

Signal blocca AI di Windows: privacy prima di tutto

Redazione | 01/06/2025 | Sicurezza digitale

Una delle app di messaggistica più sicure al mondo ha dichiarato guerra all'intelligenza artificiale di casa Microsoft. [Signal](#), nota per la sua attenzione alla riservatezza delle conversazioni, ha disattivato il sistema Recall nei PC Windows per proteggere la privacy di chi utilizza l'app su desktop.

Ma perché tanto clamore? Perché Recall, una funzione lanciata da Microsoft con Copilot+, memorizza **automaticamente schermate** di ciò che avviene sullo schermo. Inclusi i messaggi criptati. E questo, per chi usa Signal, è un problema serio.

☐☐ Cos'è Recall e perché è così controverso?

Recall è una funzione introdotta da [Windows 11](#) che archivia una vera e propria "memoria visiva" delle attività sullo schermo. In pratica, scatta continuamente screenshot per permettere all'utente di ritrovare in un secondo momento ciò che ha fatto sul computer.

L'intento può sembrare utile. Ma cosa succede se questa memoria include conversazioni private? Documenti riservati? Immagini personali? Il rischio è evidente: si apre una falla nella sicurezza della vita digitale.

☐☐ Come ha risposto Signal?

Signal ha deciso di intervenire con un aggiornamento mirato: **quando l'app è in esecuzione, Recall non può più catturare schermate**. Questo è stato possibile grazie all'utilizzo di un DRM simile a quello impiegato da Netflix per impedire la registrazione di contenuti protetti da copyright. Solo che, in questo caso, **non si tutela il copyright ma la privacy**.

Una protezione integrata

Il blocco è automatico e attivo di default. L'utente può anche disattivarlo, ma Signal lo sconsiglia fortemente. Il motivo? Se il sistema operativo può fare uno screenshot della chat, allora tutta la crittografia end-to-end va in fumo.

☐☐ “Microsoft non ci ha dato scelta”

Nel blog ufficiale, Signal spiega che “nonostante gli aggiornamenti, Recall continua a mettere a rischio qualsiasi contenuto visualizzato, anche su app pensate per la massima privacy”. Non è solo una questione tecnica, ma un paradosso etico: si usano app sicure, ma il sistema operativo salva comunque tutto.

«Microsoft non ci ha dato scelta», affermano seccamente dal team Signal.

⚙ Funziona davvero? E cosa può fare l'utente?

Recall offre opzioni per **escludere alcune app o schede del browser**, ma solo manualmente. Questo significa che l'utente deve sapere cosa disattivare e come farlo. Una barriera che non tutti sono in grado di superare. Signal invece ha scelto la strada opposta: **protezione attiva e automatica**, senza bisogno di configurazioni complicate.

□□ Signal vs AI: cosa c'è in gioco davvero?

Questa scelta non è solo una mossa tecnica. È una dichiarazione di principio.

□□ In un mondo dove l'AI è ovunque e i sistemi operativi diventano sempre più "intelligenti", Signal ribadisce un punto chiave:

la privacy deve restare sotto il controllo dell'utente, non dell'algoritmo.

Lo stesso Joshua Lund, portavoce di Signal, ha dichiarato che è fondamentale garantire agli sviluppatori la possibilità di **escludere completamente le proprie app** dall'accesso da parte dell'intelligenza artificiale integrata nei sistemi operativi.

□ Pro e contro della mossa di Signal

Aspetti positivi

- ✓ Protezione automatica della privacy
- ✓ Nessuna azione richiesta dall'utente
- ✓ Coerenza con la missione dell'app

Aspetti critici

- DRM può limitare alcune funzionalità
- Potenziale conflitto con altri strumenti
- Funzione Recall resta attiva per altre app

Questa presa di posizione di Signal riaccende il dibattito sul rapporto tra **AI e privacy**. Chi ha il controllo? L'utente o il software? Serve una regolamentazione più chiara? E cosa possono fare le altre app per difendere i propri utenti?

Domande che toccano non solo sviluppatori e aziende, ma ognuno di noi.

□□ Cosa puoi fare tu per proteggere i tuoi dati

Ecco tre azioni concrete per chi è attento alla privacy:

1. □□ Aggiorna sempre l'app Signal su desktop alla versione più recente.
2. ⚙️ Controlla le impostazioni di Recall sul tuo PC e valuta di disattivarlo per le app più sensibili.
3. □□ Informati e scegli software che mettono davvero al centro la sicurezza.



La battaglia tra strumenti di protezione e sistemi di tracciamento è sempre più complessa. La mossa di Signal ci ricorda una cosa semplice ma essenziale: **la tecnologia deve adattarsi all'essere umano, non il contrario.**

□□ Hai mai usato Signal su desktop? Ti sei accorto di questa nuova protezione? Raccontacelo nei commenti o condividi la tua esperienza nel nostro gruppo Telegram.

Una delle app di messaggistica più sicure al mondo ha dichiarato guerra all'intelligenza artificiale di casa Microsoft. [Signal](#), nota per la sua attenzione alla riservatezza delle conversazioni, ha disattivato il sistema Recall nei PC Windows per proteggere la privacy di chi utilizza l'app su desktop.

Ma perché tanto clamore? Perché Recall, una funzione lanciata da Microsoft con Copilot+, memorizza **automaticamente schermate** di ciò che avviene sullo schermo. Inclusi i messaggi criptati. E questo, per chi usa Signal, è un problema serio.

□□ Cos'è Recall e perché è così controverso?

Recall è una funzione introdotta da [Windows 11](#) che archivia una vera e propria "memoria visiva"

delle attività sullo schermo. In pratica, scatta continuamente screenshot per permettere all'utente di ritrovare in un secondo momento ciò che ha fatto sul computer.

L'intento può sembrare utile. Ma cosa succede se questa memoria include conversazioni private? Documenti riservati? Immagini personali? Il rischio è evidente: si apre una falla nella sicurezza della vita digitale.

🔍 Come ha risposto Signal?

Signal ha deciso di intervenire con un aggiornamento mirato: **quando l'app è in esecuzione, Recall non può più catturare schermate**. Questo è stato possibile grazie all'utilizzo di un DRM simile a quello impiegato da Netflix per impedire la registrazione di contenuti protetti da copyright. Solo che, in questo caso, **non si tutela il copyright ma la privacy**.

Una protezione integrata

Il blocco è automatico e attivo di default. L'utente può anche disattivarlo, ma Signal lo sconsiglia fortemente. Il motivo? Se il sistema operativo può fare uno screenshot della chat, allora tutta la crittografia end-to-end va in fumo.

🔍 “Microsoft non ci ha dato scelta”

Nel blog ufficiale, Signal spiega che “nonostante gli aggiornamenti, Recall continua a mettere a rischio qualsiasi contenuto visualizzato, anche su app pensate per la massima privacy”. Non è solo una questione tecnica, ma un paradosso etico: si usano app sicure, ma il sistema operativo salva comunque tutto.

«Microsoft non ci ha dato scelta», affermano seccamente dal team Signal.

⚙️ Funziona davvero? E cosa può fare l'utente?

Recall offre opzioni per **escludere alcune app o schede del browser**, ma solo manualmente. Questo significa che l'utente deve sapere cosa disattivare e come farlo. Una barriera che non tutti sono in grado di superare. Signal invece ha scelto la strada opposta: **protezione attiva e automatica**, senza bisogno di configurazioni complicate.

🔍 Signal vs AI: cosa c'è in gioco davvero?

Questa scelta non è solo una mossa tecnica. È una dichiarazione di principio.

🔍 In un mondo dove l'AI è ovunque e i sistemi operativi diventano sempre più “intelligenti”, Signal ribadisce un punto chiave:

la privacy deve restare sotto il controllo dell'utente, non dell'algoritmo.

Lo stesso Joshua Lund, portavoce di Signal, ha dichiarato che è fondamentale garantire agli sviluppatori la possibilità di **escludere completamente le proprie app** dall'accesso da parte dell'intelligenza artificiale integrata nei sistemi operativi.

🔍 Pro e contro della mossa di Signal

Aspetti positivi

- ✓ Protezione automatica della privacy
- ✓ Nessuna azione richiesta dall'utente
- ✓ Coerenza con la missione dell'app

Aspetti critici

- 🔍 DRM può limitare alcune funzionalità
- 🔍 Potenziale conflitto con altri strumenti
- 🔍 Funzione Recall resta attiva per altre app

Questa presa di posizione di Signal riaccende il dibattito sul rapporto tra **AI e privacy**. Chi ha il controllo? L'utente o il software? Serve una regolamentazione più chiara? E cosa possono fare le altre app per difendere i propri utenti?

Domande che toccano non solo sviluppatori e aziende, ma ognuno di noi.

🔒 Cosa puoi fare tu per proteggere i tuoi dati

Ecco tre azioni concrete per chi è attento alla privacy:

1. 🔒 Aggiorna sempre l'app Signal su desktop alla versione più recente.
2. ⚙️ Controlla le impostazioni di Recall sul tuo PC e valuta di disattivarlo per le app più sensibili.
3. 🔒 Informati e scegli software che mettono davvero al centro la sicurezza.



La battaglia tra strumenti di protezione e sistemi di tracciamento è sempre più complessa. La mossa di Signal ci ricorda una cosa semplice ma essenziale: **la tecnologia deve adattarsi all'essere umano, non il contrario.**

🔒 Hai mai usato Signal su desktop? Ti sei accorto di questa nuova protezione? Raccontacelo nei commenti o condividi la tua esperienza nel nostro gruppo Telegram.