Avviso di sicurezza del 3 marzo 2020
Campagna di phishing in atto

Gentilissimi utenti,
pubblichiamo questo avviso per informarvi su un tentativo di phishing veicolato attraverso il servizio di posta dell'Ateneo mascherato da avviso di chiusura della casella di posta. In fondo a questo documento potete trovare alcune schermate di esempio.

Il tentativo di phishing è basato su un sedicente avviso di chiusura del servizio email (vedi figura 1). La mail può essere riconosciuta come phishing da queste caratteristiche:

- Il mittente non proviene da **@unimi.it** ma da un dominio ignoto *santhoshphotography.com*
- La mail è di tono allarmistico e poco chiara: "chiudiamo tutte le versioni precedenti di email"
- **Rimanda ad un sito al di fuori del dominio unimi.it**: in questo caso il bottone "AGGIORNA ORA" rimanda ad un sito *www.good[....]concept.it* di shopping online. Il link può solitamente essere visto in anteprima prima del click sostando con il puntatore del mouse sopra il bottone per alcuni secondi.

Una volta cliccato sul bottone si raggiunge la pagina di phishing vero e proprio (vedi figura 2). LA pagina è ospitata su un sito legittimo probabilmente compromesso e servito in HTTPS. Il sito di phishing può essere riconosciuto come sito di phishing da queste caratteristiche:

- **Il dominio che ospita il sito è chiaramente fuori dal dominio unimi.it**, in questo caso un sito di shopping probabilmente compromesso.
- Il tono è di tipo allarmistico, in questo caso è stato aggiunto addirittura un timer.
- Il titolo della finestra non coerente e contenente caratteri strani.
- Il tema generale del sito non ha nessun riferimento a unimi.it: probabilmente viene usato per tentativi di phishing verso più organizzazioni.

Se aveste cliccato involontariamente sul link indicato ed aveste inserito le vostre credenziali occorre:

- Cambiare immediatamente la password attraverso il sito istituzionale: https://auth.unimi.it/password/
- Darne rapida comunicazione a questo Ufficio, sicurezza@unimi.it

Se non avete cliccato, non occorre fare nulla oltre che cancellare la mail.

Si raccomanda di prestare la massima prudenza su email contententi link o allegati sopprattutto 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 piu cordiali saluti.

Ufficio Cybersecurity, Protezione Dati e Conformita' - Direzione Generale

Figura 1: email di phishing

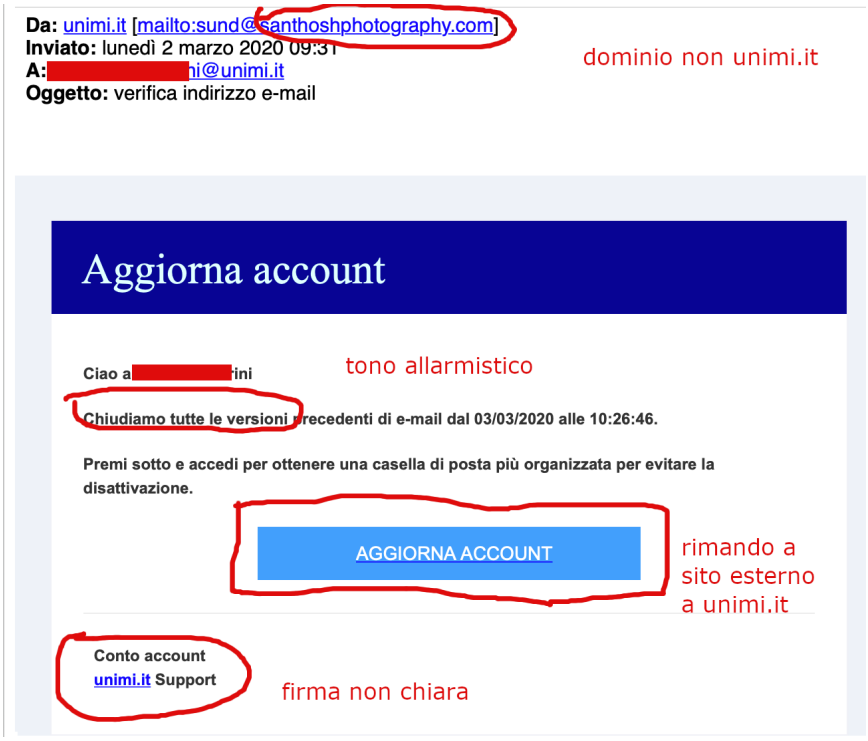

Figura 2: Sito di phishing