AirDrop espone i dati dell'iPhone: come proteggersi

Maria Cattini | 13/05/2025 | Risorse

□□ AirDrop a rischio: cosa sappiamo oggi sulla vulnerabilità che espone i tuoi dati

□□ Un sistema comodo, ma (ancora) non sicuro

AirDrop è una delle funzioni più amate dagli utenti Apple. Bastano pochi tocchi per inviare foto, file e link a un altro iPhone o Mac nelle vicinanze, senza bisogno di connessioni complicate. Ma dietro la sua apparente semplicità si nasconde un problema mai risolto del tutto.

Secondo gli esperti del *Technische Universität Darmstadt*, **la funzione di scoperta dei dispositivi AirDrop resta esposta a un tipo di attacco che permette di recuperare dati personali come indirizzi email e numeri di telefono**, semplicemente intercettando il traffico durante la fase di connessione.

E il dettaglio più inquietante? Questo bug è **ancora attuale**.

□□ Come funziona (e perché è pericoloso)

Quando attivi AirDrop, il tuo dispositivo esegue un processo di verifica per capire chi c'è nei dintorni. Se imposti AirDrop su "Solo contatti", il sistema incrocia **il tuo numero di telefono e l'email** con quelli degli altri dispositivi vicini per capire se siete "in rubrica". Questa verifica avviene tramite **hash crittografici**, che dovrebbero essere sicuri.

Il condizionale è d'obbligo.

> I ricercatori tedeschi hanno dimostrato che questi hash possono essere decifrati facilmente tramite attacchi di forza bruta, se l'aggressore ha accesso fisico alla rete (es. Wi-Fi pubblico) e si trova nelle vicinanze.

Significa che **un malintenzionato potrebbe "sniffare" i dati** trasmessi e risalire a email e numero di telefono anche senza essere nei tuoi contatti.

□□ Apple ha risolto il problema?

No. La falla è stata segnalata nel 2019, ma **non risulta ancora una patch ufficiale**. Nonostante le proteste della comunità accademica e diverse segnalazioni da parte di esperti di cybersecurity, **Apple non ha mai commentato pubblicamente né confermato un intervento correttivo definitivo**.

Nel frattempo, **oltre 1,5 miliardi di dispositivi restano potenzialmente esposti**, soprattutto in contesti affollati come aeroporti, scuole, eventi pubblici e coworking.

□□ Come proteggerti: la guida pratica

La buona notizia è che puoi **difenderti da questo tipo di attacco** con pochi gesti.

□ Disattiva AirDrop quando non lo usi

iOS (iPhone e iPad)

Come disattivare AirDrop

1

Apri il Centro di Controllo

Scorri verso il basso dall'angolo superiore destro (iPhone X o più recenti) o verso l'alto dalla parte inferiore dello schermo (iPhone 8 o precedenti).

2

Premi a lungo sul modulo connettività

Tieni premuto a lungo sul riquadro che contiene i controlli di Bluetooth e Wi-Fi per accedere alle opzioni estese.

3

Tocca "AirDrop"

Nel menu esteso che appare, individua e tocca l'opzione "AirDrop" per visualizzare le impostazioni di privacy.

4

Seleziona "Ricezione disattivata"

Tra le opzioni disponibili, scegli "Ricezione disattivata" per impedire a qualsiasi dispositivo di inviarti file tramite AirDrop.

Funziona su tutti i dispositivi iOS con AirDrop supportato (iPhone 5 o più recente)

macOS (Mac)

Come disattivare AirDrop

1

Vai su Finder

Apri il Finder sul tuo Mac facendo clic sull'icona del Finder nella barra Dock (l'icona che sembra un viso sorridente blu) o premendo ⌘+Tab per passare al Finder.

2

Apri AirDrop

Dal menu del Finder, seleziona "Vai" e poi "AirDrop", oppure utilizza la scorciatoia da tastiera ⇧⌘R (Maiusc+Comando+R) per aprire rapidamente AirDrop.

3

Clicca su "Consenti di essere visibile a"

Nella finestra di AirDrop, cerca il menu a discesa in basso che dice "Consenti di essere visibile a". Questo controlla chi può vedere il tuo dispositivo e inviarti file tramite AirDrop.

4

Seleziona "Nessuno"

Dal menu a discesa, seleziona l'opzione "Nessuno". Questo impedirà a qualsiasi dispositivo di vedere il tuo Mac tramite AirDrop, disattivando completamente la funzionalità di ricezione file.

Funziona su Mac con macOS X Yosemite (10.10) o versioni più recenti

⚠ Evita reti Wi-Fi pubbliche non protette

Il rischio aumenta drasticamente quando usi **reti Wi-Fi non cifrate**, come quelle gratuite nei luoghi pubblici. Se devi usarle, **attiva una VPN affidabile**.

□□ Alternative sicure per condividere file

Se devi condividere documenti in modo sicuro:

• iCloud Drive con link privato
• File criptati tramite servizi come ProtonDrive o Tresorit
• WeTransfer con password

Tutti questi sistemi permettono di inviare file in modo più protetto, senza trasmettere i tuoi dati personali in chiaro.

□□ Un vecchio problema che torna attuale

In un’epoca in cui la privacy è sotto pressione costante, episodi come questo ci ricordano che **anche le funzioni più banali possono nascondere insidie**.

Se da un lato Apple ha fatto della sicurezza un punto di forza, dall’altro questa mancata correzione **solleva domande sulla trasparenza e la gestione delle vulnerabilità**.

AirDrop resta comodo, ma finché non verranno introdotti meccanismi più robusti, **conviene usarlo con cautela.**

□□ Hai disattivato AirDrop dopo aver letto questo articolo?

Condividi la tua esperienza e segui il nostro canale per altri aggiornamenti sulla sicurezza digitale quotidiana.
□□ AirDrop a rischio: cosa sappiamo oggi sulla vulnerabilità che espone i tuoi dati

□□ Un sistema comodo, ma (ancora) non sicuro

AirDrop è una delle funzioni più amate dagli utenti Apple. Bastano pochi tocchi per inviare foto, file e link a un altro iPhone o Mac nelle vicinanze, senza bisogno di connessioni complicate. Ma dietro la sua apparente semplicità si nasconde un problema mai risolto del tutto.

Secondo gli esperti del *Technische Universität Darmstadt*, **la funzione di scoperta dei dispositivi AirDrop resta esposta a un tipo di attacco che permette di recuperare dati personali come indirizzi email e numeri di telefono**, semplicemente intercettando il traffico durante la fase di connessione.

E il dettaglio più inquietante? Questo bug è **ancora attuale**.

□□ Come funziona (e perché è pericoloso)

Quando attivi AirDrop, il tuo dispositivo esegue un processo di verifica per capire chi c'è nei dintorni. Se imposti AirDrop su "Solo contatti", il sistema incrocia **il tuo numero di telefono e l'email** con quelli degli altri dispositivi vicini per capire se siete "in rubrica". Questa verifica avviene tramite **hash crittografici**, che dovrebbero essere sicuri.

Il condizionale è d'obbligo.

> I ricercatori tedeschi hanno dimostrato che questi hash possono essere decifrati facilmente tramite attacchi di forza bruta, se l'aggressore ha accesso fisico alla rete (es. Wi-Fi pubblico) e si trova nelle vicinanze.

Significa che **un malintenzionato potrebbe "sniffare" i dati** trasmessi e risalire a email e numero di telefono anche senza essere nei tuoi contatti.

□□ Apple ha risolto il problema?

No. La falla è stata segnalata nel 2019, ma **non risulta ancora una patch ufficiale**. Nonostante le proteste della comunità accademica e diverse segnalazioni da parte di esperti di cybersecurity, **Apple non ha mai commentato pubblicamente né confermato un intervento correttivo definitivo**.

Nel frattempo, **oltre 1,5 miliardi di dispositivi restano potenzialmente esposti**, soprattutto in contesti affollati come aeroporti, scuole, eventi pubblici e coworking.

□□ Come proteggerti: la guida pratica

La buona notizia è che puoi **difenderti da questo tipo di attacco** con pochi gesti.

□ Disattiva AirDrop quando non lo usi

iOS (iPhone e iPad)

Come disattivare AirDrop

1

Apri il Centro di Controllo

Scorri verso il basso dall'angolo superiore destro (iPhone X o più recenti) o verso l'alto dalla parte inferiore dello schermo (iPhone 8 o precedenti).

2

Premi a lungo sul modulo connettività

Tieni premuto a lungo sul riquadro che contiene i controlli di Bluetooth e Wi-Fi per accedere alle opzioni estese.

3

Tocca "AirDrop"

Nel menu esteso che appare, individua e tocca l'opzione "AirDrop" per visualizzare le impostazioni di privacy.

4

Seleziona "Ricezione disattivata"

Tra le opzioni disponibili, scegli "Ricezione disattivata" per impedire a qualsiasi dispositivo di inviarti file tramite AirDrop.

Funziona su tutti i dispositivi iOS con AirDrop supportato (iPhone 5 o più recente)

macOS (Mac)

Come disattivare AirDrop

1

Vai su Finder

Apri il Finder sul tuo Mac facendo clic sull'icona del Finder nella barra Dock (l'icona che sembra un viso sorridente blu) o premendo ⌘+Tab per passare al Finder.

2

Apri AirDrop

Dal menu del Finder, seleziona "Vai" e poi "AirDrop", oppure utilizza la scorciatoia da tastiera ⇧⌘R (Maiusc+Comando+R) per aprire rapidamente AirDrop.

3

Clicca su "Consenti di essere visibile a"

Nella finestra di AirDrop, cerca il menu a discesa in basso che dice "Consenti di essere visibile a". Questo controlla chi può vedere il tuo dispositivo e inviarti file tramite AirDrop.

4

Seleziona "Nessuno"

Dal menu a discesa, seleziona l'opzione "Nessuno". Questo impedirà a qualsiasi dispositivo di vedere il tuo Mac tramite AirDrop, disattivando completamente la funzionalità di ricezione file.

Funziona su Mac con macOS X Yosemite (10.10) o versioni più recenti

⚠ Evita reti Wi-Fi pubbliche non protette

Il rischio aumenta drasticamente quando usi **reti Wi-Fi non cifrate**, come quelle gratuite nei luoghi pubblici. Se devi usarle, **attiva una VPN affidabile**.

□□ Alternative sicure per condividere file

Se devi condividere documenti in modo sicuro:

• iCloud Drive con link privato
• File criptati tramite servizi come ProtonDrive o Tresorit
• WeTransfer con password

Tutti questi sistemi permettono di inviare file in modo più protetto, senza trasmettere i tuoi dati personali in chiaro.

□□ Un vecchio problema che torna attuale

In un’epoca in cui la privacy è sotto pressione costante, episodi come questo ci ricordano che **anche le funzioni più banali possono nascondere insidie**.

Se da un lato Apple ha fatto della sicurezza un punto di forza, dall’altro questa mancata correzione **solleva domande sulla trasparenza e la gestione delle vulnerabilità**.

AirDrop resta comodo, ma finché non verranno introdotti meccanismi più robusti, **conviene usarlo con cautela.**

□□ Hai disattivato AirDrop dopo aver letto questo articolo?

Condividi la tua esperienza e segui il nostro canale per altri aggiornamenti sulla sicurezza digitale quotidiana.