Obiettivo: simulare un email phishing.

Scenario: mail proveniente dalla nasa con vincita un viaggio nello spazio, si chiede di andare sui link dove si dovranno inserire varie informazioni personali e dati finanziari.

Mittente: NASA Official contact@nasa-space-program.org
Oggetto: Congratulazioni! Sei stato selezionato per un volo spaziale gratuito con la NASA 🚀

Corpo dell'email:

Gentile [Nome],

Congratulazioni!

Siamo lieti di informarti che sei stato **selezionato casualmente** per partecipare al nostro nuovo programma di **volo turistico nello spazio**, in collaborazione con Space Frontier Initiative.

Questa opportunità **unica nella vita** ti permetterà di vivere l'esperienza di un astronauta, a bordo di una navetta spaziale ufficiale della NASA.

Per **confermare la tua partecipazione**, ti preghiamo di cliccare sul seguente link e completare il modulo con i tuoi dati personali e di pagamento (sarà richiesto solo un piccolo deposito rimborsabile per la prenotazione del posto):

👉 **https://nasa-prize-confirmation.space/winnerID=98423**

⚠️ ATTENZIONE: Hai tempo fino a **domani alle 18:00 (EST)** per completare il modulo. Dopo tale scadenza, il tuo posto verrà riassegnato ad altri candidati.

Per qualsiasi domanda, contattaci via email: **support@nasa-program.org**

Grazie per il tuo entusiasmo verso l'esplorazione spaziale!

Cordiali saluti,
Dr. Alan Shepard Jr.
NASA Public Relations Officer

"To the stars – and beyond."

Campanelli d’allarme:

1. Indirizzo email sospetto

- **contact@nasa-space-program.org** non è un dominio ufficiale NASA.
- Gli indirizzi ufficiali della NASA terminano in **@nasa.gov**.
- I truffatori usano domini simili per sembrare legittimi.

2. Premio troppo bello per essere vero

- La promessa di un **volo spaziale gratuito** è altamente improbabile, soprattutto senza alcuna candidatura.
- Le truffe spesso fanno leva su premi eccezionali per generare entusiasmo e abbassare l’attenzione critica.

3. Senso di urgenza

- Frasi come "**Hai tempo fino a domani alle 18:00**" sono usate per **mettere pressione** e spingere l’utente a **non riflettere** prima di agire.

4. Richiesta di dati personali e di pagamento

- Anche se il “deposito” è “rimborsabile”, chiedere **dati sensibili** tramite link sospetti è un segnale tipico di phishing.

5. Link sospetto (URL ingannevole)

- Il link **https://nasa-prize-confirmation.space** non è un dominio ufficiale.
- I phisher spesso usano **nomi verosimili** per ingannare, ma i veri siti NASA hanno URL chiari e sicuri, come **https://www.nasa.gov**.

6. Falsi riferimenti a personale NASA

- Il nome "**Dr. Alan Shepard Jr.**" è quello di un **vero astronauta deceduto nel 1998**. Usare nomi noti è una tecnica per dare credibilità.

7. Tono e formattazione sospetti

- L’eccesso di emoji, l’uso informale e la mancanza di stile istituzionale **non sono in linea con le comunicazioni ufficiali** della NASA