Avviso di sicurezza del 31/03/2021

Segnalazione di campagna di phishing in atto

Gent.Utenti,

pubblichiamo il presente avviso per segnalarvi una campagna malevola in atto in queste ore che ha come obbiettivo il furto di credenziali di Ateneo. In fondo a questo documento potete trovare alcune schermate di esempio.

La campagna malevola è un tentativo di phishing particolarmente insidioso poiché il link malevolo ed il sito di phishing sono ospitati su piattaforme cloud ad alta reputazione. In fondo a questo documento potete trovare un esempio della mail in questione (Figura 1 e Figura 2). Un esempio del link malevolo è visibile in Figura 3 ma possono essere possibili varianti. Il sito, visibile in Figura 4, ha un tema generico ma personalizzato con la dicitura "UNIMI" in modo da cercare di trarre in inganno la vittima.

La mail può essere riconosciuta come phishing da queste caratteristiche:

- Il mittente non proviene da **@unimi.it** ma da un dominio esterno (Vedi Figura 1 e Figura 2)
- La mail è di tono allarmistico e poco chiara: **"le tue email sono in quarantena!"**
- **Rimanda ad un sito al di fuori del dominio unimi.it,** in questo caso i link presenti rimandano ad un sito del dominio .dynamics . com. (vedi immagini allegate). Il link può solitamente essere visto in anteprima prima del click sostando con il puntatore del mouse sopra il bottone/link per alcuni secondi**.**

Il sito di phishing può essere riconosciuto come tale da queste caratteristiche:

- Il dominio che ospita il sito è chiaramente fuori dal dominio unimi.it.
- Il tema generale del sito non è coerente con quello adottato da Unimi: probabilmente viene usato per tentativi di phishing verso più organizzazioni.

Il Settore Cybersecurity, Protezione dati e Conformità della direzione ICT ha attuato le operazioni necessarie a contrastare le campagne in atto.

Se non avete inserito le vostre credenziali nel sito, non occorre fare nulla oltre che cancellare la mail.

Se al contrario avete cliccato involontariamente sul link indicato e inserito le vostre credenziali, vi chiediamo, di:

- Cambiare immediatamente la password attraverso il sito istituzionale: https://auth.unimi.it/password/
- Darne rapida comunicazione, sicurezza@unimi.it avendo cura di specificare l'orario indicativo in cui si è cliccato sul link malevolo e l'orario in cui è stato effettuato il cambio della password.

Si raccomanda sempre di prestare la massima prudenza su email contenenti link o allegati soprattutto se non sollecitate.

Altre informazioni su come migliorare la sicurezza dell'Ateneo possono essere trovate sul portale istituzionale al link: https://work.unimi.it/servizi/security_gdpr/118546.htm

I più cordiali saluti.

Nicla Diomede
Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano - Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Figura 1: esempio della mail di phishing

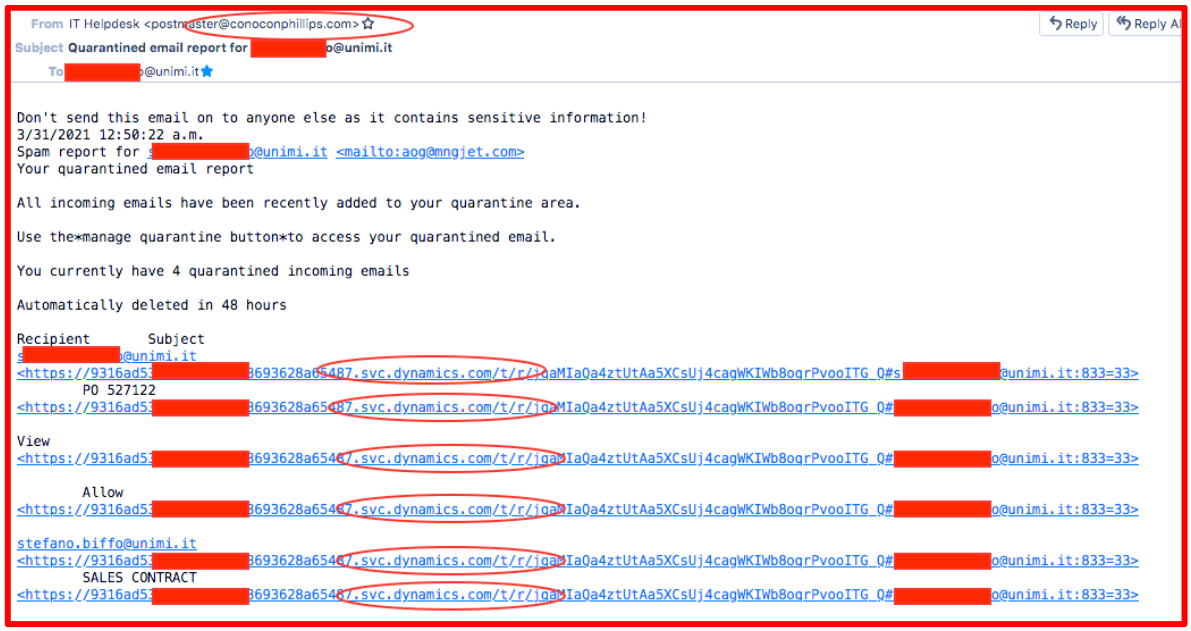

Figura 2: esempio della mail di phishing

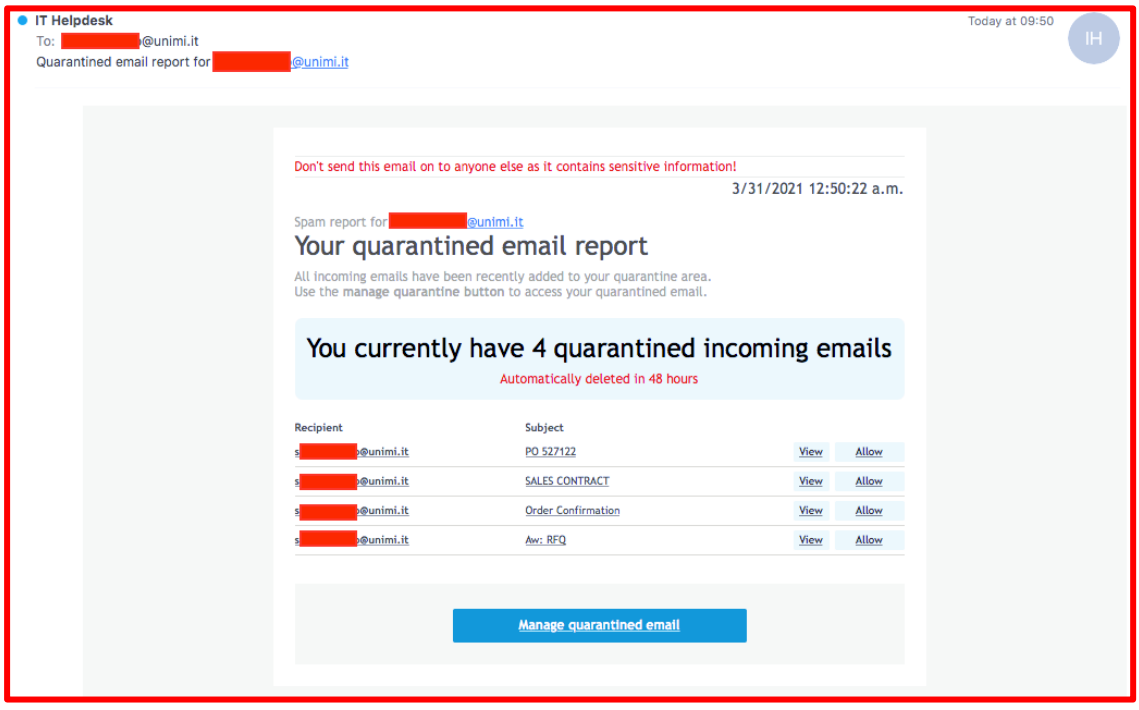

Figura 3: Url malevolo

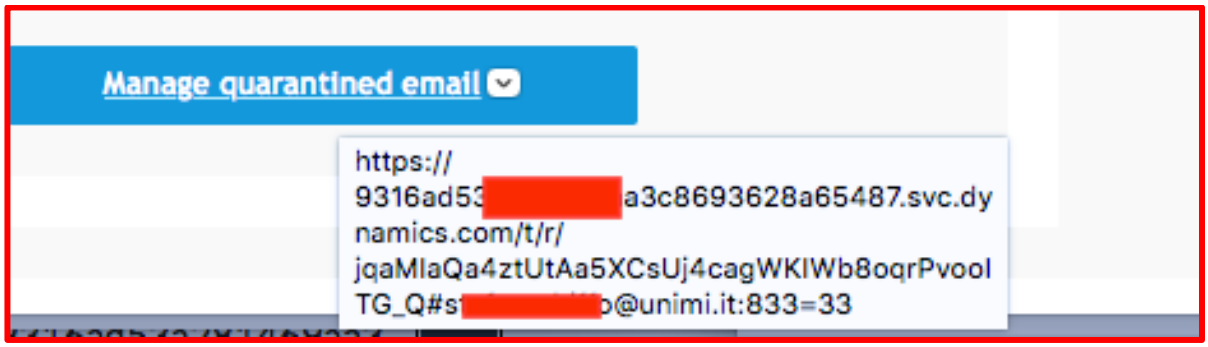

Figura 4: Sito malevolo