

# LinkedIn per OSINT: come indagare senza farsi notare

Maria Cattini | 04/08/2025 | Open source intelligence

---

LinkedIn per OSINT. [LinkedIn](#) non è solo per cercare lavoro: è un vero paradiso per chi raccoglie informazioni online. Profili personali, annunci, post, badge, certificazioni, strutture aziendali, preferenze linguistiche... tutto pubblico, tutto utile.

Ecco perché investigatori digitali, giornalisti, red teamer e chiunque faccia indagini **Open Source** lo usa regolarmente.

## Sicurezza operativa prima di tutto: non usare il tuo profilo

Prima di iniziare, pensa a come ti muovi:

- Se accedi con il tuo profilo personale, le visite sono visibili al target.
- Meglio attivare la navigazione privata nelle impostazioni di LinkedIn.
- Oppure creare un account sock puppet (finto) solo per le indagini.

⚠ Attenzione però: LinkedIn è **molto bravo a rilevare i profili fake**. Se decidi di crearne uno, fallo bene, con una storia credibile.

## OSINT su aziende: cosa puoi scoprire da un profilo aziendale

I profili aziendali su LinkedIn sono una fonte continua di dati:

### Dove guardare

- Informazioni: descrizione, sede, sito ufficiale
- Post: eventi, annunci, campagne recenti
- Lavori: tecnologie usate, processi interni, esigenze
- Persone: struttura del team, ruoli, background, scuole

### Dati strategici

- Crescita del personale nel tempo
- Turnover elevato = potenziale crisi o riorganizzazione
- Distribuzione per dipartimenti utile per costruire pretesti credibili (es. phishing simulato)

## OSINT su persone: come ottenere più di quanto mostrano

I profili personali nascondono più di quanto sembri, anche quando l'utente crede di tutelarsi.

### Ricostruire un cognome nascosto

- Usa la barra di ricerca di LinkedIn: se inserisci iniziali corrette, il profilo compare; se sbagli,

sparisce.

- Puoi scoprire lettera per lettera un cognome "nascosto".

## Altri modi per identificare una persona

- URL personalizzato: molti utenti lo impostano con nome e cognome.
- Certificati postati: mostrano spesso il nome completo.
- Raccomandazioni ricevute: contengono il nome intero.
- Lingua predefinita: scaricando il profilo in PDF puoi capire in che lingua è stato creato l'account.

## Verifiche e indizi nascosti per LinkedIn per OSINT

### Profili verificati

LinkedIn permette la verifica via:

- Identità (documento)
- Email lavorativa
- Email scolastica

☐☐ Se un utente ha verificato il profilo con una email aziendale, puoi ipotizzare che quella casella riceva notifiche da LinkedIn → utile per costruire pretesti credibili in attività simulate.

### Attenzione alle foto: badge, scrivanie e documenti

Le immagini pubblicate dagli utenti rivelano **molto di più di quanto pensino**:

- Badge con nome, ruolo, layout grafico dell'azienda
- Screenshot di email, stanze, desktop
- Immagini dell'ultimo giorno di lavoro: mostrano ambienti e routine

Ogni dettaglio può essere **replicato** in contesti di ingegneria sociale (anche per simulazioni etiche, come nei test di sicurezza).

## Strumenti esterni per espandere la ricerca

LinkedIn ha limiti di accesso, ma puoi aggirarli usando:

### Google Dorks

Usa operatori avanzati tipo:

```
bashCopiaModificasite:linkedin.com/in/ "nome azienda"
```

oppure:

```
bashCopiaModificasite:linkedin.com/in/ intitle:"cybersecurity" AND "Torino"
```

Ti aiutano a trovare profili anche se non hai un account LinkedIn attivo.

## Wayback Machine

Serve per visualizzare profili o pagine aziendali **modificati o cancellati**:

- Vai su [web.archive.org](http://web.archive.org)
- Incolla l'URL del profilo
- Cerca uno snapshot precedente

Se non conosci l'URL, cerca prima nei siti web aziendali salvati.

## Collegare un'email a un profilo LinkedIn

Se hai un'email valida:

- Aggiungila in Outlook online come contatto
- Se l'integrazione LinkedIn è attiva, potresti vedere il profilo associato

## È tutto legale?

Sì, **se resti nel perimetro pubblico**:

- Non violi la legge se raccogli solo ciò che è accessibile a tutti
- Ma è tua responsabilità usare le informazioni in modo etico e lecito

## In sintesi: cosa puoi fare con LinkedIn e OSINT

- Ricostruire gerarchie aziendali
- Identificare persone e verificare identità
- Raccogliere dettagli su ruoli, progetti, tecnologie
- Analizzare flussi di personale
- Preparare simulazioni, investigazioni e inchieste

☐☐ Ti interessa scoprire come usare l'OSINT per le tue indagini digitali, anche se non sei un esperto?  
Iscriviti alla newsletter "[OSINT & AI per tutti](#)" su Substack o unisciti al nostro gruppo Telegram.

LinkedIn per OSINT. [LinkedIn](#) non è solo per cercare lavoro: è un vero paradiso per chi raccoglie informazioni online. Profili personali, annunci, post, badge, certificazioni, strutture aziendali, preferenze linguistiche... tutto pubblico, tutto utile.

Ecco perché investigatori digitali, giornalisti, red teamer e chiunque faccia indagini **Open Source** lo usa regolarmente.

## Sicurezza operativa prima di tutto: non usare il tuo profilo

Prima di iniziare, pensa a come ti muovi:

- Se accedi con il tuo profilo personale, le visite sono visibili al target.
- Meglio attivare la navigazione privata nelle impostazioni di LinkedIn.
- Oppure creare un account sock puppet (finto) solo per le indagini.

⚠ Attenzione però: LinkedIn è **molto bravo a rilevare i profili fake**. Se decidi di crearne uno, fallo bene, con una storia credibile.

## OSINT su aziende: cosa puoi scoprire da un profilo aziendale

I profili aziendali su LinkedIn sono una fonte continua di dati:

### Dove guardare

- Informazioni: descrizione, sede, sito ufficiale
- Post: eventi, annunci, campagne recenti
- Lavori: tecnologie usate, processi interni, esigenze
- Persone: struttura del team, ruoli, background, scuole

### Dati strategici

- Crescita del personale nel tempo
- Turnover elevato = potenziale crisi o riorganizzazione
- Distribuzione per dipartimenti utile per costruire pretesti credibili (es. phishing simulato)

## OSINT su persone: come ottenere più di quanto mostrano

I profili personali nascondono più di quanto sembri, anche quando l'utente crede di tutelarsi.

### Ricostruire un cognome nascosto

- Usa la barra di ricerca di LinkedIn: se inserisci iniziali corrette, il profilo compare; se sbagli, sparisce.
- Puoi scoprire lettera per lettera un cognome "nascosto".

### Altri modi per identificare una persona

- URL personalizzato: molti utenti lo impostano con nome e cognome.
- Certificati postati: mostrano spesso il nome completo.
- Raccomandazioni ricevute: contengono il nome intero.
- Lingua predefinita: scaricando il profilo in PDF puoi capire in che lingua è stato creato l'account.

## Verifiche e indizi nascosti per LinkedIn per OSINT

### Profili verificati

LinkedIn permette la verifica via:

- Identità (documento)
- Email lavorativa
- Email scolastica

☐☐ Se un utente ha verificato il profilo con una email aziendale, puoi ipotizzare che quella casella riceva notifiche da LinkedIn → utile per costruire pretesti credibili in attività simulate.

### Attenzione alle foto: badge, scrivanie e documenti

Le immagini pubblicate dagli utenti rivelano **molto di più di quanto pensino**:

- Badge con nome, ruolo, layout grafico dell'azienda
- Screenshot di email, stanze, desktop
- Immagini dell'ultimo giorno di lavoro: mostrano ambienti e routine

Ogni dettaglio può essere **replicato** in contesti di ingegneria sociale (anche per simulazioni etiche, come nei test di sicurezza).

## Strumenti esterni per espandere la ricerca

LinkedIn ha limiti di accesso, ma puoi aggirarli usando:

### Google Dorks

Usa operatori avanzati tipo:

```
bashCopiaModificasite:linkedin.com/in/ "nome azienda"
```

oppure:

```
bashCopiaModificasite:linkedin.com/in/ intitle:"cybersecurity" AND "Torino"
```

Ti aiutano a trovare profili anche se non hai un account LinkedIn attivo.

### Wayback Machine

Serve per visualizzare profili o pagine aziendali **modificati o cancellati**:

- Vai su [web.archive.org](http://web.archive.org)
- Incolla l'URL del profilo
- Cerca uno snapshot precedente

Se non conosci l'URL, cerca prima nei siti web aziendali salvati.

### Collegare un'email a un profilo LinkedIn

Se hai un'email valida:

- Aggiungila in Outlook online come contatto
- Se l'integrazione LinkedIn è attiva, potresti vedere il profilo associato

## È tutto legale?

Sì, **se resti nel perimetro pubblico**:

- Non violi la legge se raccogli solo ciò che è accessibile a tutti
- Ma è tua responsabilità usare le informazioni in modo etico e lecito

## In sintesi: cosa puoi fare con LinkedIn e OSINT

- Ricostruire gerarchie aziendali
- Identificare persone e verificare identità
- Raccogliere dettagli su ruoli, progetti, tecnologie
- Analizzare flussi di personale
- Preparare simulazioni, investigazioni e inchieste

☐☐ Ti interessa scoprire come usare l'OSINT per le tue indagini digitali, anche se non sei un esperto?

Iscriviti alla newsletter “[OSINT & AI per tutti](#)” su Substack o unisciti al nostro gruppo Telegram.