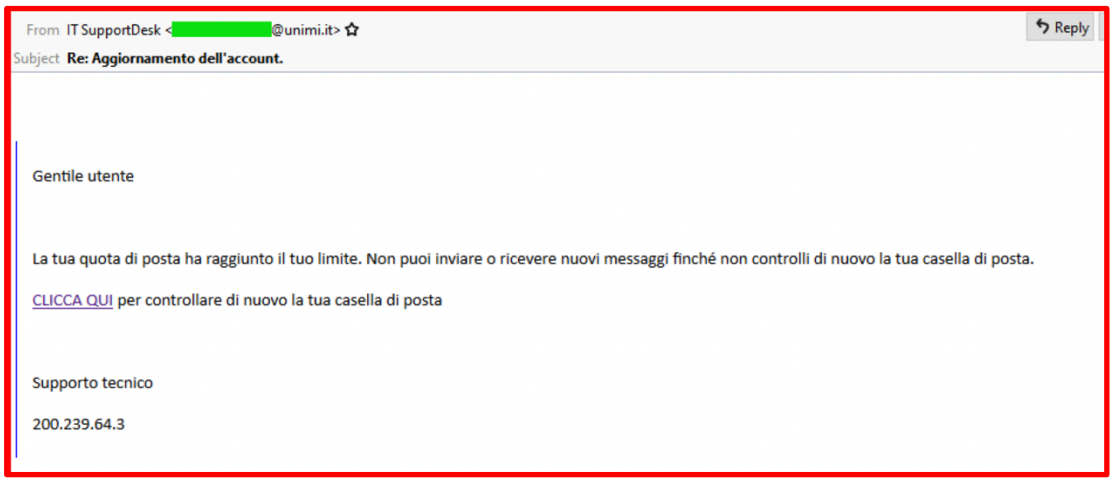
Segnalazione di campagna di phishing del 20 Ottobre 2020

Gentilissimi Utenti,
pubblichiamo questo avviso di sicurezza informatica di una campagna di phishing particolarmente insidiosa che in questi giorni stanno raggiungendo le nostre caselle di posta elettronica dell'Ateneo.

La mail si presenta come segue:



Il link indicato dalla mail è il seguente:

e rimanda ad un form malevolo ospitato da una piattaforma di form gratuiti, *emailmeform*.com.

La mail purtroppo è stata spedita da un account istituzionale compromesso e quindi risulta effettivamente spedita dall'Ateneo da un account di Ateneo, rendendo il riconoscimento della mail come malevola più difficile.

La mail di per sé non è pericolosa come neppure il form malevolo ospitato dalla piattaforma. Se non avete inserito le vostre credenziali in tale form l'unica azione richiesta è cancellare la mail.

Qualora abbiate inserito le vostre credenziali nel form malevolo occorre:

- Cambiare tempestivamente la password usando l'unico servizio di Ateneo deputato a questo scopo (verificate sempre l'url prima di inserire le vostre credenziali):

  https://auth.unimi.it/password

- Darcene riscontro scrivendo a sicurezza@unimi.it

Ricordiamo che le credenziali di Ateneo permettono l'accesso a svariati servizi di Ateneo contenente dati sensibili e personali; occorre quindi prestare nella scelta della password, che non deve essere troppo semplice e deve essere cambiata periodicamente, e nell'utilizzo della stessa, controllando sempre nella barra dell'indirizzo del browser l'url del sito in cui si stanno inserendo le

proprie credenziali. A questo indirizzo potete trovare una serie di guide per migliorare la propria sicurezza informatica:

https://work.unimi.it/servizi/security_gdpr/118582.htm

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:


[redacted]

Re: Buongiorno

To: [redacted]@unimi.it,

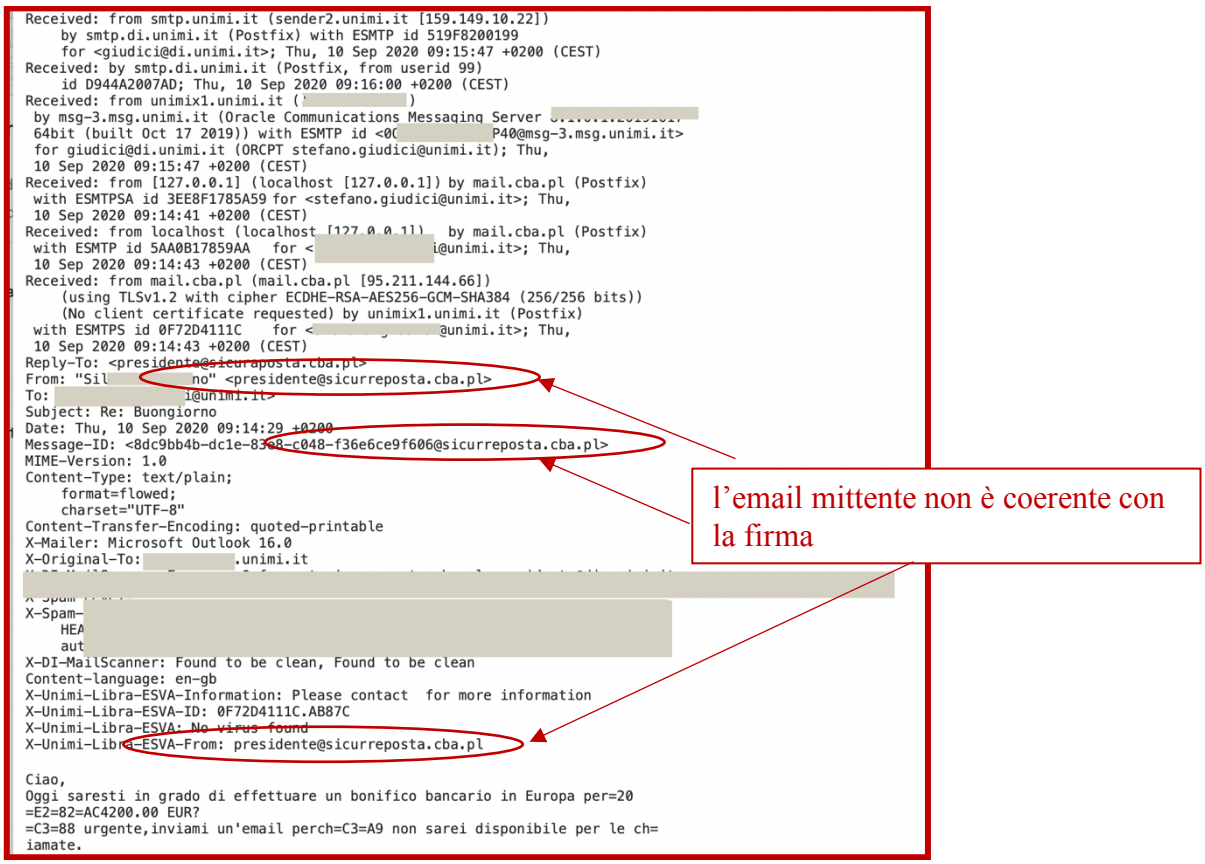
Reply-To: presidente@sicuraposta.cba.pl

Ciao,
Oggi saresti in grado di effettuare un bonifico bancario in Europa per €4200.00 EUR?
È urgente,inviami un'email perché non sarei disponibile per le chiamate.
Cordiali saluti,
[redacted]

--

Inviato dallo smartphone Samsung Galaxy.

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

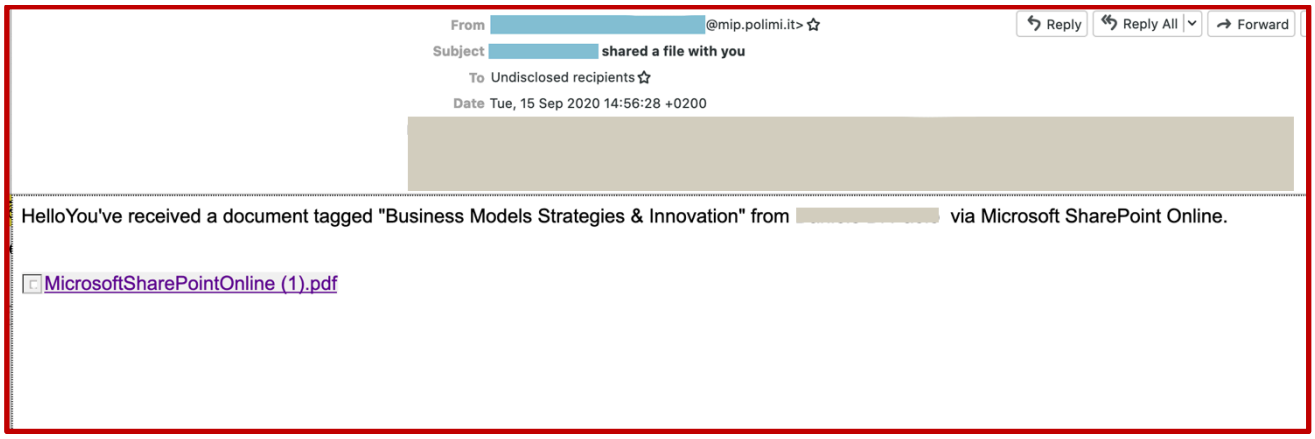


[1] Per esaminare l'header delle mail potete consultare:
https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

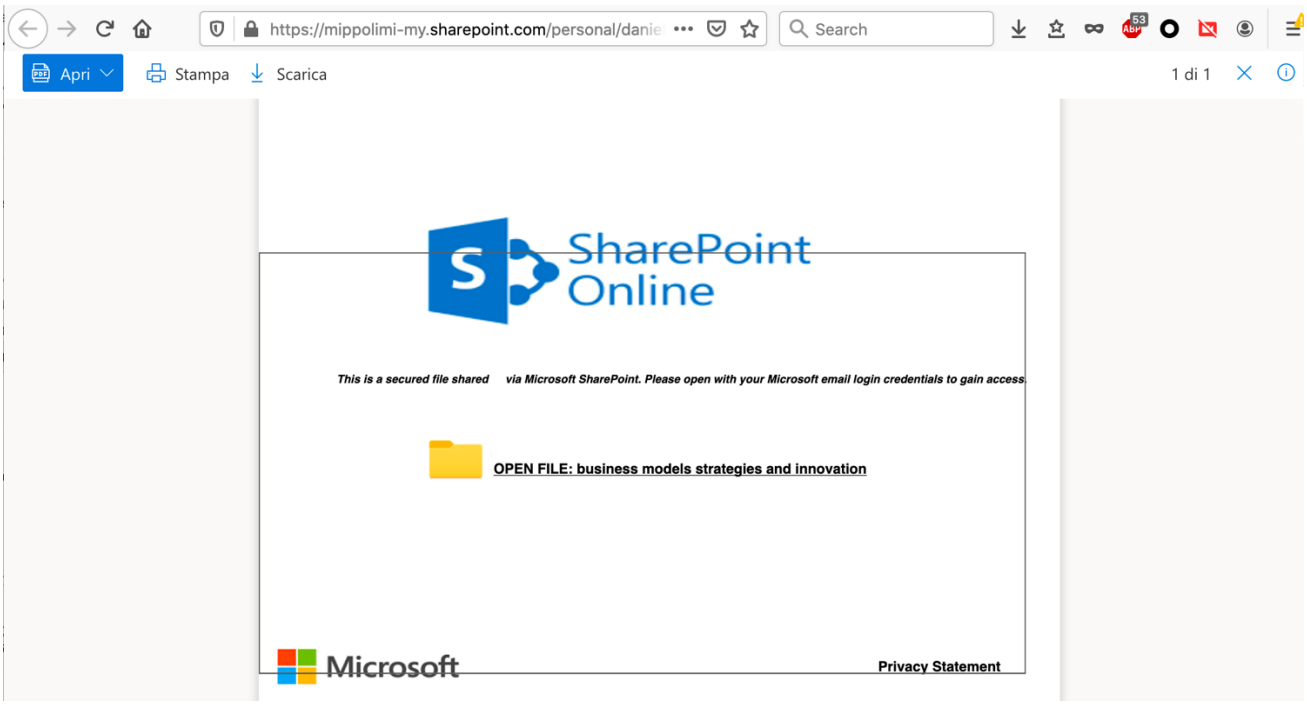
In questi casi è sempre opportuno verificare attraverso un altro canale di comunicazione la richiesta, es. chiamata a cellulare noto, interno, conferma da un collega parimenti coinvolto nella richiesta.

Documenti office che rimandano a link malevoli

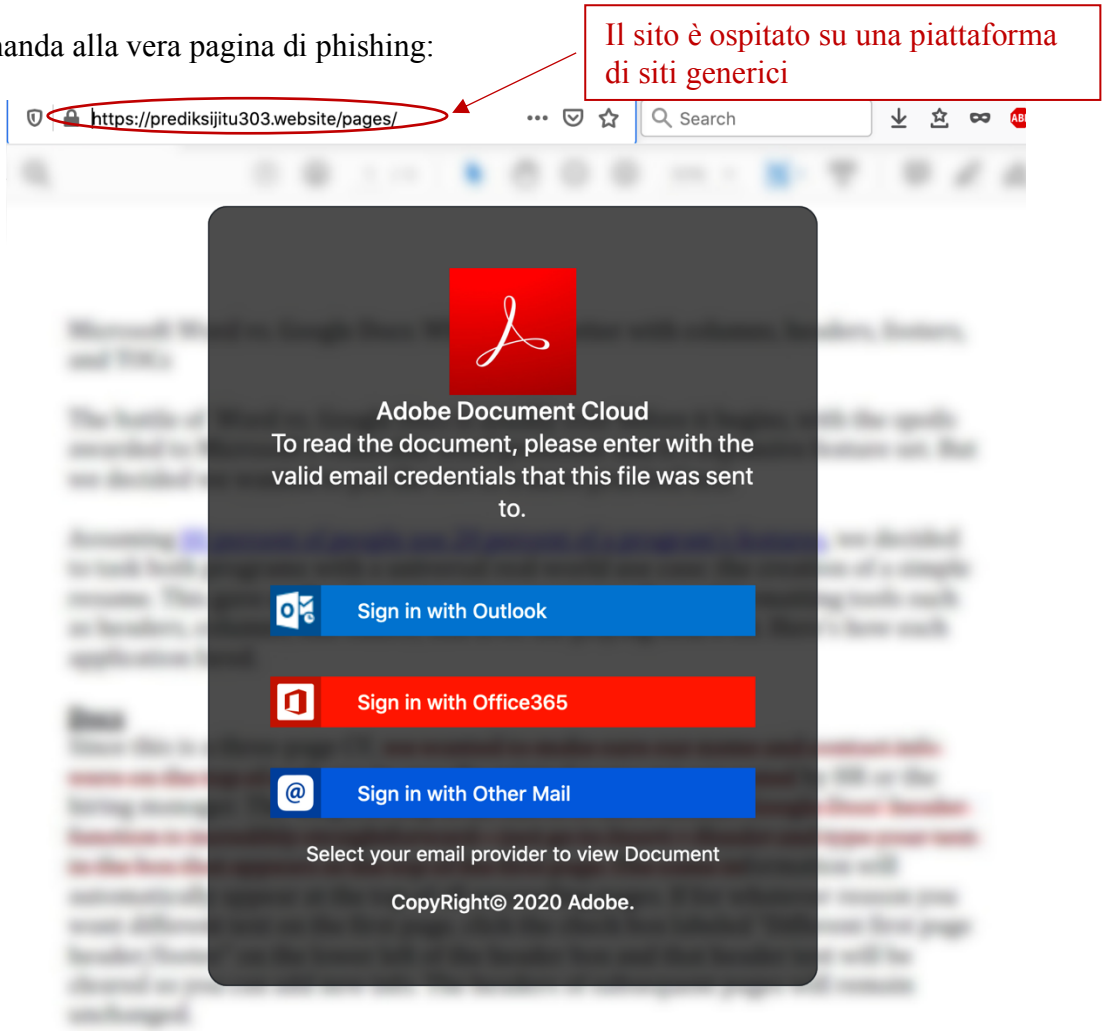
E' attiva in questi giorni una campagna di phishing veicolata attraverso mail che usa un elaborato sistema di rilanci tra documenti office condivisi via rete. L'attacco inizia con una mail simile alla seguente:



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