Il decalogo della sicurezza

1
SCEGLI CON CURA
Password sicura
Il primo passo è quello di adottare password alfanumeriche complesse. Quelle semplificate possono compromettere la sicurezza dei tuoi dispositivi informatici.

2
CUSTODISCI GELOSAMENTE
Rischio truffe
Password e codici di accesso non vanno condivisi con nessuno. Ricordati che corri il rischio di diventare vittima di truffe online o di hackeraggio a causa di una banale distrazione.

3
PENSA PRIMA, CONDIVIDI POI
Consapevolezza
Prenditi il tuo tempo: prima di rilanciare un contenuto, prima di mettere un like o un cuore, prima di pubblicare un selfie o postare un video rifletti bene e poniti una domanda: ne vale davvero la pena?

4
FAI ATTENZIONE
Tutto è pubblico
Ricorda che in rete e sui social tutto è pubblico, anche quello che può sembrare privato. Perchè i contenuti online hanno una viralità difficilmente prevedibile. Quindi stai attento a ciò che decidi di condividere.

5
USA LA TESTA, NON LA PANCIA
Le parole hanno un peso
Non rispondere in modo impulsivo. Parla, scrivi, chatta, ma con consapevolezza. Le parole hanno un peso. Scegli di interagire in modo tale da evitare di alimentare tutto questo.

6
NON CADERE NELLA RETE
Rischio fake news
Perché in rete le fake news si moltiplicano su siti poco affidabili, presentati con video coinvolgenti e con titoli acchiappaclic, rilanciati spesso inconsapevolmente da profili di amici e conoscenti.

7
AIUTA CHI È PIÙ IN DIFFICOLTÀ A COMPRENDERE SOCIAL E RETE
Influencer di buone pratiche
Diventa anche tu un influencer delle buone pratiche e spiega a tua mamma o a tuo papà , ai tuoi nonni e agli amici le opportunità di Internet, ma anche i rischi connessi.

8
NON FIDARTI!
Occhio anche ai contatti stretti
I tentativi di phishing e di truffe cibernetiche vengono talvolta messi a segno attraverso account di amici e parenti, spesso hackerati. Quindi anche i tuoi contatti più stretti, senza volerlo, diventano diffusori di malware. Fidarsi è bene, non fidarsi è meglio.

9
ALZA LA MANO, MAI LE MANI
Si può chiedere aiuto
Chiedi aiuto a chi ne sa più di te se pensi di trovarti in una situazione di rischio a causa delle interazioni in rete. Hai a disposizione un indirizzo sempre presidiato: vai su Commissariatodips.it e mettiti in contatto con gli operatori della Polizia Postale e delle Comunicazioni.

10
TIENITI AGGIORNATO SUI RISCHI CHE SI CORRONO QUANDO SI NAVIGA.
Impara a essere prudente
Cerca di cogliere i segnali che arrivano dagli esperti e impara ad essere prudente, a non fidarti ciecamente dei link condivisi e a ragionare prima di cliccare.

«Pensaci prima di cliccare»: la sicurezza parte da noi

Cybersecurity. Il digitale pervasivo obbliga le persone a una consapevolezza maggiore nei comportamenti, a partire dai piccoli gesti. Ma serve una formazione che parta a scuola

Pagina a cura di
Giampaolo Colletti

«La sicurezza informatica è un argomento che andrebbe trattato in tutte le famiglie durante il pranzo della domenica. Bisogna incentivare una narrazione che coinvolga tutti, nessuno escluso». Non usa mezzi termini Jen Easterly, da luglio 2021 direttrice dell'Agenzia per la sicurezza informatica negli Stati Uniti. Pochi giorni fa a Seattle, dopo la visita agli headquarter di colossi del calibro di Amazon e Boeing, ha deciso di visitare scuole, mercati, centri di aggregazione. Obiettivo: rafforzare la collaborazione pubblico-privato e aumentare la consapevolezza sulla sicurezza informatica. La sua missione è abbattere il linguaggio da nerd che avvolge questo mondo spesso così tecnico e promuovere il *cyber-storytelling*. Questa declinazione è stata coniata da Chirag Joshi e implica un racconto divulgativo chiaro, accessibile, empatico. «D'altronde cosa hanno in comune tecniche di *storytelling* efficaci con gli attacchi informatici? In fondo la creazione di una storia avvincente influisce sulla sicurezza informatica perché la narrazione ispira azioni e comportamenti chiave che influenzano i risultati nella nostra vita personale e professionale», ha detto Joshi. Intanto in Svezia una campagna della Swedish Internet Foundation ha dichiarato guerra alle password deboli e con banali sequenze alfanumeriche. Tutto nasce da una ricerca che ha evidenziato come la password più diffusa nel nord-Europa sia "123456".

> **Tecnologie e machine learning non bastano: ancora oggi l'81% delle violazioni è dovuto a errori umani**

«Avere cura di proteggere i dati personali è fondamentale. Soltanto qualche anno fa pensavamo che bastasse mettere in sicurezza il computer per difendere i nostri dati e la nostra privacy. L'internet onnipresente ci espone a nuovi pericoli ed è terreno fertile per il *cybercrime*, ma anche per attacchi terroristici e *cyberwar*. Come cittadini e utilizzatori di dispositivi e servizi digitali dobbiamo applicare un minimo di cyber igiene, ovvero una serie di regole di base nel mondo digitale simili a quelle che da secoli usiamo nel mondo fisico quando ci proteggiamo da infezioni e malattie», afferma Fabio Martinelli, dirigente del Cnr per le attività in cybersecurity e coordinatore del Cybersecurity Lab. Per Martinelli la protezione passa da gesti semplici, eppure spesso trascurati. Conoscere per prevenire è il motto dell'Osservatorio sulla sicurezza. E questa consapevolezza è anche nel *claim* del decimo mese europeo della sicurezza informatica: «Pensaci, prima di cliccare», accompagnato dall'*hashtag* #ThinkB4UClick.

«La partita si giocherà sempre più partendo dalle scuole e arrivando al mondo del lavoro. L'alfabetizzazione digitale deve essere una costante nel sistema scolastico, e con essa le basi della sicurezza informatica. Come Iit-Cnr da anni promuoviamo la cultura della sicurezza informatica. Per quanto riguarda le industrie, le grandi hanno ormai una serie di risorse umane, competenze e strumenti specifici. Per le piccole ancora si deve accrescere la consapevolezza, e per questo esistono strumenti di *self-assessment* della propria postura di sicurezza che possono dare una prima fotografia ed indicazione del proprio stato. Da qui si passa poi alla protezione dei propri asset informatici o con strutture interne o utilizzando servizi di terzi, incluso anche i vantaggi offerti dalle soluzioni cloud dove la sicurezza è nativa e gestita da esperti», precisa Martinelli. Entro il 2025 il 40% dei board Fortune 500 avrà una figura dedicata di cybersecurity. Si amplia così il perimetro professionale in un settore in trasformazione.

Tecnologie evolute e *machine learning* sono già schierate, ma c'è la componente umana a fare la differenza, nel bene e nel male. Perché ancora oggi l'81% delle violazioni sono dovute ad errori umani. «Prima della tecnologia si tratta di un problema di comportamenti da migliorare. Le persone sono l'anello debole, come tutte le statistiche riconoscono. La tecnologia ci può aiutare a definire meglio come comportarci, a capire quando facciamo qualcosa di sbagliato, oppure quando ci muoviamo in maniera non congrua. Viviamo in un mondo di dispositivi digitali pieni di sensori che raccolgono informazioni su di noi. Ecco perché sono importanti le regolamentazioni europee. Dobbiamo usare nei dispositivi strumenti antivirus aggiornati, evitare di rispondere in maniera sconsiderata a mail e messaggi di sconosciuti o da contatti conosciuti ma che ci appaiono inusuali e sospette. E poi non dobbiamo dare le nostre informazioni private o sensibili a terzi, proteggendo le chiavi di accesso al mondo digitale come facciamo con quelle nel mondo fisico». In fondo bisogna metterci la testa. Lo ripete spesso anche Tim Cook: «Se ancora oggi continui a mettere la tua chiave di casa sotto lo zerbino, sappi che anche un ladro può trovarla».

(Si veda altro articolo a pag.8)

UN MANIFESTO PER TUTTI

Per studenti (ma non solo)
Il digitale è fondamentale per lavorare, formarsi, divertirsi. È un abilitatore di opportunità, ma presenta rischi sempre più evidenti che occorre imparare a individuare e a gestire con consapevolezza. Così l'acquisizione di competenze digitali passa anche dagli elementi legati alla cybersecurity. Lo racconta il manifesto "Ma siamo sicuri? A scuola di cybersecurity", decalogo dedicato alle studentesse e agli studenti italiani e promosso dalla Ludoteca di Registro.it (qui sopra nell'immagine). Il manifesto, lanciato a maggio, ha visto il contributo di Matteo Flora, Alessandro Bencivenni, Mirta Michilli, Matteo Uggeri, Barbara Strappato, Guido Scorza, Nicola Palmieri, Fabiana Andreani, Elia Bombardelli, Sandro Marenco e Andrea Plazzi. «Sono più di dieci anni che con la Ludoteca facciamo laboratori nelle scuole e ci siamo resi conto che ci sono argomenti su cui è necessario insistere. Abbiamo pensato di raccoglierli in uno schema di dieci punti, che diventerà uno strumento di riflessione negli incontri con i ragazzi e speriamo utile anche per gli adulti», afferma Anna Vaccarelli, dirigente dell'Istituto di informatica e telematica del Cnr di Pisa.

> PROCESSO
> **Da strumenti di self-assessment si passa alla protezione degli asset informativi e alla tutela del cloud**

STORIE

ERMES

Difesa fondata sull'architettura diffusa

Affrontare le sfide della sicurezza informatica con un'intuizione rivelatasi nel tempo vincente. Quella di spostare a livello di rete il paradigma di protezione da un approccio centralizzato ad uno distribuito: è quello che fa Ermes, start up nata nel 2017 da attività di ricerca del Politecnico di Torino e supportata dall'incubatore I3P, che oggi offre soluzioni B2B per proteggere in tempo reale la navigazione dei dipendenti aziendali, riducendo la finestra di esposizione alle minacce. Tutto nasce da un'idea di Hassan Metwalley, Stefano Traverso e Marco Mellia, esperti di web security e ricercatori di intelligenza artificiale. La loro impresa fornisce protezione alle aziende grazie ad algoritmi proprietari brevettati, riducendo l'esposizione agli attacchi del 99% rispetto alle principali soluzioni presenti sul mercato. Pochi giorni fa la tecnologia anti-hacker – una delle più promettenti nel campo dell'Ai – si è aggiudicata la nuova edizione dell'Italian Master Startup Award (Imsa), promossa dall'Associazione italiana degli incubatori universitari PNICube e organizzata in collaborazione con l'incubatore del Politecnico di Torino I3P. Ermes, che possiede oltre dieci metodologie proprietarie di Ai ed è in grado di analizzare più di dieci milioni di siti web ogni giorno, è stata selezionata anche da Gartner e inserita nella top 100 mondiale della cybersecurity.

CYBERANGELS

Manager e Pmi protetti via gamification

La sana ossessione dei fondatori è racchiusa in un'azione scontata eppure difficile da perseguire: semplificare la sicurezza informatica. Cyberangels, start up milanese fondata nel 2021 e dedicata alla cybersecurity per Pmi, ha realizzato una soluzione che strizza l'occhio alla *gamification*. Così attraverso dinamiche di gioco si aiutano professionisti e manager a ridurre fino al 90% il rischio cyber. La start up è nata all'interno dell'incubatore insurtech di Vittoria Assicurazioni. «Lì abbiamo capito che il business model per Pmi deve prevedere un meccanismo di ripristino. Queste realtà vivono quotidianamente sfide sempre più grandi col digitale. I vantaggi nell'abbracciare i nuovi sistemi tecnologici sono enormi, ma bisogna tener conto anche delle vulnerabilità legate alla tutela delle password, dei dati sensibili, della tutela dei clienti. Abbiamo voluto creare un sistema affidabile ed economicamente sostenibile per scongiurare in maniera definitiva i *cyber risk*», afferma Andrea Toponi, cofounder e Ceo di Cyberangels. Il primo round di pre-seed nel 2021 ha aperto la strada al consolidamento della prima versione beta del prodotto. Poi la selezione con Cdp per il programma CyberX e a oggi il rilascio della prima versione a pagamento per microimprese.

EXEIN

Una soluzione per ogni oggetto connesso

Sono scesi in campo per proteggere l'oggetto connesso, che è sempre più diffuso tra aziende e privati e presenta però sempre più elementi di vulnerabilità. L'intuizione iniziale di Exein, start up romana oggi presente con una propria filiale anche a San Francisco, è di Gianni Cuozzo, nato in Germania nel 1990, volto noto del mondo digitale, un passato come membro di un noto collettivo hacker tedesco. «Siamo l'unica realtà in Italia e tra le pochissime nel mondo a sviluppare soluzioni di sicurezza che vanno ad agire in tempo reale direttamente sul dispositivo legato all'Internet of Things: ogni oggetto connesso debba essere protetto con un sistema specifico. Le nostre soluzioni hanno una base pubblica attraverso codice *open source*, anche perché crediamo molto nella trasparenza. Poi andiamo a implementare una serie di algoritmi proprietari che proponiamo col pacchetto aziendale», afferma Gerardo Gagliardo, Cfo di Exein, un passato in Ferrari e da tre anni parte di questa squadra composta da venti persone divise tra Italia, Stati Uniti e vari Paesi al mondo. La società ha fatto un primo round da 2 milioni di euro e poi è arrivato nell'agosto 2021 un round da 6 milioni, soprattutto con investitori esteri. Oggi nel portafoglio conta una decina di grandi aziende.