Avviso di sicurezza del 10.2.2020

Gentilissimi utenti,

Vi inviamo questa mail per informarvi su alcuni eventi connessi alla sicurezza ICT dell'Ateneo e sulle principali campagne malevoli in atto in questi mesi veicolate attraverso la posta elettronica di Ateneo.

Termine del supporto per Microsoft Window 7

Il data 14 gennaio 2020 è terminato il supporto al sistema operativo a Microsoft Window 7 così come era già accaduto per le versioni precedenti del sistema operativo di Microsoft. Questo fatto comporta che non saranno rilasciati ulteriori aggiornamenti per Window 7, compresi gli aggiornamenti di sicurezza su eventuali falle che venissero scoperte in futuro. Per tale motivo l'uso di tale sistema operativo sulle postazioni connesse alla rete di Ateneo costituisce un potenziale problema di sicurezza. Occorre quindi procedere quanto prima all'upgrade verso Microsoft Window 10 o altro sistema operativo supportato come indicato nelle direttive del Regolamento ICT.

Tentativo di phishing tramite impersonificazione del Magnifico Rettore.

In queste settimane è stata rilevata la presenza di una campagna malevola veicolata attraverso la posta di Ateneo avente come obbiettivo il furto delle credenziali di Ateneo. Come altre campagne che periodicamente colpiscono il nostro Ateneo, l'email della campagna si presenta come un messaggio inviato dal nostro Magnifico Rettore e recante come allegato un documento malevolo di tipo Microsoft Office docx (potete vedere in fondo a questo documento, in Figura 1, un esempio di come potrebbe presentarsi una mail di questo tipo). Il documento allegato consiste semplicemente in una immagine (vedi figura 2 come possibile esempio) che rimanda ad un link esterno all'Ateneo in cui è ospitata una pagina di phishing in cui è presente un form in cui viene chiesto di inserire le proprie credenziali. Poiché il documento è sostanzialmente innocuo (non sono presenti macro pericolose ed i siti che ospitano i phishing solitamente non sono ancora classificati come tali) è estremamente difficile sia per l'antispam che per l'antivirus di Ateneo rilevare questo tipo di minaccia.

Qualora doveste una mail come questa, inviarla a spam@unimi.it in modo da migliorare la capacità di riconoscimento dell'antispam di Ateneo. In ogni caso non dovete aprire il documento allegato.

Qualora aveste inavvertitamente inserito le vostre credenziali di Ateneo nel form malevolo occorre:

- effettuare un cambio repentino della password dell'account di Posta di Unimi, tramite il link:

  https://auth.unimi.it/password/

- segnalarlo all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it specificando a che ora è stata fornita la password (collegata a servizi Unimi) e ora di cambio password

Nel caso in cui la password fosse utilizzata anche su altri sistemi (interni o esterni al dominio Unimi) si richiede di cambiarla immediatamente su tutti i sistemi interessati, utilizzando un PC diverso da quello con cui si è acceduto al link.

In caso di dubbio potete inviare la mail sospetta come allegato a sicurezza@unimi.it.

Raccomandiamo a tutti voi di consultare frequentemente la sezione del portale di Ateneo dedicata alla sicurezza ICT e protezione dati e in particolare:

- **gli avvisi di sicurezza delle campagne malevole (tra cui quelle odierne) in atto al link https://work.unimi.it/servizi/security_gdpr/118606.htm**

- **le linee guida e indicazioni (tra cui quelle per proteggersi dal Phishing) al link https://work.unimi.it/servizi/security_gdpr/118582.htm**

Ulteriori raccomandazioni

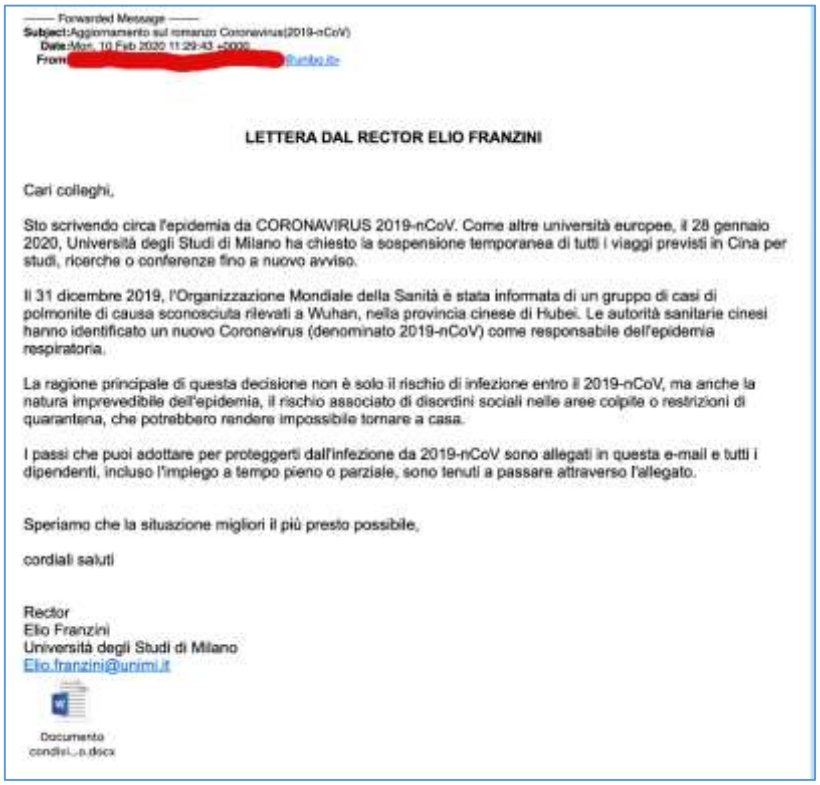
Si approfitta dell'occasione per ricordare altresì agli utenti quanto segue:

- utilizzare password per ciascun account univoche e robuste (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente);
- attivare la domanda di controllo per il recupero della password
- cambiare le password regolarmente e con frequenza almeno ogni 6 mesi;
- non riutilizzare la stessa password a breve distanza di tempo;
- mantenere sistema operativo e antivirus aggiornati.

Cordialmente


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


Fig.1: Esempio di truffa con impersonificazione (le parti in rosso sono state volutamente offuscate)



—— Forwarded Message ——
Subject:Aggiornamento sul romanzo Coronavirus(2019-nCoV)
Date:Mon, 10 Feb 2020 11:29:43 +0000
From: [redacted]

LETTERA DAL RECTOR ELIO FRANZINI

Cari colleghi,

Sto scrivendo circa l'epidemia da CORONAVIRUS 2019-nCoV. Come altre università europee, il 28 gennaio 2020, Università degli Studi di Milano ha chiesto la sospensione temporanea di tutti i viaggi previsti in Cina per studi, ricerche o conferenze fino a nuovo avviso.

Il 31 dicembre 2019, l'Organizzazione Mondiale della Sanità è stata informata di un gruppo di casi di polmonite di causa sconosciuta rilevati a Wuhan, nella provincia cinese di Hubei. Le autorità sanitarie cinesi hanno identificato un nuovo Coronavirus (denominato 2019-nCoV) come responsabile dell'epidemia respiratoria.

La ragione principale di questa decisione non è solo il rischio di infezione entro il 2019-nCoV, ma anche la natura imprevedibile dell'epidemia, il rischio associato di disordini sociali nelle aree colpite o restrizioni di quarantena, che potrebbero rendere impossibile tornare a casa.

I passi che puoi adottare per proteggerti dall'infezione da 2019-nCoV sono allegati in questa e-mail e tutti i dipendenti, incluso l'impiego a tempo pieno o parziale, sono tenuti a passare attraverso l'allegato.

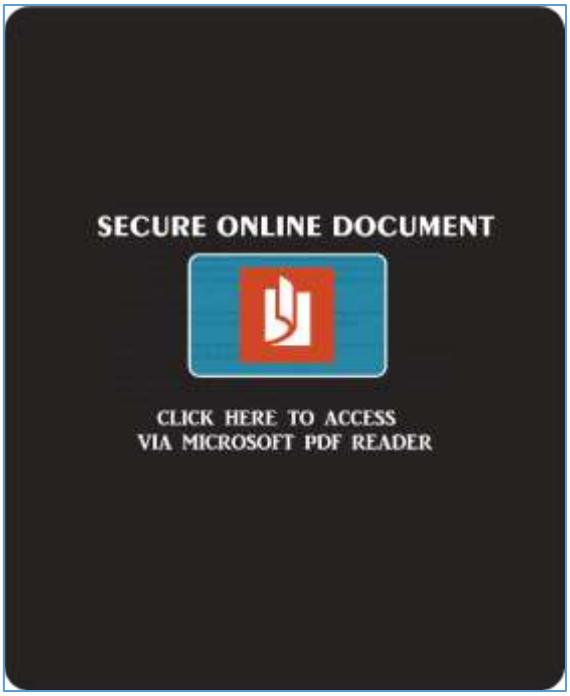
Speriamo che la situazione migliori il più presto possibile.

cordiali saluti

Rector
Elio Franzini
Università degli Studi di Milano
Elio.franzini@unimi.it

Documento
condivi...o.docx

Fig2: Esempio di immagine contenuta nell'allegato malevolo


SECURE ONLINE DOCUMENT
CLICK HERE TO ACCESS
VIA MICROSOFT PDF READER