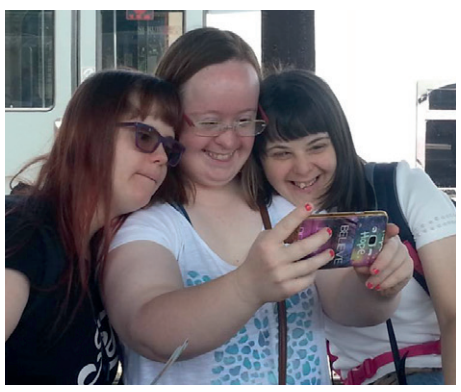
Disabilità intellettiva, un'«app» per il tempo libero

Raggiungere il maggior livello possibile di autonomia, nella vita privata come al lavoro, è uno degli obiettivi principali che i ragazzi con sindrome di Down devono affrontare. Un percorso che comincia da bambini e arriva fino all'età adulta, passo dopo passo. Al loro fianco ci sono le famiglie e la scuola, ma anche realtà specifiche come l'Associazione Italiana Persone Down (AIPD), che nell'ultimo periodo ha messo in campo molte idee innovative al fine di incoraggiare il riavvio della vita sociale e l'indipendenza. È così che a Bergamo è stato lanciato un crowdfunding per la realizzazione dell'applicazione «App and Out». Nata nell'ambito del progetto «Il Buon tempo», l'applicazione «ha lo



scopo di far sviluppare le potenzialità di ognuno ed accrescere l'empowerment in un mondo adulto fatto di relazioni. Come tutti, si impara a rapportarsi con gli altri e a coltivare un tempo di qualità», come spiega Gabriella Ciullo, Responsabile operativo dell'AIPD di Bergamo. L'app infatti sostituisce il cosiddetto «foglio uscita», uno strumento in grado di fissare le informazioni utili per svolgere al meglio gli incontri con gli amici. Il proposito dell'applicazione è quello di essere gradualmente collegata a varie realtà del territorio, per favorire al meglio lo scambio delle informazioni ed aumentarne l'utilità per la comunità.
Un altro progetto significativo è «Museo per tutti», promosso da L'abilità Onlus, che nasce con lo scopo di rendere più inclusivi i luoghi di cultura, in occasione delle Giornate Europee del patrimonio. «L'iniziativa è rivolta a bambini, ragazzi, adulti con ogni tipo di disabilità intellettiva, quindi da persone con sindrome di down a quelle con sindromi rare in cui è compromessa la funzione mentale, persone con deficit di attenzione, concentrazione, memoria, orientamento», spiega Carlo Riva, direttore della Onlus. E aggiunge, «punta a promuovere l'autonomia perché la persona con disabilità non ha bisogno di una visita guidata ad hoc, ma prende la guida e può andare da sola al museo».

Jasmine MILONE

APOSTOLATO DIGITALE

condividere codici di salvezza

SUGLI SMARTPHONE LA NUOVA FRONTIERA DEL CYBERCRIME – VIGILARE NON SOLO SULLE MAIL

Frodi on line a Natale, attenzione agli Sms dei finti corrieri…

I phisher sono cyber criminali specializzati nel progettare ed eseguire attacchi che hanno come scopo principale quello di sottrarre alle vittime le credenziali d'accesso ai più comuni siti internet (banche, vettori logistici, e-commerce ad esempio).
La stagione dello shopping natalizio rappresenta un periodo di grandi affari per i phisher, una sorta di «alta stagione del Cyber Crime»!
I tradizionali attacchi di phishing arrivano ai malcapitati attraverso una mail, scritta spesso in maniera sgrammaticata e con un allegato da scaricare: accortezza, diffidenza delle persone e sistemi di sicurezza antiphishing, contribuiscono a rendere meno efficaci gli attacchi di questo tipo.
Oggi la nuova frontiera del cybercrime e di questo tipo di attacchi sono però i dispositivi mobili: i nostri smartphone. Giorno dopo giorno, infatti, aumentano i tentativi di queste nuove truffe telefoniche e l'efficacia è in crescita grazie ad un mix criminale di approcci nuovi e vecchi.
Lo «smishing» è un attacco di phishing su mobile che arriva con un sms e di solito include un testo ed un falso link (della nostra banca ad esempio o relativo ad una consegna) attraverso il quale l'attaccante prova a sottrarre informazioni personali.
Vale la pena porre l'attenzione su due tipologie di questo attacco; sono entrambe raffinate, acute e spesso efficaci.
Caso uno: arriva un messaggino: grafica di un notissimo vettore logistico che dichiara problemi con una consegna e chiede di riprogrammare (siamo in dicembre, ci teniamo che i regali arrivino puntuali). Il link inserito nell'sms è però un link malevolo che indirizzerà gli sprovveduti su una finta pagina, nella grafica totalmente identica all'originale, in cui sarà necessario

accedere inserendo le proprie credenziali. È questo il momento in cui gli attaccanti le sottraggono e possono avere accesso al profilo della vittima sottraendone (rubando!) i dati sensibili, compresi quelli della carta di credito.
Caso due: questo attacco usa una nuova formula ibrida, sullo smartphone arriva un sms proveniente apparentemente dalla banca del malcapitato (la banca non c'entra nulla ovviamente), stavolta senza alcun link su cui cliccare, e che pone una domanda semplicissima: «Hai autorizzato un pagamento di 500 euro dal tuo conto corrente? Sì o no».
Richiesta semplice e ragionevole a cui si fa in fretta a rispondere: no, ad esempio.

Lo «smishing» è un attacco che arriva con un testo ed un falso link per rubare informazioni personali

A quel punto scatta la seconda fase della truffa, alla vecchia maniera: una telefonata dell'attaccante che si presenta come addetto dell'ufficio antifrodi della banca e comunica che è stato rilevato un tentativo di frode e deve verificare se al telefono ci sia il titolare del conto o il truffatore: per farlo ha bisogno di verificare le credenziali d'accesso al conto corrente. Da qui è semplice immaginare il seguito.
C'è anche la buona notizia fortunatamente: che siano sofisticati o meno gli attacchi di phishing su mobile possono essere disinnescati!
Il consiglio è semplice: hai un dubbio? Non reagire impulsivamente! Prenditi un minuto per riflettere: ad esempio cerca il contatto della tua banca sui canali pubblici, richiama e accertati di cosa sta succedendo.
Chiudo augurando buone feste e consigliando due bei regali per familiari ed amici.
Il primo: ricordargli le regole base per evitare le truffe legate al phishing. Non rispondere in caso di dubbio e prendere tempo!
Il secondo: un tool di Web Protection Antiphishing, ce ne sono anche sviluppati da aziende italiane! Affidiamoci anche professionisti e non solo al buon senso.

Giacomo RICCIARDIELLO
Ermes Cyber Security

ProTECHt migrants
Il progetto di ricerca di Hermes Center for Transparency and Digital Human Rights.

POLITECNICO – CON L'INAPP

Industria 4.0 una ricerca su come cambiano gli investimenti

Nonostante l'enfasi dei Piani governativi per sostenere gli investimenti nelle tecnologie e nelle competenze di Industria 4.0, le modalità con cui queste tecnologie stanno cambiando i modelli operativi e di gestione delle risorse umane delle imprese sono stati finora studiate in modo parziale e non sistemico.
Per ovviare a questa difficoltà, il Politecnico di Torino e l'Istituto Nazionale per l'Analisi delle Politiche pubbliche (Inapp) hanno condotto un programma di ricerca che ha combinato analisi quantitative sviluppate su dati relativi agli investimenti aziendali in Industria 4.0 - raccolti dall'Inapp attraverso l'indagine campionaria Rilevazione longitudinale Imprese e Lavoro (Ril) - oltre che casi di studio e focus group condotti sul territorio nazionale da un team

di ricerca del Politecnico di Torino che ha coinvolto nelle analisi più di 150 tra manager, formatori e altri testimoni privilegiati. In questo team sono stati coinvolti il Dipartimento di Ingegneria Gestionale e della Produzione e il Dipartimento Interateneo di Scienze, Progetto e Politiche per il Territorio dell'Ateneo.
«Si tratta di risultati molto originali che permettono una lettura nuova del fenomeno rispetto a quella che emerge dalle analisi presenti in letteratura su aziende diverse da quelle italiane per via di essere localizzate in altri Paesi o di essere 'native digitali'», ha affermato Paolo Neirotti, docente del Politecnico e uno dei responsabili scientifici del progetto.
E aggiunge: «questi risultati ci hanno permesso di delineare molte conclusioni sul cambiamento specifico prodotto da questa rivoluzione tecnologica su compiti e competenze di manager, professionals, ruoli operativi, oltre che sulle modalità con cui università e gli altri attori delle filiere di istruzione e formazione devono adattare la propria offerta formativa per permettere di ridurre gli inevitabili skills mismatch generatisi in questa fase di transizione epocale».