

MAIL GENERATA PHISHING

Utilizzando una mail di phishing che avevo ricevuto dalla Geeks Academy, accademia di corsi informatica di Roma e altre città, ho voluto ricreare una mail indirizzata alla mia ragazza in cui le veniva proposto un corso di informatica scontato di 1000 euro, e per poter usufruire di questo sconto bisogna cliccare sul link indicato nella mail. Quindi ho chiesto a ChatGPT di scrivermi una mail accattivante indirizzata appunto a Laura.

Questo è il messaggio generato da ChatGPT:

Oggetto: Voglio proporti un affare, che ne diresti del corso migliore d'Italia super scontato?



Ciao Laura,

Come stai? Anche se **settember** segna il ritorno alla quotidianità, non ci siamo mai fermati, nemmeno ad agosto 🦵 .

E ora abbiamo una **gran notizia** che potrebbe davvero interessarti!

GeeksAcademy è pronta a lanciare i nuovi corsi, perfetti per chi come te:

- 🦵 È una studentessa ambiziosa che non si accontenta di un lavoro precario
- 🦵 Vuole uscire da un lavoro che non la soddisfa e puntare a una **cariera** di successo
- 🦵 Cerca un vero **upgradd** di competenze per il proprio futuro

E per te abbiamo preparato un'offerta davvero **speciale**! Se ti iscrivi ai nostri corsi entro il 30 settembre, potrai risparmiare **1000** euro su uno dei migliori corsi di sicurezza informatica disponibili in Italia! 🚀

👉 [Clicca qui IMMEDIATAMENTE per confermare l'iscrizione e riscattare i tuoi 1000 euro di sconto!](#)

Ma c'è di più! Giovedì **26 settembre**, alle ore 21, terremo un webinar gratuito intitolato: "Il piano del professore per una carriera stabile e ben pagata nel **2025**"

Durante questo evento di **50 minuti** (solo 50 minuti?), ti guideremo attraverso le strategie per costruire una carriera stabile e ben retribuita nel **2025**. Parleremo dei trend del mondo del lavoro, in particolare di come l'**Intelligenza Artificiale** sta rivoluzionando il settore IT, e ti presenteremo il nostro miglior corso di sicurezza informatica in Italia.

Non solo avrai la possibilità di conoscere in dettaglio il corso, ma scoprirai anche tutte le opportunità per **transformare** il tuo futuro professionale, con consigli pratici e strumenti per intraprendere una carriera di successo nel campo della **cyber securiti**.

Ricorda: iscrivendoti entro il **30 settembre**, potrai usufruire di uno sconto **esclusivo di 1000 euro** sul costo del corso! Non perdere questa occasione.

👉 [Clicca qui IMMEDIATAMENTE per confermare l'iscrizione e riscattare i tuoi 1000 euro di sconto!](#)

Se hai domande o desideri maggiori informazioni, **clicca su questo link** (link sospetto) o contatta la nostra assistenza.

A presto,

Il Team di GeeksAcademy

Descrizione dell'email modificata

L'email in esame sembra essere inviata da un'azienda di formazione (Geeks Academy) e propone sconti significativi per l'iscrizione a un corso di sicurezza informatica. Tuttavia, la presenza di diversi segnali può suggerire che si tratti di un tentativo di phishing.

Elementi sospetti e tipici di un'email di phishing:

1. **Errori ortografici e grammaticali:** L'email contiene una serie di errori grammaticali e ortografici, come "settember" al posto di "settembre", "cariera" invece di "carriera", e "cyber securiti" invece di "cybersecurity". Questi errori sono spesso un segnale di phishing, poiché le e-mail legittime di aziende professionali sono generalmente ben curate e prive di errori grossolani.
2. **Incoerenza nei nomi e nei dettagli:** Il nome dell'azienda è scritto in modo errato ("GeeksAcademyy" con doppia "y") in modo incoerente, il che è un indizio di non professionalità e può indicare che si tratti di un tentativo fraudolento. Inoltre, la data menzionata per il webinar, "26 settembre", potrebbe non corrispondere a un evento reale, e l'anno indicato in una parte dell'email è "20255", chiaramente un errore.
3. **Tono di urgenza e pressioni per cliccare:** Le frasi "Clicca qui immediatamente" e l'offerta di sconto esclusivo fino a 1000 euro creano un senso di urgenza artificiale, una tattica comune nei tentativi di phishing per spingere la vittima a cliccare sui link senza pensarci troppo. Il tono eccessivamente pressante, abbinato alla ripetizione di sconti e benefici, è un segnale classico di un attacco di phishing.
4. **Link sospetti:** L'email include più inviti a cliccare su link, spesso evidenziati come "Clicca qui immediatamente". I link in e-mail di phishing spesso conducono a siti web fasulli o infetti da malware, progettati per sembrare reali, ma creati con l'obiettivo di rubare dati personali.
5. **Offerte troppo vantaggiose:** L'offerta di sconti eccezionali, come 1000 euro di sconto su un corso, senza fornire dettagli chiari sull'offerta o condizioni trasparenti, è un classico esempio di esca utilizzata nei tentativi di phishing. Spesso, le offerte troppo vantaggiose rispetto al normale sono utilizzate per attirare le persone e spingerle ad agire rapidamente senza verificare la legittimità dell'email.