AI nelle email: perché phishing e messaggi falsi sono diventati più credibili

Maria Cattini | 30/06/2026 | Intelligenza Artificiale

Una mail falsa non deve più sembrare scritta male per essere pericolosa.

Per anni molte persone hanno imparato a riconoscere il phishing da segnali abbastanza visibili: errori grammaticali, traduzioni strane, loghi sgranati, formule generiche, frasi costruite male. Quei segnali esistono ancora, ma non bastano più.

Con l'intelligenza artificiale generativa, un messaggio falso può essere scritto in italiano corretto, con un tono plausibile, senza errori evidenti e con riferimenti più vicini al contesto della persona che lo riceve.

Il problema non è che l'AI abbia inventato il phishing.

Il phishing esiste da molto prima dei chatbot. Il cambiamento è un altro: l'AI rende più facile produrre messaggi credibili, adattarli a pubblici diversi, correggere il tono, tradurre bene, imitare uno stile aziendale e creare molte varianti dello stesso inganno.

Questo sposta il punto della verifica.

Non possiamo più chiederci solo: "questa email sembra scritta male?".

Dobbiamo chiederci: "che cosa mi sta chiedendo di fare, con quale urgenza, attraverso quale canale e con quali prove?".

Che cosa cambia con l'AI

Una truffa via email funziona quando riesce a farci compiere un'azione prima che ci fermiamo a controllare.

Può chiederci di:

• aprire un allegato;
• cliccare un link;
• inserire una password;
• aggiornare un metodo di pagamento;
• confermare un codice;
• pagare una fattura;
• rispondere con dati personali;
• scaricare un file;
• contattare un numero indicato nel messaggio.

L'AI non cambia questa logica. La rende più pulita.

Un messaggio generato o rifinito con l’AI può eliminare molti segnali che in passato ci aiutavano. Può correggere errori, scegliere parole più naturali, adattare il registro a un contesto professionale, rendere meno evidente la traduzione automatica.

Può anche produrre versioni diverse dello stesso messaggio: una più formale per un ufficio, una più diretta per un cliente, una più urgente per chi gestisce pagamenti, una più tecnica per chi lavora con strumenti digitali.

Il risultato è che la qualità linguistica non è più una garanzia.

Una mail scritta bene può essere falsa.

Il phishing non punta solo al link

Quando pensiamo al phishing, immaginiamo spesso una mail con un link verso una pagina falsa.

Succede ancora. Ma molte email pericolose non cercano subito il clic.

Possono servire a preparare il terreno.

Un primo messaggio può sembrare innocuo: “puoi controllare questa pratica?”, “ti giro il documento dopo”, “sei disponibile per una conferma veloce?”. Solo dopo arriva la richiesta vera.

Questo è importante perché molte persone abbassano la guardia quando il primo messaggio non contiene link, allegati o richieste economiche.

Il rischio, però, può essere nella conversazione.

Se un attaccante riesce a ottenere una risposta, ha già un vantaggio: conferma che l’indirizzo è attivo, capisce il tono della persona, può raccogliere dettagli e rendere il secondo messaggio più credibile.

L’AI può aiutare proprio in questa fase: non solo a scrivere il messaggio iniziale, ma a mantenere una conversazione più fluida.

Per questo la domanda non deve essere solo:

```
il link è sicuro?
```

La domanda completa è:

```
questa richiesta ha senso, arriva dal canale giusto e può essere verificata fuori dal
l'email?
```

Perché le email false sembrano più personali

Molte informazioni utili per personalizzare un messaggio sono pubbliche o semi-pubbliche.

Un profilo LinkedIn, una pagina aziendale, un comunicato stampa, una firma email, un sito personale, una bio social, un post pubblico, una pagina “chi siamo” possono rivelare ruolo, colleghi, interessi, progetti, eventi, linguaggio usato dall’organizzazione.

Non serve immaginare uno scenario sofisticato.

Se una persona scrive spesso online di un settore, partecipa a eventi, pubblica il proprio ruolo e usa

sempre lo stesso indirizzo professionale, un messaggio falso può diventare più credibile semplicemente perché usa dettagli reali.

Esempio:

```
Ciao, ho visto che stai seguendo il progetto sulla formazione digitale.
Ti giro la versione aggiornata del documento per la revisione di oggi.
```

Questa frase non dimostra nulla, ma sembra più plausibile di una mail generica.

Il punto è questo: la personalizzazione non è una prova di autenticità.

Una mail può contenere informazioni vere e restare una truffa.

I vecchi segnali non bastano più

Gli errori di grammatica, gli indirizzi strani e i loghi malfatti restano segnali utili.

Ma non sono più sufficienti.

Oggi bisogna guardare soprattutto il comportamento richiesto dal messaggio.

Un’email va trattata con cautela quando:

• crea urgenza improvvisa;
• chiede di uscire dalla procedura normale;
• spinge a non coinvolgere altre persone;
• chiede dati che normalmente non si mandano via email;
• cambia un IBAN, un link di pagamento o un metodo di accesso;
• chiede di inserire credenziali dopo un clic;
• usa un allegato inatteso;
• arriva in un momento coerente ma da un canale insolito;
• sembra scritta da una persona nota, ma con una richiesta fuori abitudine.

Il segnale più importante non è sempre l’errore visibile.

È la deviazione.

Se un messaggio chiede di fare qualcosa che modifica denaro, accessi, dati o documenti, va verificato con un secondo canale.

Il controllo più semplice: uscire dall’email

Il modo più pratico per verificare una mail sospetta è non usare i contatti presenti nella mail.

Se il messaggio sembra arrivare da una banca, non usare il link nella mail: apri il sito digitando l’indirizzo o usa l’app ufficiale.

Se sembra arrivare da un collega, non rispondere subito con dati o conferme: usa un canale già noto, per esempio una telefonata, una chat interna o un numero salvato.

Se sembra arrivare da un fornitore che chiede un cambio di pagamento, non usare il numero indicato nel messaggio: recupera il contatto da un contratto, da una rubrica interna o da una comunicazione precedente già verificata.

La regola è semplice:

quando una richiesta è sensibile, la verifica deve uscire dal messaggio che la contiene.

Questo vale anche quando la mail è scritta bene.

Anzi: vale soprattutto quando è scritta bene.

Che cosa controllare prima di cliccare

Prima di aprire un link o un allegato, fermati su cinque punti.

1. Il mittente reale

Non guardare solo il nome visualizzato.

Il nome può dire “assistenza”, “amministrazione”, “ufficio pagamenti” o il nome di una persona che conosci. Devi controllare anche l’indirizzo email completo.

Attenzione però: anche un indirizzo apparentemente plausibile non basta da solo. Account compromessi, domini simili e servizi legittimi abusati possono rendere l’email più difficile da leggere.

2. La richiesta

Chiediti che cosa vuole ottenere il messaggio.

Vuole una password? Un codice? Un pagamento? Un file? Una risposta veloce? Un clic? Un accesso a un documento?

Se la richiesta riguarda dati, denaro o credenziali, non deve essere trattata come una comunicazione normale.

3. L’urgenza

Molte truffe cercano di ridurre il tempo di riflessione.

“Scade oggi”, “azione richiesta”, “ultimo avviso”, “conto sospeso”, “pagamento bloccato”, “documento urgente”: non sono prove di falsità, ma sono segnali da verificare.

L’urgenza è una tecnica, non una prova.

4. Il percorso del link

Passare il mouse su un link può aiutare, ma non risolve tutto.

Su mobile è più difficile controllare. Alcuni link usano servizi di tracciamento, abbreviazioni, redirect o domini simili. Se la richiesta è importante, non seguire il link: raggiungi il servizio da un percorso indipendente.

5. Il contesto

La domanda finale è pratica:

questa richiesta era attesa?

Se non lo era, va verificata.

Se lo era, ma chiede una procedura diversa dal solito, va verificata lo stesso.

Che cosa fare se hai già cliccato

Cliccare non significa automaticamente essere compromessi, ma non va ignorato.

La risposta dipende da cosa è successo dopo.

Se hai solo aperto una pagina, chiudila e non inserire dati. Se hai inserito una password, cambiala subito dal sito ufficiale e attiva o controlla l'autenticazione a più fattori. Se hai scaricato un file, non aprirlo e chiedi supporto tecnico. Se lo hai aperto, scollega il dispositivo dalla rete se sospetti malware e avvisa chi gestisce la sicurezza o l'assistenza informatica.

Se hai comunicato dati bancari, codici, documenti o informazioni personali, contatta subito banca, servizio coinvolto o referente tecnico. Se il messaggio riguardava il lavoro, avvisa l'organizzazione: spesso una campagna di phishing non colpisce una sola persona.

La vergogna è un alleato degli attaccanti.

Segnalare in fretta riduce il danno.

Checklist rapida

Prima di fidarti di una mail, chiediti:

• conosco davvero il mittente?
• l'indirizzo completo è coerente?
• questa richiesta era attesa?
• chiede soldi, password, codici o dati?
• crea urgenza?
• mi spinge a uscire dalle procedure normali?
• posso verificare da un canale indipendente?
• il link porta davvero al servizio ufficiale?
• l'allegato era previsto?
• qualcuno può confermare la richiesta?

Se due o più risposte ti mettono in dubbio, fermati.

Non serve diventare paranoici. Serve cambiare abitudine.

Le email false sono diventate più credibili perché l'AI può migliorare il testo, il tono e la personalizzazione. Ma una truffa, anche quando è scritta bene, deve ancora chiederti qualcosa.

È lì che va fatta la verifica.

Non sulla bellezza della mail.

Sulla richiesta che contiene.
Una mail falsa non deve più sembrare scritta male per essere pericolosa.

Per anni molte persone hanno imparato a riconoscere il phishing da segnali abbastanza visibili: errori grammaticali, traduzioni strane, loghi sgranati, formule generiche, frasi costruite male. Quei segnali esistono ancora, ma non bastano più.

Con l'intelligenza artificiale generativa, un messaggio falso può essere scritto in italiano corretto, con un tono plausibile, senza errori evidenti e con riferimenti più vicini al contesto della persona che lo

riceve.

Il problema non è che l’AI abbia inventato il phishing.

Il phishing esiste da molto prima dei chatbot. Il cambiamento è un altro: l’AI rende più facile produrre messaggi credibili, adattarli a pubblici diversi, correggere il tono, tradurre bene, imitare uno stile aziendale e creare molte varianti dello stesso inganno.

Questo sposta il punto della verifica.

Non possiamo più chiederci solo: “questa email sembra scritta male?”.

Dobbiamo chiederci: “che cosa mi sta chiedendo di fare, con quale urgenza, attraverso quale canale e con quali prove?”.

Che cosa cambia con l’AI

Una truffa via email funziona quando riesce a farci compiere un’azione prima che ci fermiamo a controllare.

Può chiederci di:

• aprire un allegato;
• cliccare un link;
• inserire una password;
• aggiornare un metodo di pagamento;
• confermare un codice;
• pagare una fattura;
• rispondere con dati personali;
• scaricare un file;
• contattare un numero indicato nel messaggio.

L’AI non cambia questa logica. La rende più pulita.

Un messaggio generato o rifinito con l’AI può eliminare molti segnali che in passato ci aiutavano. Può correggere errori, scegliere parole più naturali, adattare il registro a un contesto professionale, rendere meno evidente la traduzione automatica.

Può anche produrre versioni diverse dello stesso messaggio: una più formale per un ufficio, una più diretta per un cliente, una più urgente per chi gestisce pagamenti, una più tecnica per chi lavora con strumenti digitali.

Il risultato è che la qualità linguistica non è più una garanzia.

Una mail scritta bene può essere falsa.

Il phishing non punta solo al link

Quando pensiamo al phishing, immaginiamo spesso una mail con un link verso una pagina falsa.

Succede ancora. Ma molte email pericolose non cercano subito il clic.

Possono servire a preparare il terreno.

Un primo messaggio può sembrare innocuo: “puoi controllare questa pratica?”, “ti giro il documento dopo”, “sei disponibile per una conferma veloce?”. Solo dopo arriva la richiesta vera.

Questo è importante perché molte persone abbassano la guardia quando il primo messaggio non

contiene link, allegati o richieste economiche.

Il rischio, però, può essere nella conversazione.

Se un attaccante riesce a ottenere una risposta, ha già un vantaggio: conferma che l'indirizzo è attivo, capisce il tono della persona, può raccogliere dettagli e rendere il secondo messaggio più credibile.

L'AI può aiutare proprio in questa fase: non solo a scrivere il messaggio iniziale, ma a mantenere una conversazione più fluida.

Per questo la domanda non deve essere solo:

```
il link è sicuro?
```

La domanda completa è:

```
questa richiesta ha senso, arriva dal canale giusto e può essere verificata fuori dal
l'email?
```

Perché le email false sembrano più personali

Molte informazioni utili per personalizzare un messaggio sono pubbliche o semi-pubbliche.

Un profilo LinkedIn, una pagina aziendale, un comunicato stampa, una firma email, un sito personale, una bio social, un post pubblico, una pagina "chi siamo" possono rivelare ruolo, colleghi, interessi, progetti, eventi, linguaggio usato dall'organizzazione.

Non serve immaginare uno scenario sofisticato.

Se una persona scrive spesso online di un settore, partecipa a eventi, pubblica il proprio ruolo e usa sempre lo stesso indirizzo professionale, un messaggio falso può diventare più credibile semplicemente perché usa dettagli reali.

Esempio:

```
Ciao, ho visto che stai seguendo il progetto sulla formazione digitale.
Ti giro la versione aggiornata del documento per la revisione di oggi.
```

Questa frase non dimostra nulla, ma sembra più plausibile di una mail generica.

Il punto è questo: la personalizzazione non è una prova di autenticità.

Una mail può contenere informazioni vere e restare una truffa.

I vecchi segnali non bastano più

Gli errori di grammatica, gli indirizzi strani e i loghi malfatti restano segnali utili.

Ma non sono più sufficienti.

Oggi bisogna guardare soprattutto il comportamento richiesto dal messaggio.

Un’email va trattata con cautela quando:

• crea urgenza improvvisa;
• chiede di uscire dalla procedura normale;
• spinge a non coinvolgere altre persone;
• chiede dati che normalmente non si mandano via email;
• cambia un IBAN, un link di pagamento o un metodo di accesso;
• chiede di inserire credenziali dopo un clic;
• usa un allegato inatteso;
• arriva in un momento coerente ma da un canale insolito;
• sembra scritta da una persona nota, ma con una richiesta fuori abitudine.

Il segnale più importante non è sempre l’errore visibile.

È la deviazione.

Se un messaggio chiede di fare qualcosa che modifica denaro, accessi, dati o documenti, va verificato con un secondo canale.

Il controllo più semplice: uscire dall’email

Il modo più pratico per verificare una mail sospetta è non usare i contatti presenti nella mail.

Se il messaggio sembra arrivare da una banca, non usare il link nella mail: apri il sito digitando l’indirizzo o usa l’app ufficiale.

Se sembra arrivare da un collega, non rispondere subito con dati o conferme: usa un canale già noto, per esempio una telefonata, una chat interna o un numero salvato.

Se sembra arrivare da un fornitore che chiede un cambio di pagamento, non usare il numero indicato nel messaggio: recupera il contatto da un contratto, da una rubrica interna o da una comunicazione precedente già verificata.

La regola è semplice:

```
quando una richiesta è sensibile, la verifica deve uscire dal messaggio che la contie
ne.
```

Questo vale anche quando la mail è scritta bene.

Anzi: vale soprattutto quando è scritta bene.

Che cosa controllare prima di cliccare

Prima di aprire un link o un allegato, fermati su cinque punti.

1. Il mittente reale

Non guardare solo il nome visualizzato.

Il nome può dire “assistenza”, “amministrazione”, “ufficio pagamenti” o il nome di una persona che conosci. Devi controllare anche l’indirizzo email completo.

Attenzione però: anche un indirizzo apparentemente plausibile non basta da solo. Account compromessi, domini simili e servizi legittimi abusati possono rendere l’email più difficile da leggere.

2. La richiesta

Chiediti che cosa vuole ottenere il messaggio.

Vuole una password? Un codice? Un pagamento? Un file? Una risposta veloce? Un clic? Un accesso a un documento?

Se la richiesta riguarda dati, denaro o credenziali, non deve essere trattata come una comunicazione normale.

3. L’urgenza

Molte truffe cercano di ridurre il tempo di riflessione.

“Scade oggi”, “azione richiesta”, “ultimo avviso”, “conto sospeso”, “pagamento bloccato”, “documento urgente”: non sono prove di falsità, ma sono segnali da verificare.

L’urgenza è una tecnica, non una prova.

4. Il percorso del link

Passare il mouse su un link può aiutare, ma non risolve tutto.

Su mobile è più difficile controllare. Alcuni link usano servizi di tracciamento, abbreviazioni, redirect o domini simili. Se la richiesta è importante, non seguire il link: raggiungi il servizio da un percorso indipendente.

5. Il contesto

La domanda finale è pratica:

```
questa richiesta era attesa?
```

Se non lo era, va verificata.

Se lo era, ma chiede una procedura diversa dal solito, va verificata lo stesso.

Che cosa fare se hai già cliccato

Cliccare non significa automaticamente essere compromessi, ma non va ignorato.

La risposta dipende da cosa è successo dopo.

Se hai solo aperto una pagina, chiudila e non inserire dati. Se hai inserito una password, cambiala subito dal sito ufficiale e attiva o controlla l’autenticazione a più fattori. Se hai scaricato un file, non aprirlo e chiedi supporto tecnico. Se lo hai aperto, scollega il dispositivo dalla rete se sospetti malware e avvisa chi gestisce la sicurezza o l’assistenza informatica.

Se hai comunicato dati bancari, codici, documenti o informazioni personali, contatta subito banca, servizio coinvolto o referente tecnico. Se il messaggio riguardava il lavoro, avvisa l’organizzazione: spesso una campagna di phishing non colpisce una sola persona.

La vergogna è un alleato degli attaccanti.

Segnalare in fretta riduce il danno.

Checklist rapida

Prima di fidarti di una mail, chiediti:

• conosco davvero il mittente?
• l’indirizzo completo è coerente?
• questa richiesta era attesa?
• chiede soldi, password, codici o dati?
• crea urgenza?
• mi spinge a uscire dalle procedure normali?
• posso verificare da un canale indipendente?
• il link porta davvero al servizio ufficiale?
• l’allegato era previsto?
• qualcuno può confermare la richiesta?

Se due o più risposte ti mettono in dubbio, fermati.

Non serve diventare paranoici. Serve cambiare abitudine.

Le email false sono diventate più credibili perché l’AI può migliorare il testo, il tono e la personalizzazione. Ma una truffa, anche quando è scritta bene, deve ancora chiederti qualcosa.

È lì che va fatta la verifica.

Non sulla bellezza della mail.

Sulla richiesta che contiene.