Con i dati tutti a rischio, non importa quanto “piccoli”

Maria Cattini | 15/11/2022 | Di tutto di più

Con i dati tutti a rischio. Probabilmente non ci avete mai fatto caso, ma il tesoro di informazioni che conserviamo nel dispositivo trasforma anche noi in bersagli molto allettanti per i criminali informatici, intenti a sottrarre credenziali di accesso, dati bancari o a iniettare qualche virus nel terminale che li custodisce. Poco conta quale dispositivo utilizziamo per accedere, se usiamo Internet per svago o per lavoro, se facciamo acquisti online o guardiamo film in streaming: chiunque svolga attività online può essere a rischio. Quello che importa sono i nostri dati e, pur di ottenerli, i criminali informatici sfrutteranno qualsiasi vulnerabilità umana e di sicurezza dei nostri dispositivi.

Siamo tutti a rischio, non importa quanto “piccoli” possiamo essere.

Tre notizie provenienti rispettivamente dalla Cina, dagli Stati Uniti e dall’Europa confermano che i nostri dati digitali personali costituiscono un tema importante del ventunesimo secolo, e che faremmo bene a preoccuparcene un po’ di più. I dati personali di un miliardo di cinesi – identità, coordinate e fedina penale – sarebbero stati prelevati dal sito della polizia di Shanghai. Potrebbe trattarsi della più grande operazione di pirateria informatica della storia. I dati sono in vendita, tra l’altro a un prezzo stracciato. Gli hacker, infatti, chiedono 10 bitcoin (la moneta digitale che garantisce l’anonimato), ovvero appena 200mila euro. La Cina ha imposto la censura di qualsiasi commento sulla vicenda, segno di imbarazzo e nervosismo.

Negli Stati Uniti, Google ha annunciato l’intenzione di eliminare qualsiasi tracciabilità delle visite delle donne alle cliniche per l’aborto. La mossa è chiaramente legata alla recente decisione della corte suprema e al bando dell’aborto in diversi stati del paese. I più fanatici vorrebbero infatti perseguire le donne che si sottoporranno a un’interruzione di gravidanza in un altro stato. In questo caso i dati personali potrebbero essere utilizzati come prova in un tribunale.

Oggi scopriamo, o riscopriamo, fino a che punto lasciamo le nostre tracce in tutte le interazioni digitali, spesso senza saperlo. La società della sorveglianza sul modello cinese, ovvero la centralizzazione dei dati raccolti, non esiste ancora nelle società democratiche, ma gli strumenti che impediscono questa deriva sono fragili e potrebbero scomparire. La decisione di Google è dunque encomiabile, ma solleva un interrogativo a proposito di tutti i dati raccolti dal gigante americano.

In Europa il 5 luglio scorso il parlamento europeo ha adottato il Digital services act (Dsa), in discussione da mesi. Il Dsa corrisponde a quella che potremmo definire “una visione europea” della regolamentazione delle piattaforme digitali, più severa e allineata sulle regole del mondo reale.

La posta in gioco è alta, anche se il cittadino digitale non sempre si sente coinvolto. Al centro di tutto ci sono né più né meno che le nostre libertà davanti a tecnologie che per loro natura sono duali, al contempo ludiche e minacciose.

Sentiamo spesso parlare di violazioni di dati, ma quello che non sentiamo è cosa viene fatto con le informazioni personali rubate. La verità è che la sottrazione dei dati è solo il primo elemento della catena di un business molto redditizio, in cui tutte le informazioni sottratte vengono sfruttate. A volte è solo questione di tempo prima che il furto venga a galla. Essere coinvolti in una fuga di dati finiti nelle mani di criminali può comportare conseguenze anche nel lungo periodo:

1. **Vendita dei dati rubati**: un modo in cui gli hacker traggono profitto dai dati rubati è venderli in massa ad altri criminali sul dark web. Queste collezioni possono includere milioni di record di dati rubati, che vengono successivamente utilizzati per altre finalità losche.
2. **Furto d’identità**: i dati sono utilizzati per ottenere benefici a spese della vittima, come ad esempio usando i dettagli della sua carta di credito per effettuare acquisti.
3. **Furto degli account personali**: le credenziali di accesso rubate sono utilizzate dai criminali per introdursi negli account con i dettagli di pagamento, come quelli dei negozi online. Se la password è stata utilizzata anche per accedere ad altri account, i danni sono ancora più gravi.
4. **Attacchi di phishing**: con le informazioni personali rubate i criminali possono colpire le vittime con attacchi di phishing ancora più mirati e indurle a concedere volontariamente dati più importanti come quelli bancari o credenziali di accesso.
5. **Attacchi alle aziende**: le informazioni sottratte possono essere usate per danneggiare le aziende per cui le vittime lavorano. I criminali possono anche cercare di accedere alla rete aziendale per metterla fuori uso o sottrarre i dati sensibili dei clienti.