**Bollettino di sicurezza del 16 Settembre 2020**
**Lista di minacce in corso ed esempi di tentativi di phishing in atto**

Gentilissimi utenti,
pubblichiamo questo bollettino di sicurezza informatica per fornirvi elementi utili a riconoscere alcune tipologie di email malevole che in questi giorni stanno raggiungendo le nostre caselle di posta elettronica dell'Ateneo.
Ogni esempio è seguito da una analisi dettagliata come indicato nella guida disponibile al link che invitiamo tutti voi a consultare:

https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

Vi chiediamo di segnalare allo scrivente Settore Cybersecurity**,** Protezione Dati e all'indirizzo sicurezza@unimi.it esclusivamente mail ritenute sospette e che possono costituire un problema di sicurezza informatica. Per problemi di natura diversa, gli utenti sono invitati ad avvalersi dei canali e procedure previste per gli specifici servizi.

Ricordiamo che l'unico servizio abilitato al cambio della password della posta elettronica e degli altri servizi di ateneo è:

https://auth.unimi.it/password

e che per qualunque problema relativo al servizio di Posta Elettronica di Ateneo (ad esempio spazio esaurito, cancellazione di email e simili) è necessario aprire un ticket presso il Settore Servizi di Telecomunicazioni all'indirizzo: https://auth.unimi.it/servicedesktlc

Ricordiamo in ultimo che per problemi o dubbi inerenti il servizio di firma digitale è possibile scrivere a firma.digitale@unimi.it o consultare la pagina autenticata:

https://work.unimi.it/aree_protette/119597.htm

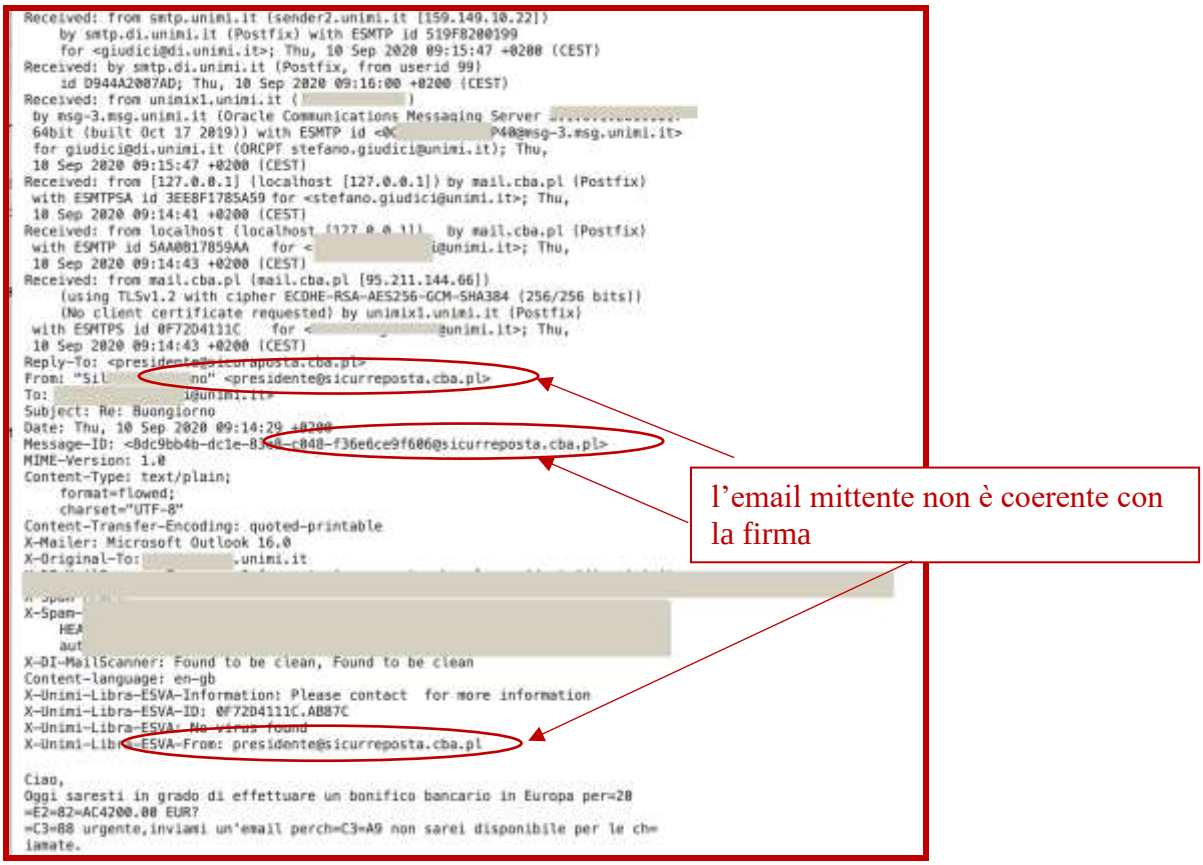
I più cordiali saluti.

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

## Recrudescenza del tentativo di frode tramite personificazione di un dirigente, direttore di Dipartimento

In questi mesi si è ripresentata una campagna tesa alla sottrazione di fondi di Ateneo attraverso l'impersonificazione del dirigente/direttore della struttura. La mail si presenta come una richiesta di disponibilità di fondi, come segue:


Se si esamina l'header[1] della mail si possono notare alcune anomalie:

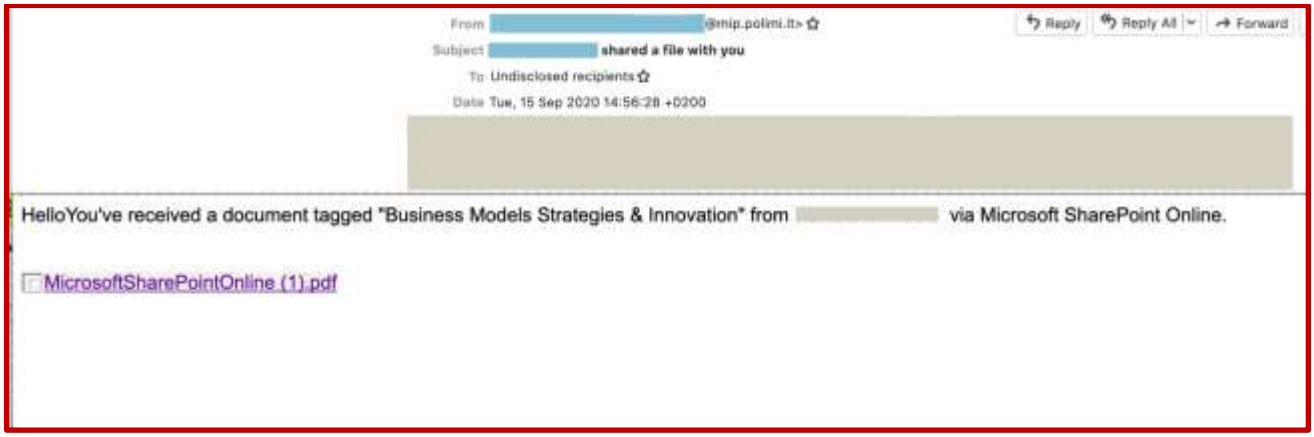



[1] Per esaminare l'header delle mail potete consultare:
https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

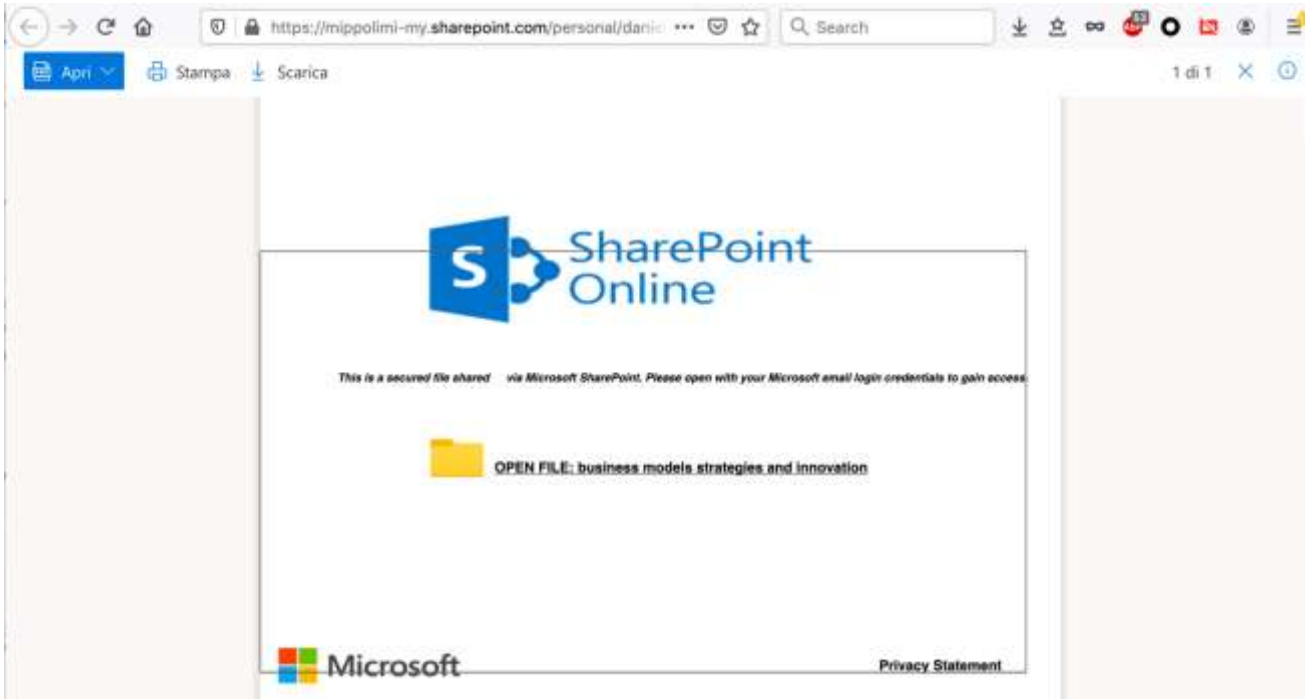
In questi casi è sempre opportuno verificare attraverso un altro canale di comunicazione la richiesta, es. chiamata a cellulare noto, interno, conferma da un collega parimenti coinvolto nella richiesta.

## Documenti office che rimandano a link malevoli

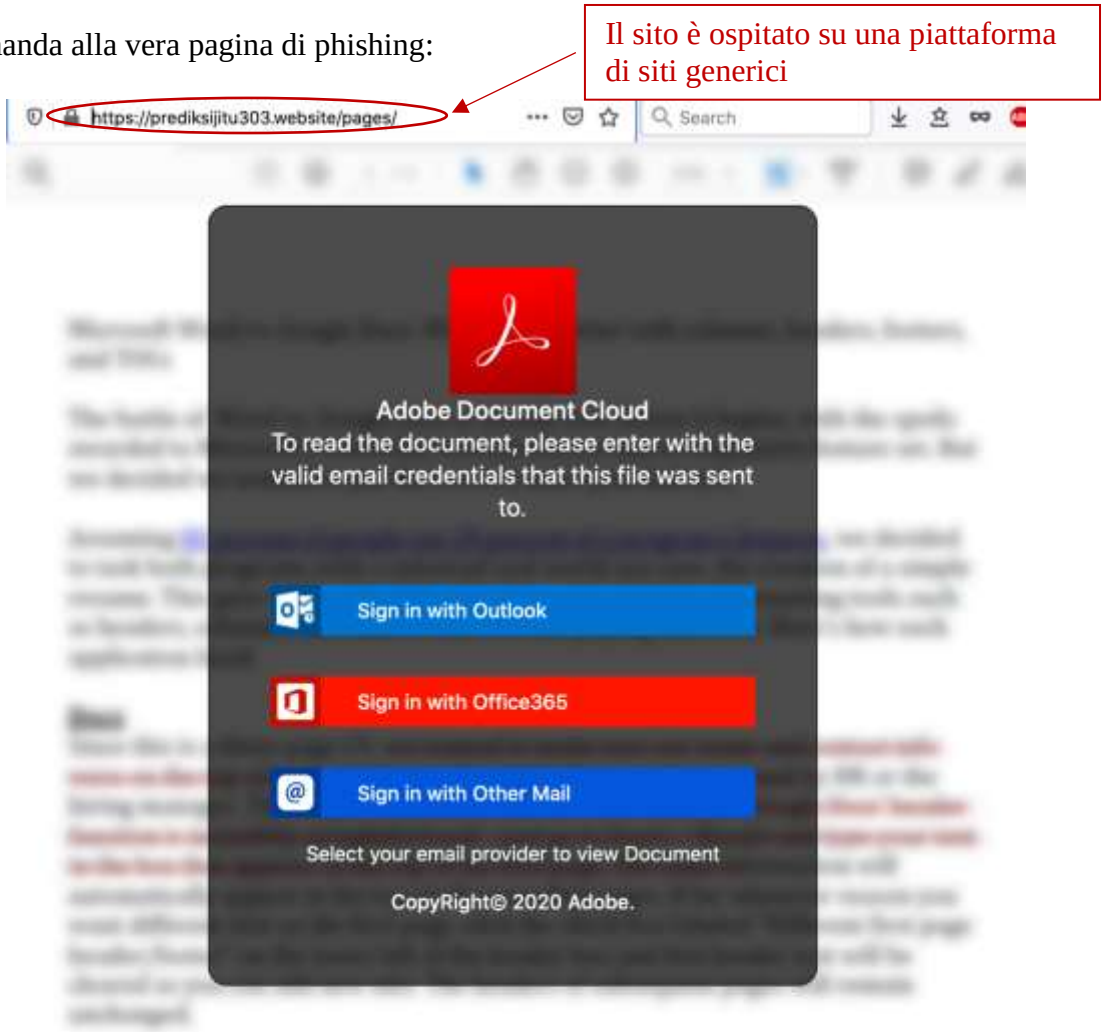
E' attiva in questi giorni una campagna di phishing veicolata attraverso mail che usa un elaborato sistema di rilanci tra documenti office condivisi via rete. L'attacco inizia con una mail simile alla seguente:




Il link nel corpo della mail rimanda ad una condivisione su cloud contenente un link malevolo:



Il link rimanda alla vera pagina di phishing:




E’ possibile notare che il sito è ospitato su una piattafoma di dubbia credibilità. In ogni caso la richiesta di credenziali di tipo così vario deve destare sospetto; in caso di dubbio potete inoltrare la mail, COME ALLEGATO per permettere di esaminare anche l’header nascosto a:

sicurezza@unimi.it