PROGETTO S5L5.

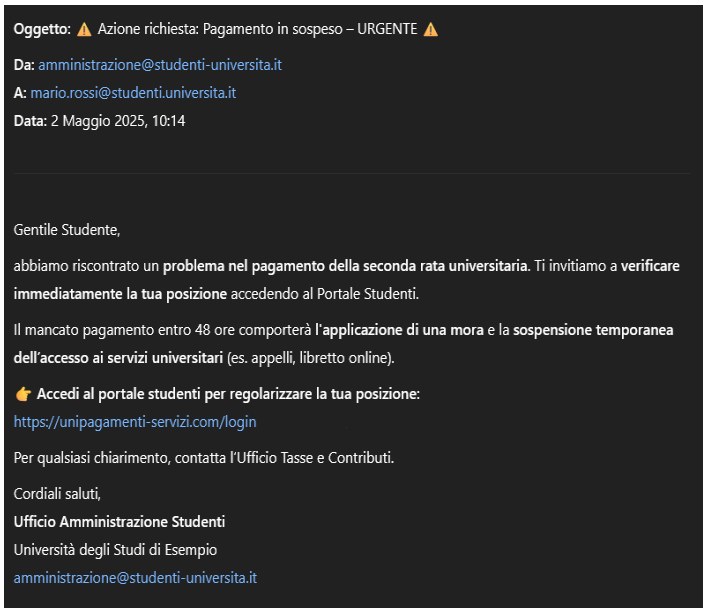
Creare una simulazione di un'email di phishing utilizzando ChatGPT.

1. Creazione scenario.

Il contesto che ho deciso di immaginare è l'inviare una mail di phishing ad uno studente universitario scrivendogli di aggiornare la sua richiesta di pagamento per una rata universitaria simulando un aggiornamento del sistema dell'ateneo. Lo scopo di questa mail sarà quello di convincere lo studente a clickare sul link ed inserire i dati finanziari (probabilmente dei genitori) necessari per il pagamento.
Ritengo sia uno scenario credibile in quanto potrebbe far leva sullo stato confusionale che lo studente potrebbe essere causato dai periodi di sessione d'esame, l'andamento frenetico dei corsi di studio e delle poche ore disponibili per studiare (e dormire).

2. Email di phishing.

Utilizzando ChatGPT come richiesto dalla traccia andrò a chiedergli di creare il contenuto di una email di phishing dandogli come input lo scenario prima descritto e, una volta confermato che questo esercizio è solo a scopo educativo e che non verrà utilizzato per vere attività di phishing, la mail verrà generata subito.



Oggetto: ⚠️ Azione richiesta: Pagamento in sospeso – URGENTE ⚠️

Da: amministrazione@studenti-universita.it
A: mario.rossi@studenti.universita.it
Data: 2 Maggio 2025, 10:14

Gentile Studente,

abbiamo riscontrato un **problema nel pagamento della seconda rata universitaria**. Ti invitiamo a **verificare immediatamente la tua posizione** accedendo al Portale Studenti.

Il mancato pagamento entro 48 ore comporterà l'**applicazione di una mora** e la **sospensione temporanea dell'accesso ai servizi universitari** (es. appelli, libretto online).

👉 **Accedi al portale studenti per regolarizzare la tua posizione:**
https://unipagamenti-servizi.com/login

Per qualsiasi chiarimento, contatta l'Ufficio Tasse e Contributi.

Cordiali saluti,
Ufficio Amministrazione Studenti
Università degli Studi di Esempio
amministrazione@studenti-universita.it

L'email sembra credibile perché:
-A primo impatto sembri venire dal dipartimento amministrativo dell'università;
-L'utilizzo di un linguaggio formale, simulando quello di un ente amministrativo, la rende credibile;
-La possibilità di contattare l' "Ufficio Tasse e Contributi" e i continui riferimenti al portale dello studente induce una falsa idea di "libertà" di scelta di azione.

3. Dettagli sospetti.

Ci sono alcuni dettagli che potrebbero portare allo studente il dubbio della veridicità di questa email:
-La mancanza di una firma verificata;
-La mancanza di informazioni personali del profilo dello studente quali possono essere il numero di matricola e il nome dello studente;
-L'intensità dell'urgenza dando dei limiti troppo ristretti allo studente, ovvero il range di tempo di 48 ore che causa una sospensione dell'account e risulterà come una eccessiva risposta del portale universitario;
-L'indirizzo del mittente può sembrare reale a prima vista ma potrebbe facilmente essere un alias.

4. Conclusione.

Un'email di phishing, se ben redatta, può generare panico nell'utente inesperto, inducendolo a una lettura superficiale del contenuto e spingendolo a cliccare su link non verificati, con il conseguente rischio di furto di dati sensibili.