oneway

DOCUMENTO DI ESEMPIO — DATI SIMULATI

RAPPORTO MENSILE DI SORVEGLIANZA

Servizio SENTINELLA · Piano Diamond · Rapporto n. 014

CLIENTE	DOMINIO PRINCIPALE	PERIODO	EMESSO IL
Ferrucci Impianti S.r.l.	ferrucciimpianti.it	1 – 31 ottobre 2026	1 novembre 2026
DOMINI SORVEGLIATI	**VERIFICHE ESEGUITE**	**EVENTI RILEVATI**	**STATO GENERALE**
3	31 su 31 giorni	4	ATTENZIONE

1 Il mese in quattro numeri

412
invii non autorizzati a vostro nome, rilevati e respinti dai server riceventi

102
di questi provenienti da origini sconosciute

87,1%
delle vostre email correttamente autenticate

1
dominio simile al vostro registrato da terzi

In una riga. Nel mese di ottobre 412 messaggi hanno tentato di partire dal vostro dominio senza autorizzazione. Di questi, 310 provengono da **vostri servizi legittimi non ancora configurati** (li elenchiamo al punto 2) e 102 da **origini che non vi appartengono**. Nessuno di essi è stato consegnato con autenticazione valida.

2 Autenticazione della posta

I server di posta che ricevono messaggi a nome del vostro dominio verificano se il mittente era autorizzato e ci trasmettono i rapporti aggregati. Di seguito la loro sintesi.

Origine	Messaggi	Esito verifica	Classificazione
Server di posta aziendale	2.772	superata	LEGITTIMO
Piattaforma di invio newsletter	188	non superata	VOSTRO, DA CONFIGURARE
Gestionale di fatturazione	77	non superata	VOSTRO, DA CONFIGURARE
Piattaforma prenotazione interventi	45	non superata	VOSTRO, DA CONFIGURARE
Indirizzo di rete non riconosciuto — area asiatica	61	non superata	ORIGINE SCONOSCIUTA
Indirizzo di rete non riconosciuto — area est-europea	28	non superata	ORIGINE SCONOSCIUTA
Indirizzi di rete diffusi, singole occorrenze	13	non superata	ORIGINE SCONOSCIUTA
Totale messaggi valutati	**3.184**		

Come leggere questi dati. «Origine sconosciuta» significa che il messaggio non proviene da un sistema da voi autorizzato. Non costituisce prova di un attacco né identificazione di un responsabile: la collocazione geografica deriva dall'indirizzo di rete e può essere alterata. I 310 messaggi classificati come vostri non sono un pericolo, ma vanno regolarizzati: finché restano non autenticati, quelle comunicazioni rischiano di finire nella posta indesiderata dei vostri clienti.

Andamento degli ultimi sei mesi

Mese	Non autorizzati	Andamento
Maggio	96	
Giugno	134	
Luglio	203	
Agosto	288	
Settembre	351	
Ottobre	**412**	

L'aumento è in larga parte riconducibile all'incremento degli invii dalla piattaforma newsletter, non ancora configurata. Le origini sconosciute sono passate da 71 a 102 nello stesso periodo.

3 Domini e certificati

Elemento	Stato	Scadenza	Esito
ferrucciimpianti.it	Intestato a Ferrucci Impianti S.r.l.	14/12/2027	OK
ferrucci-impianti.it	Intestato a Ferrucci Impianti S.r.l.	03/05/2027	OK
ferrucciclima.it	**Intestato a soggetto terzo** (agenzia web)	22/02/2027	DA SANARE
Certificato sito principale	Valido, rinnovo automatico attivo	19/01/2027	OK
Liste nere antispam (7 elenchi)	Nessuna segnalazione	—	OK

4 Domini simili di nuova registrazione

Dominio	Registrato il	Osservazioni
ferrucciimpianti.net	12/10/2026	Registrato da soggetto non identificabile, con dati di contatto oscurati. Nessun sito pubblicato, nessuna configurazione di posta attiva al 31/10. Resta sotto osservazione quotidiana

La registrazione di un dominio simile non costituisce di per sé un illecito. Viene segnalata perché, nei casi di frode, precede tipicamente l'invio di comunicazioni ai clienti dell'azienda imitata.

5 Credenziali comparse in violazioni pubbliche

Indirizzo	Rilevato il	Origine della violazione
a•••••@ferrucciimpianti.it	21/10/2026	Archivio reso pubblico nel 2026, relativo a un portale di servizi di terze parti

La segnalazione riguarda la comparsa dell'indirizzo in un elenco pubblicamente accessibile. Non implica che i vostri sistemi siano stati violati.

6 Cosa vi consigliamo di fare, in ordine

Pr.	Azione	Perché
1	Autorizzare i tre servizi vostri elencati al punto 2	Elimina 310 invii non autenticati al mese e riduce il rischio che le vostre comunicazioni finiscano nella posta indesiderata
2	Richiedere il trasferimento di *ferrucciclima.it* a nome della società	Oggi quel dominio non è vostro. In caso di contrasto con l'attuale intestatario non avreste titolo per ottenerlo
3	Cambiare la password dell'indirizzo segnalato al punto 5	La credenziale è pubblicamente reperibile
4	Valutare la registrazione difensiva di *ferrucciimpianti.net*	Costo contenuto, elimina alla radice l'utilizzo di quel nome

Le prime due azioni rientrano nell'attivazione guidata compresa nel vostro piano: se lo desiderate, ve ne indichiamo i parametri esatti e ne verifichiamo il funzionamento. Le attività eseguite direttamente da noi sui vostri sistemi sono oggetto di separata offerta.

7 Registro giornaliero delle verifiche

Di seguito il dettaglio di ogni verifica svolta nel periodo. Il registro viene conservato e resta disponibile per l'intera durata del servizio.

Data	Ore	Controlli	Non autorizz.	Sconosciuti	Eventi rilevati
01/10	03:12	9/9	11	2	—
02/10	03:09	9/9	14	3	—
03/10	03:14	9/9	44	4	Picco invii: campagna newsletter del 03/10
04/10	03:11	9/9	21	2	—
05/10	03:08	9/9	6	1	—
06/10	03:15	9/9	9	3	—
07/10	03:10	9/9	17	5	—
08/10	03:13	9/9	12	2	—
09/10	03:07	9/9	15	4	—
10/10	03:12	9/9	10	2	—
11/10	03:09	9/9	8	1	—
12/10	03:11	9/9	13	3	**Rilevata registrazione del dominio ferrucciimpianti.net — avviso immediato inviato ore 03:18**
13/10	03:14	9/9	16	4	Dominio simile: nessuna attività
14/10	03:10	9/9	19	6	—
15/10	03:08	9/9	22	5	—
16/10	03:13	9/9	14	3	—
17/10	03:09	9/9	11	2	Certificato: rinnovo automatico verificato
18/10	03:12	9/9	7	1	—
19/10	03:11	9/9	9	3	—
20/10	03:15	9/9	18	7	Aumento invii da origine asiatica
21/10	03:07	9/9	16	6	**Credenziale aziendale rilevata in archivio pubblico — avviso inviato ore 03:20**
22/10	03:13	9/9	13	4	—
23/10	03:10	9/9	15	5	—
24/10	03:12	9/9	20	4	—
25/10	03:09	9/9	6	2	—
26/10	03:14	9/9	8	3	—
27/10	03:11	9/9	17	9	**Nuova origine sconosciuta est-europea, 9 tentativi in 24 ore — sotto osservazione**
28/10	03:08	9/9	14	6	Stessa origine: 6 tentativi
29/10	03:13	9/9	12	4	—
30/10	03:10	9/9	10	3	—
31/10	03:12	9/9	15	5	Chiusura periodo, elaborazione rapporto
Totale	**—**	**279/279**	**412**	**102**	**4 eventi, 3 avvisi immediati inviati**

I nove controlli giornalieri comprendono: autenticazione della posta, scadenza e intestazione dei tre domini, validità del certificato, presenza in sette elenchi antispam, comparsa di credenziali in archivi pubblici, registrazione di domini simili, raggiungibilità del sito, integrità dei record di instradamento della posta.

8 Metodo e limiti

Le verifiche sono condotte **esclusivamente dall'esterno**, su informazioni pubblicamente accessibili e su rapporti aggregati trasmessi dai server riceventi. **Non accediamo ai vostri sistemi e non leggiamo il contenuto delle vostre comunicazioni**: i rapporti che riceviamo contengono unicamente dati numerici e indirizzi di rete, senza testo, oggetto, destinatari o allegati.

Il servizio consiste nella sorveglianza e nella segnalazione. Non impedisce materialmente l'invio di messaggi contraffatti, che viene respinto dai server riceventi sulla base della configurazione pubblicata. **Un rapporto privo di segnalazioni non costituisce attestazione di sicurezza** né certificazione di conformità.