Avviso di sicurezza del 24 marzo 2020
Campagna di phishing contro account Aruba e possibili disguidi con le mail di rinnovo della firma digitale

Gentilissimi utenti,
pubblichiamo questo avviso per informarvi delle campagne di phishing rivolte agli utenti dei servizi Aruba (attualmente fornitore della soluzione di Ateneo per la firma digitale) che periodicamente arrivano alle caselle di posta di Ateneo.

Chiediamo, perciò, agli di prestare particolare attenzione a questi attacchi in modo da non confonderli con le email legittime di rinnovo della firma elettronica che vengono spedite da Aruba agli utenti per cui la firma digitale sia in scadenza.

Di seguito trovate un esempio di come potrebbe presentarsi una mail di phishing che ha come target il furto delle credenziali per accedere al pannello di controllo dei servizi di Aruba:

Ciao Utente

Il tuo nome di dominio è attualmente registrato con Aruba.

Il nostro sistema di fatturazione ha rilevato che questo servizio è scaduto, non rinnovato.

Il tuo nome di dominio è stato sospeso.

Per riattivarlo, vai semplicemente sul nostro sito e usa l'ordine di rinnovo:

IL MIO ACCOUNT >

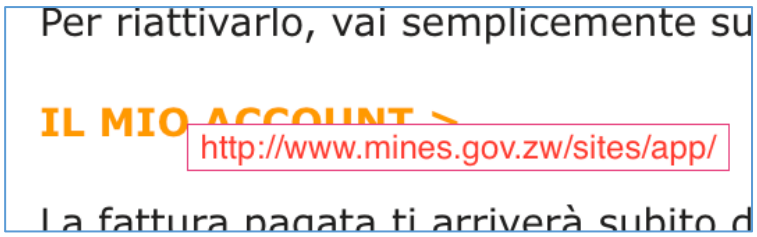
La fattura pagata ti arriverà subito dopo la convalida dell'ordine, confermando il rinnovo della royalty per il periodo prescelto.

IMPORTANTE: in caso di mancato pagamento entro 5 giorni, il tuo dominio potrebbe essere DEFINITAMENTE cancellato.

Per qualsiasi ulteriore informazione, il nostro supporto rimane a vostra disposizione.

Il tuo supporto.

A seconda del client di posta elettronica, è possibile evidenziare il link sottostante e verificare che il link punta ad un sito presumibilmente malevolo, nel caso specifico:



Circa il rinnovo delle firme digitali fornite dall'Ateneo, ricordiamo che le email di rinnovo verranno inviate solo ai possessori di firme digitali in scadenza. Per qualunque chiarimento sul rinnovo della firma digitale, informazione o appronfondimento sul servizio digitale, potete fare riferimento alla pagina dedicata sul portale di Ateneo all'indirizzo autenticato (richiede l'inserimento delle credenziali di Ateneo):

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

In caso di dubbi, potete contattare il servizio firma digitale all'indirizzo firma.digitale@unimi.it.

Infine all'indirizzo di seguito potete trovare due brevi guide con alcune semplici verifiche da fare per riconoscere le mail malevoli:

https://work.unimi.it/filepub/sicurezza_ict/Indicazioni%20utili%20a%20proteggersi%20dal%20Phishing.pdf
https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

Grazie per la vostra collaborazione a migliorare la sicurezza cibernetica dell'Ateneo.

I più cordiali saluti.

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