

# Simulazione di phishing

Scelgo come obiettivo gli utenti del servizio di logistica Bartolini (BRT). L'idea alla base è quella di creare un'email il più possibile credibile, capace di ingannare un destinatario e indurlo a rivelare informazioni sensibili.

Per farlo, ho costruito un messaggio che sembra provenire dal reparto di sicurezza IT di BRT, segnalando un accesso sospetto all'account aziendale del destinatario. L'email include elementi studiati per rendere il messaggio più credibile. Inoltre, il testo mette in evidenza l'urgenza, chiedendo alla vittima di verificare la propria identità entro sei ore per evitare la sospensione dell'account. Il link fornito rimanda a una landing page identica a quella ufficiale di BRT, ma idealmente progettata per raccogliere le credenziali inserite dall'utente.

Questa tecnica, basata sull'ingegneria sociale, punta a manipolare psicologicamente il destinatario, facendolo agire d'impulso senza verificare attentamente i dettagli. Nel mio scenario, i dati rubati potrebbero essere sfruttati non solo per accedere ai sistemi aziendali, ma anche per raccogliere informazioni sensibili da usare per un possibile ricatto. Un attaccante potrebbe, ad esempio, minacciare di divulgare dati riservati o compromettere l'account dell'utente per ottenere un riscatto.

## Di seguito riporto la mail:

**Oggetto:** URGENTE: Verifica Account IT – Accesso Sospetto Segnalato

**Da:** security@brt-logistica.com

**A:** Mario Rossi





**Data:** 28/02/2025 13:07

---

**Caro Mario Rossi,**

CyberSec Solutions, **partner di sicurezza informatica di BRT**, ha rilevato un **accesso sospetto** al tuo account aziendale "**mariorossi@brt.it**".

### **Dettagli dell'attività anomala:**

-  **Tentativo di accesso:** 27/02/2025 14:19
-  **Indirizzo IP sconosciuto:** 45.176.89.XX (Brasile)
-  **Dispositivo:** Windows 10, Chrome Browser
-  **Sede di accesso:** Esterno alla rete aziendale BRT

Per proteggere il tuo account e prevenire la sospensione, è necessario confermare la tua identità entro le prossime **6 ore**.

**Accedi al Portale Sicurezza IT e verifica il tuo account:**

 <security.brt.it/verifica-utente> ({{.URL}})

Questa operazione è richiesta in conformità alle politiche di sicurezza di [Nome Azienda] e alle linee guida ISO/IEC 27001.

 **Supporto IT & CyberSec**

 security@cybersec-solutions.com

 **Numero interno:** 0245 678 910

 **Help Desk IT Aziendale:** +39 02 1234 5678

 **Ticket ID:** SEC-2024028745

 **Firma digitale verificata**

**Luca Ferri**

**Security Operations Manager**

CyberSec Solutions | Partner ufficiale di BRT

 [www.security.cybersec-solutions.com](http://www.security.cybersec-solutions.com)

**Il processo è il seguente:**

**L'email arriva ai dipendenti** con un testo credibile e un link tracciato ({{.URL}}).

**Alcuni dipendenti cliccano sul link**, aprendo la **landing page fake**.

**Se inseriscono le credenziali, GoPhish registra l'azione** (ma non raccoglie realmente le password).

**Dopo averle inserite, vengono reindirizzati al sito ufficiale di BRT**, quindi potrebbero non accorgersi subito del phishing.

**Dati che possiamo raccogliere:**

- **Quanti dipendenti aprono l'email**
- **Quanti cliccano sul link** nella mail
- **Quanti inseriscono le credenziali** nella landing page

Sebbene l'email sia ben costruita, alcuni segnali potrebbero allertare un occhio attento:

- il dominio dell'indirizzo email del mittente, leggermente diverso da quello ufficiale;
- il link sospetto, la richiesta di un'azione immediata (tipico degli attacchi di phishing);
- la presenza di una società esterna poco conosciuta come supposto partner di sicurezza.

Questi dettagli sono indicatori comuni di tentativi di truffa e rappresentano i primi elementi da controllare per evitare di cadere vittima di attacchi informatici.

Questa simulazione mostra quanto possa essere facile costruire una mail credibile e quanto sia importante saper riconoscere i segnali di phishing, per evitare di mettere a rischio dati personali e aziendali.

\*Screenshot landing page del sito ufficiale BRT utilizzando GOPHISH.

