DIGITAL METRICS
LEAD YOUR MARKETING AHEAD

Il punto sulla Privacy

Approfondimenti e novità in tema privacy che più ci hanno interessato in questi ultimi mesi

WhatsApp: I numeri di 300 mila utenti finiscono su Google

Nuovi problemi di privacy per WhatsApp: come riportano da Threatpost, su Google sono presenti oltre 300 mila numeri di telefono di utenti che provengono dalla nota applicazione di messaggistica istantanea.
Già a febbraio WhatsApp aveva apportato alcuni correttivi per un problema analogo che consentiva a chiunque di trovare su Google i link per entrare a far parte di una chat di gruppo.
Il problema è nuovamente legato all'indicizzazione dei contenuti su Google.
La causa è da ricercare nella funzionalità «Click to Chat», uno strumento utilizzato su numerosi siti web che consente ad aziende e utenti di comunicare direttamente, tramite WhatsApp.
Quando viene attivata questa funzionalità sul sito web, i metadati delle comunicazioni vengono però indicizzati da Google. E all'interno dei metadati è presente anche il numero di telefono dell'utente. La URL incriminata si conosce: https://wa.me./numeroditelefono.
I problemi di privacy sono evidenti: una volta ottenuto il contatto telefonico, il rischio concreto è di divenire vittime di spam, tentativi di phishing e frodi. Non solo, perché un hacker che riuscisse ad entrare in possesso del numero di telefono, potrebbe carpire anche le immagini del profilo, stato e le altre informazioni di profilo presenti su WhatsApp.
Non è ancora chiaro come e se interverrà la nota applicazione, che al momento ha semplicemente dichiarato che quanto segnalato non è un errore…

Automobili e privacy: il rischio se non si cancellano i nostri dati

Le autovetture sono sempre più smart e secondo le previsioni di mercato entro il 2026 tutti i nuovi veicoli saranno connessi. Potremo utilizzare tecnologie bluetooth e applicazioni per scambiare dati con le nostre auto, riversando dati e informazioni personali.

In UK è stato condotto un interessante sondaggio dall'associazione consumatori «Which?», per verificare se gli automobilisti, prima di vendere la loro smart car, avessero eseguito la cancellazione dei dati memorizzati sulla vettura.

Ebbene, l'80% non lo ha fatto, consegnando al nuovo acquirente la propria auto con una miniera di dati personali ancora memorizzati.

Le informazioni che si rischia di trasmettere con tanta leggerezza non sono di poco conto: rubrica telefonica, conversazioni e messaggi, indirizzi e posizioni Gps.

Tutti dati che, se prima di vendere la propria smart car non si procedere alla corretta disconnessione del proprio account e rimozione delle informazioni memorizzate, di fatto consegnati al successivo proprietario dell'auto.

Questi veicoli moderni sono oramai dotati di sistemi operativi, connessioni web, hard disk con memoria che arriva fino ai 25 gigabyte.

Dovremo abituarci a trattarli come tutti gli altri dispositivi elettronici, al pari quindi di pc, smartphone, tablet &co.

Immuni: le preoccupazioni degli esperti Privacy

A volte dobbiamo constatare che «la Privacy è come la democrazia, un mito».

E il Covid-19 ha dimostrato che in alcune circostanze, che ci hanno abituato a definire straordinarie, allora il nostro diritto alla privacy deve essere messo da parte in favore di altri diritti superiori.

È stata condotta una indagine che ha coinvolto oltre 85 professionisti del settore, tra DPO e consulenti legali/professionisti. Nonostante i tentativi di rassicurarci sull'utilizzo dei nostri dati, massiccio in questo periodo di pandemia, gli esperti rinnovano le elevatissime preoccupazioni sui rischi connessi all'utilizzo e raccolta di questi dati.

La gran parte degli esperti ravvisa in particolare due nuovi rischi connessi alle applicazioni di tracking come Immuni:

1. La possibilità che questi dati raccolti finiscano all'estero, senza adeguate tutele (il 63% degli esperti);
2. L'elevata probabilità che questi dati verranno alla fine impiegati da aziende private per scopi non del tutto chiari e ravvisabili ancora (il 58% degli esperti).

Il tutto fermo restando il rischio più grande di tutti, ovvero quello legato al fatto che a trattare e conservare tali dati sarebbe il sistema sanitario pubblico, che a livello di sicurezza informatica non è affatto affidabile.

In definitiva gli esperti ribadiscono che i rischi ci sono ancora, eccome. Opinione diffusa è che mancano ancora sufficienti garanzie e strumenti a tutela della protezione dei dati personali dei cittadini.

Fase 2: largo uso dei Termoscanner, nel rispetto della privacy

Non solo il controllo della temperatura corporea ai dipendenti in ingresso a lavoro. Con il Dpcm del 26 Aprile 2020 è stato esteso l'obbligo di verificare la temperatura anche negli aeroporti, stazioni, centri commerciali e negozi.

A molti potrà sembrare un'intromissione nella loro privacy ed in parte lo è. Non possiamo parlare effettivamente di privacy fin tanto che ci si limita alla misurazione (anonima) della nostra sola temperatura corporea.

Diverso il caso in cui invece ci siano anche delle telecamere che riprendono gli ingressi. In questi casi si dovranno seguire tutte le accortezze già note relative all'informativa per poter effettuare le riprese.

In generale, anche se le informazioni non verranno raccolte ma solo elaborate (come per la mera rilevazione della temperatura), le aziende saranno comunque tenute la rispetto delle prescrizioni che il GDPR impone. Soprattutto perché, non dimentichiamolo, trattasi di dati sulla salute (quali la temperatura corporea) che rientrano nelle «categorie particolari» elencate all'art. 9 del Regolamento.

Quindi il Titolare del Trattamento Dati, ovvero l'azienda, sarà comunque tenuta ad effettuare una valutazione d'impatto in conformità all'art. 35 del GDPR, nonché redigere una serie di documenti e registri nel rispetto dei principi della privacy by-design e by-default.

L'impiego di Termoscanner è certamente funzionale alla sicurezza sanitaria. Cerchiamo di far sì che non si debba di contro rinunciare alla sicurezza però dei dati.

Lezioni e videoconferenze: come vengono trattati i nostri dati?

Sono numerosissime le piattaforme a disposizione per seguire lezioni e corsi online, così come videoconferenze di lavoro. Ma quali sono effettivamente i dati che vengono trattati? E come vengono trattati? Come spiega il Sole24Ore in un articolo, queste piattaforme accedono anche alle nostre registrazioni audio e video. Dati ulteriori quindi che possono essere incrociati e impiegati per attività di profilazione ancora più spinta.

Talvolta i dati che vengono raccolti e trattati sono funzionali e necessari all'erogazione dei servizi. Quindi in mancanza del consenso al trattamento i provider non possono effettivamente garantire le funzionalità richieste. Altre volte invece i dati sono invece facoltativi, non necessari per l'erogazione dei servizi e il mancato consenso al trattamento non dovrebbe incidere sulle funzionalità.

È sempre necessario leggere con cura l'Informativa Privacy.

Oltre ai dati raccolti e trattati, queste piattaforme presentano serie criticità legate alla sicurezza. La piattaforma Zoom è stata oggetto di vari cyber attacchi negli ultimi mesi, soprattutto incidenti legati all'intrusione di hacker durante videoconferenze e lezioni online.

Due consigli in generale per ridurre questi rischi:

1. Prediligere le versioni web di queste piattaforme, piuttosto che utilizzare le versioni Desktop dei software;
2. Utilizzare, ove possibile, password e sistemi che riducano i rischi di accessi non autorizzati.

Da quindici anni Digital Metrics affianca grandi realtà italiane e internazionali della GDO e Industria, per aiutarli ad implementare progetti e strategie di Marketing relazionale e digitale.

Siamo a fianco dei nostri clienti fin dall'inizio, per impostare i progetti e monitorarne lo sviluppo affinché rispondano ai più alti livelli di compliance rispetto ala normativa sulla Privacy e Sicurezza dei dati.

Scopri cosa possiamo fare per te.

www.digitalmetrics.eu

DIGITAL METRICS

LEAD YOUR MARKETING AHEAD