fine di aprile. Azioni che si sono intensificate a maggio e giugno. Ma non siamo solo nel mirino come comuni cittadini: anche le nostre attività commerciali e le imprese, piccole o grandi che siano, si devono attrezzare. Nessuna esclusa. Infatti, se è vero che aumenta ogni anno il budget che le grandi aziende stanziano per la cyber security, le Piccole Medie Imprese spesso stentano a percepirlo come un rischio reale per il loro business, diventando uno degli obiettivi privilegiati dei cyber criminali. Poco difese, inconsapevoli dei rischi, e spesso neppure in grado di rilevare la portata dei furti subiti. Molti attacchi non vengono denunciati e spesso nemmeno rilevati. Ogni dato di tipo commerciale, informazioni private, know-how o indirizzi di posta elettronica vengono sottratti per finire poi sul mercato nero e alimentare altri reati informatici. Queste azioni possono costare fino a diversi milioni di euro per ogni singola azienda.
Nell'ultimo rapporto dell'Europol IOCTA 2020, vengono identificati i trend in questo settore e gli ambiti maggiormente sotto controllo da parte delle forze dell'ordine. I cyber criminals stanno adottando nuove tecniche per colpire le loro vittime a un ritmo senza precedenti e sono costantemente alla ricerca di «metodi per evitare il rilevamento» (per esempio attraverso crittografia e anonimizzazione). Già oggi dobbiamo essere pronti ad un significativo aumento di malware studiati per il *mobile*, visto il crescente utilizzo di dispositivi portatili.
Ma è davvero così vicino a noi? Per farvi un esempio: nella sola settimana del 25 settembre 2020, il Cert-Agid (Computer Emergency Response Team dell'Agenzia per l'Italia Digitale) ha rilevato 22 campagne malevole del cybercrime contro l'Italia. Il phishing ha sfruttato soprattutto Aruba, Office365 e Wetransfer. I principali vettori dei malware, invece, sono stati gli allegati (19 campagne) e i link (tre).
E allora che possiamo fare? Intanto informarci di più e meglio. Il Cert-Agid ad esempio ha creato una serie di «pillole informative» alla portata di tutti, installare e aggiornare anti virus adeguati: ma soprattutto non esitare a contattare la Polizia Postale (https://www.commissariatodips.it) per chiedere informazioni, segnalare reati informatici o fare denuncia (anche online).

Come cittadini siamo esposti al phishing, una frode informatica realizzata con l'invio di e-mail contraffatte, finalizzata all'acquisizione illegale di dati riservati

Vittoria LUDA
Nazioni Unite - UNICRI