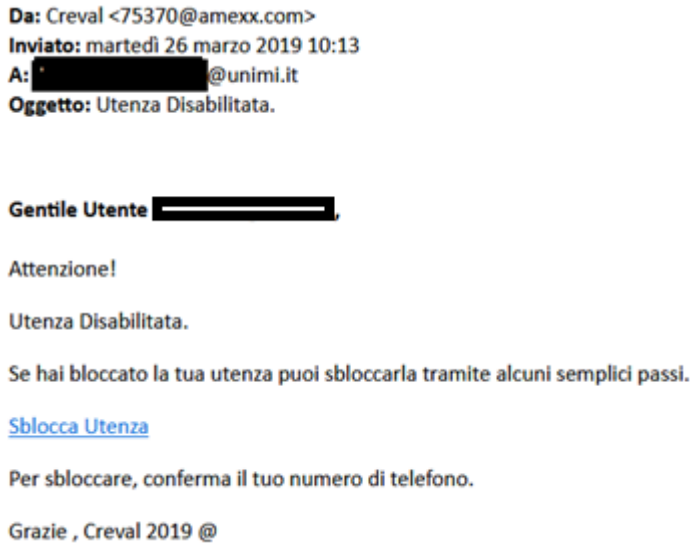
Campagna di phishing "Utenza Disabilitata"

Gentilissimi utenti,

è attualmente in corso una nuova campagna di phishing, veicolata tramite la posta elettronica, il cui obiettivo è quello di **sottrarre ai loro destinatari le credenziali** normalmente utilizzate per **accedere ad alcuni servizi erogati in rete.**

Le email in esame **vengono apparentemente inviate da Creval < <75370@amexx[.]com> e hanno come oggetto "Utenza Disabilitata".**

Ecco un esempio di mail:



Da: Creval <75370@amexx.com>
Inviato: martedì 26 marzo 2019 10:13
A: [redacted]@unimi.it
Oggetto: Utenza Disabilitata.

Gentile Utente [redacted],

Attenzione!

Utenza Disabilitata.

Se hai bloccato la tua utenza puoi sbloccarla tramite alcuni semplici passi.

Sblocca Utenza

Per sbloccare, conferma il tuo numero di telefono.

Grazie , Creval 2019 @

Si fa presente che sia l'oggetto che il testo delle email potrebbero presentarsi con alcune modifiche.

Ci troviamo di fronte ad un tentativo di truffa informatica, per cui invitiamo gli utenti interessati a:

- **non cliccare sul link riportato nell'email ricevuta;**
- **non rispondere all'email ricevuta;**
- **non compiere alcuna delle azioni suggerite nell'email ricevuta.**

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza della campagna in esame, ha attuato tutte le misure tecnologiche utili ad impedire dall'interno della rete di Ateneo la raggiungibilità del sito web malevolo linkato nel testo delle email in esame.

Tuttavia, **non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella casella INBOX, ve ne sia qualcuno che abbia cliccato sul collegamento malevolo da una**

rete esterna ad Unimi (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Chiunque abbia ricevuto la mail fraudolenta ed inserito le proprie credenziali sul sito malevolo deve:

- **segnalarlo** all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it

- **effettuare un cambio repentino della password dell'account Creval e contattare il servizio di assistenza di Creval per segnalare l'accaduto e seguire le loro istruzioni.**

Ricordiamo infine che l'Ufficio Sicurezza ICT nella sezione dedicata del portale di Ateneo pubblica:

- **gli avvisi di sicurezza della campagne malevoli 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**

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Staff Sicurezza ICT