Proteggere i Webinar Pubblici dalle Registrazioni Bot — Best Practice di Sicurezza

🛡️ **Scopo:** Questa guida illustra le impostazioni di sicurezza consigliate per Zoom Webinar, al fine di proteggere i webinar pubblici dalle registrazioni automatizzate (bot) e dagli accessi non autorizzati. Si tratta di azioni concrete che il vostro amministratore Zoom e gli host dei webinar possono implementare immediatamente.

Comprendere il Rischio

I webinar pubblici con link di registrazione aperti possono attirare registrazioni automatizzate da parte di bot — spesso centinaia di iscrizioni fraudolente nel giro di pochi secondi. Gli indicatori più comuni includono:

- **URL spam** nei campi nome dei registranti
- **Indirizzi email generati in massa** da provider di posta elettronica gratuiti
- **Titoli professionali, organizzazioni o paesi** uniformi o privi di senso
- **Velocità di registrazione elevata** — molte registrazioni in un intervallo di tempo molto breve

Le impostazioni seguenti sono organizzate per priorità ed efficacia. Consigliamo di implementarne il maggior numero possibile in base al vostro caso d'uso.

---

1. Impostazioni di Registrazione *(Priorità Massima)*

Queste impostazioni controllano **chi può registrarsi** e come vengono elaborate le registrazioni.

Impostazione	Cosa Fa	Raccomandazione
Approvazione Manuale delle Registrazioni	L'host esamina e approva o rifiuta manualmente ogni registrante prima che venga inviato il link di accesso. I bot possono ancora inviare registrazioni, ma non possono accedere al webinar senza approvazione.	⭐ **Fortemente Consigliato**
Nascondere il Link di Accesso nella Pagina di Conferma	Il link di accesso viene inviato solo via email e non viene mostrato nel browser dopo la registrazione. Questo impedisce ai bot di acquisire immediatamente il link.	⭐ **Fortemente Consigliato**
Campi di Registrazione Obbligatori	Richiedere nome completo, organizzazione, paese e un campo scopo/settore. Questo fornisce dati più ricchi per lo screening manuale e rende più rilevabile la compilazione automatica dei moduli.	**Consigliato**
Limite Massimo di Registrazioni	Imposta un numero massimo di registranti. Agisce come misura di contenimento per limitare il volume degli abusi.	**Consigliato**
Link di Tracciamento per Fonte	Creare URL di registrazione separati per ogni canale di distribuzione (sito web, newsletter, partner, social media). Se un link viene compromesso, può essere disabilitato senza influire sugli altri canali.	**Consigliato**

💡 **Suggerimento per l'Approvazione Manuale:** Prestare attenzione a incongruenze geografiche o linguistiche e a grandi gruppi di registrazioni che arrivano nel giro di pochi secondi — sono indicatori forti di attività automatizzata.

---

2. Impostazioni di Accesso *(Più Efficaci Contro i Bot)*

Queste impostazioni controllano **chi può effettivamente entrare** nel webinar. Rappresentano la barriera più efficace contro i partecipanti automatizzati.

Impostazione	Cosa Fa	Raccomandazione
CAPTCHA per Utenti Ospiti	Richiede agli utenti del client web di completare una verifica CAPTCHA prima di accedere. Aggiunge un attrito minimo per i partecipanti legittimi, bloccando efficacemente gli strumenti automatizzati.	⭐ **Fortemente Consigliato**
Accesso Obbligatorio per il Client Web	Gli utenti che accedono tramite browser devono effettuare il login con un account Zoom. Questo blocca il metodo di ingresso bot più comune (browser web headless) mantenendo invariata l'esperienza per le app desktop/mobile.	⭐ **Fortemente Consigliato**
Non Incorporare il Passcode nell'URL	Richiede ai partecipanti di inserire manualmente il passcode invece che venga compilato automaticamente dal link. Impedisce ai bot di estrarre il passcode direttamente dall'URL.	**Consigliato**

🎯 **Combinazione ottimale per webinar pubblici:** Abilitare sia il **CAPTCHA per utenti ospiti** che l'**Accesso obbligatorio per il client web**. Insieme, bloccano gli strumenti automatizzati aggiungendo solo un attrito minimo (~10%) per i partecipanti umani legittimi.

Opzioni di Autenticazione (Per Webinar ad Accesso Limitato)

Se il pubblico del vostro webinar è limitato a organizzazioni o domini specifici, potete applicare un'autenticazione più restrittiva:

- **Accesso con account Zoom** — qualsiasi utente Zoom autenticato può partecipare
- **Accesso con domini specificati** — solo gli utenti con domini email approvati (es. `@vostraorganizzazione.org`) possono partecipare
- **Corrispondenza email di registrazione con account Zoom** — l'account utilizzato per accedere deve corrispondere all'email usata per la registrazione
- **SSO Esterno** — integrazione con il vostro identity provider per il controllo degli accessi più rigoroso

Nota: Requisiti di autenticazione completi potrebbero impedire ad alcuni partecipanti legittimi privi di un account Zoom di accedere. Per eventi realmente pubblici, la combinazione CAPTCHA + accesso obbligatorio per il client web è il bilanciamento consigliato.

---

3. Misure di Protezione Aggiuntive

- **Non pubblicare i link di accesso pubblicamente** — considerare qualsiasi link di registrazione o accesso pubblicato come potenzialmente esposto allo scraping. Distribuire i link solo attraverso canali controllati.
- **Verificare i domini email dei registranti** — durante l'approvazione manuale, prestare attenzione a gruppi di registrazioni provenienti da domini email insoliti o generati in massa.
- **Monitorare prima dell'evento** — esaminare e rifiutare in blocco le registrazioni sospette in attesa o già approvate prima dell'inizio del webinar.

- **Protezione bot integrata** — Il rilevamento bot integrato di Zoom è attivo per impostazione predefinita nella Web App e non può essere disabilitato. Questo fornisce un livello di protezione di base.

---

4. Checklist delle Azioni Consigliate

Per ogni prossimo webinar pubblico, verificare che le seguenti impostazioni siano attive:

- [ ] **Approvazione manuale delle registrazioni** abilitata
- [ ] **CAPTCHA per utenti ospiti** abilitato
- [ ] **Accesso obbligatorio per gli utenti del client web** abilitato
- [ ] **Link di accesso nascosto** dalla pagina di conferma registrazione (invio solo via email)
- [ ] **Passcode non incorporato** nell'URL di accesso
- [ ] **Campi di registrazione obbligatori** configurati (nome, organizzazione, paese, scopo/settore)
- [ ] **Limite massimo di registrazioni** impostato su un valore appropriato
- [ ] **Link di tracciamento per fonte** creati per ogni canale di distribuzione
- [ ] Pianificare la **revisione delle registrazioni** e il rifiuto in blocco delle voci sospette prima dell'inizio dell'evento

---

Domande o Supporto

In caso di attacco bot in corso o per assistenza nella configurazione di queste impostazioni, contattate il vostro team Zoom di riferimento. Siamo a disposizione per garantirvi un'esperienza webinar sicura e di successo.