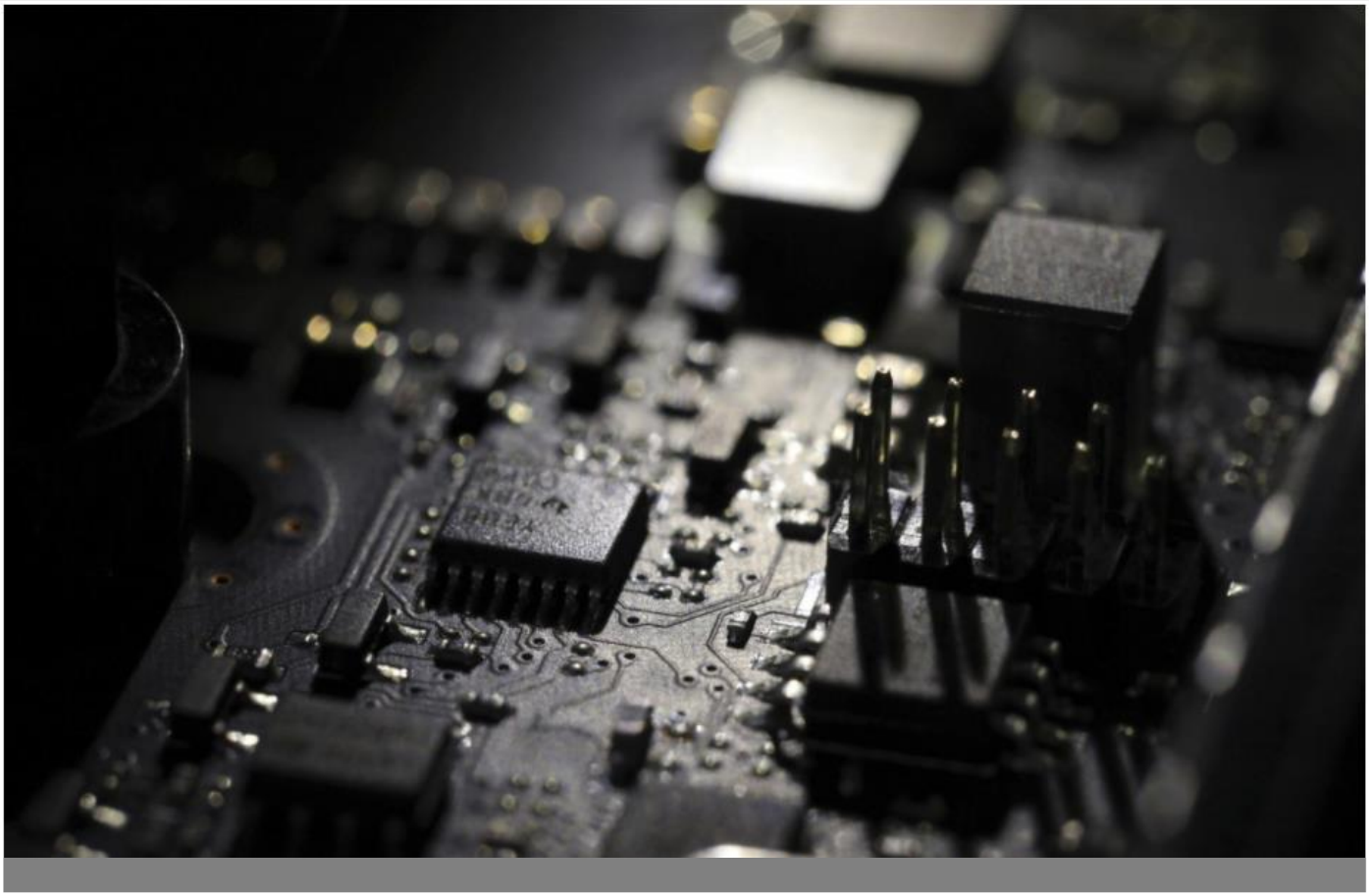
RUBRICHE

Gli italiani navigano senza protezione

Hacker's Dictionary. *Secondo una ricerca Avira il 61% dei datori di lavoro non bada alla protezione informatica nello smartworking. La metà degli italiani è preoccupata da furti e frodi informatiche ma solo il 24% comprerebbe un software per la sicurezza digitale*



L'interno di un computer. © LaPresse

Arturo Di Corinto

EDIZIONE DEL
29.10.2020

PUBBLICATO
28.10.2020, 23:59

Dall'inizio della pandemia oltre la metà degli italiani (53%) ha acquistato un nuovo computer o un nuovo dispositivo tecnologico, ma meno di un terzo (31%) ci ha installato sopra un software di sicurezza. Lo dice **l'ultima ricerca** condotta da Opinion Matter per l'azienda di cybersecurity Avira.

La ricerca, che ha coinvolto 2.000 persone dai 18 anni in su residenti in Italia, Francia, Germania e Stati Uniti, illustra i cambiamenti comportamentali intervenuti durante la pandemia a cominciare dall'introduzione massiccia del così detto smartworking.

Con un effetto collaterale che a tutti apparirà ovvio: il distanziamento sociale ha aumentato il bisogno di interagire e comunicare con gli altri. Secondo la ricerca infatti, durante la pandemia gli italiani hanno utilizzato Pc (78%) e dispositivi mobili (75%) più frequentemente sia per comunicare con gli altri che per il lavoro.

Il 72% degli italiani con messaggi diretti via smartphone e il 70% per ricevere notizie e informazioni. In particolare le generazioni più anziane si sono viste costrette a imparare l'uso delle tecnologie moderne come mezzo di comunicazione con i propri cari.

In vista di nuove ondate della pandemia, gli italiani attribuiscono la priorità all'acquisto di articoli tecnologici mirati a migliorare l'organizzazione dell'ecosistema domestico: il 32% acquisterebbe un nuovo computer ma solo il 24% prende in considerazione la possibilità di acquistare un software di sicurezza digitale e protezione dei dati in previsione di futuri lockdown o di situazioni di smart working e didattica a distanza.

Ma, e qui viene il bello, quasi la metà degli intervistati (45%) ha ammesso di essere molto o abbastanza preoccupato per i rischi legati alle minacce informatiche durante il lavoro da casa, affermando che ben il 61% dei datori di lavoro non avrebbe fornito ai suoi impiegati strumenti per proteggerne le attività, nonostante l'alto rischio di furto di informazioni riservate e di violazione dei dati.

Ma quali sono queste minacce? Le ha elencate per bene Ermes, azienda torinese che usa l'intelligenza artificiale per un avanzato sistema di protezione contro il phishing (la pesca) di credenziali. Ne citiamo alcune relative alla sola navigazione web.

Furto d'identità: si realizza a partire dalle informazioni su dipendenti e i loro dispositivi tracciate e archiviate su sistemi esterni all'azienda mettendo a rischio privacy professionale e sicurezza aziendale.

Keylogging: i siti possono "registrare" qualsiasi azione eseguita sulle pagine visitate, come clic e sequenze di tasti. I dati raccolti contengono anche credenziali e numeri di carta di credito.

Tabnabbing: furto delle credenziali di accesso attraverso false tab o finestre web simili a quelle dei siti più comuni come Facebook e Gmail in cui l'utente immette senza saperlo username e password.

Raccolta fraudolenta dei dati: in seguito alla normale navigazione dei dipendenti, cronologie web, tracce di clic, contatti e credenziali forniti nei moduli possono essere rubati e utilizzati per scopi dannosi.

Spionaggio digitale: I profili creati dagli elementi traccianti della pagina possono essere ceduti a concorrenti o utilizzati per bloccare linee produttive.

Cryptojacking: i siti incorporano script che sfruttano la potenza di calcolo dei nostri dispositivi per estrarre cryptovalute rallentando le prestazioni dei dispositivi fino al 95%.

Senza un aumento della consapevolezza delle minacce alla sicurezza informatica associate al nuovo stile di vita digitale ci aspettiamo una catastrofe digitale. Anche dentro casa.