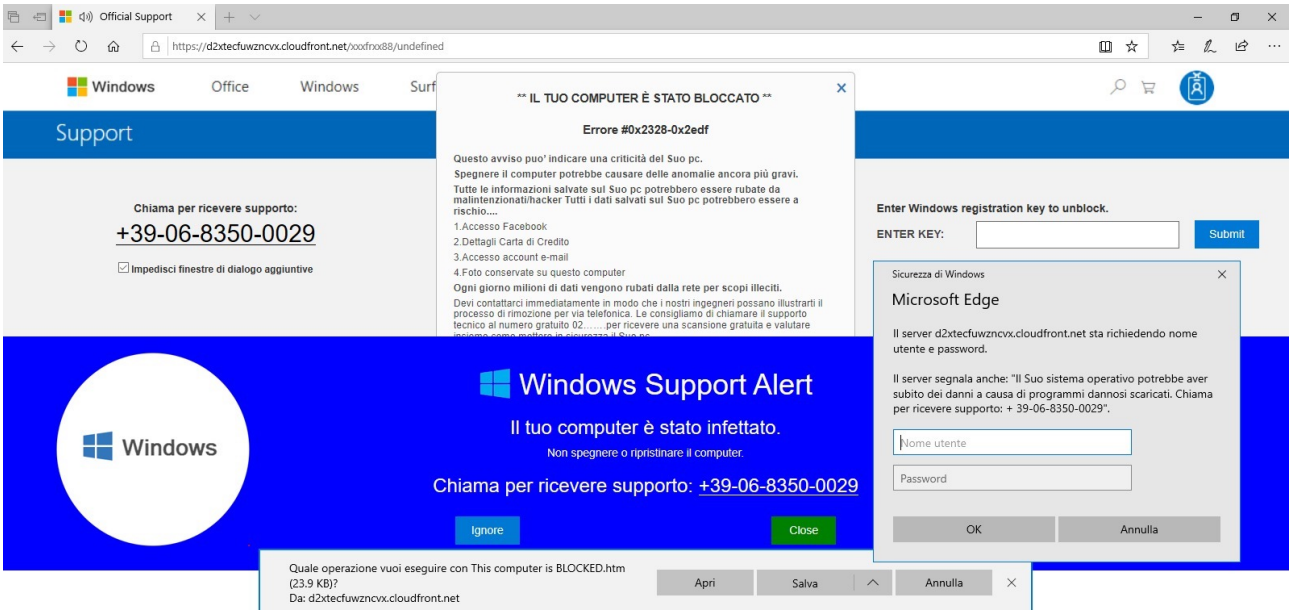
Avviso di sicurezza del 29 maggio 2020
Segnalazione di truffa on-line durante la navigazione su Internet

Gentilissimi utenti,
pubblichiamo questo bollettino di sicurezza per segnalarvi un insidioso meccanismo di truffa che potrebbe accadervi durante la navigazione su Internet. L'obbiettivo di questa truffa è vendervi un servizio di assistenza inutile e presumibilmente farvi infettare il PC realmente facendovi installare volontariamente un programma malevolo.

Cliccando su alcuni banner di pubblicità malevoli dall'apparenza innocua come "Pizzerie a Milano" o simili, che possono apparire ovunque su Internet anche all'interno di siti fidati come Google.com o Ansa.it, può capitare che il vostro computer venga bloccato con una schermata come questa:



accompagnata da una frase ad alto volume del tipo "Il vostro computer è stato infettato!!!".

Qualora vi dovesse capitare,

NON INSERITE ALCUNA CREDENZIALE NEL FORM

NON CHIAMATE IL NUMERO INDICATO

ma seguite una delle due procedure riportate di seguito.

Posso riavviare il pc perchè non ho nessun documento aperto ancora da salvare

Il modo più semplice per uscire dal blocco è riavviare il PC:

- Premere contemporaneamente il tasto “Windows”+ il tasto “R”
- Digitate nella casella che si apre il comando “shutdown”

Questo provoca il riavvio del computer. Al successivo riavvio il PC è di nuovo funzionante come prima.

Ho dei documenti ancora aperti che non posso perdere con il riavvio

Se non potete riavviare allora occorre chiudere il browser uin uso attraverso l’applicazione Task Manager (la procedura indicata qui sotto è quella per il sistema operativo Windows 10; per altri sistemi la procedura è simile):

- Premete contemporaneamente i tasti CTRL+ALT+CANC
- Individuate tra i programmi attivi il processo del browser che state usando
- Selezionate il processo del browser e premete il tasto End Task

Questo termina il browser e riporta il PC alla sua funzionalità normale.

Non riesco a fare nessuna delle due procedure indicate

Se non riuscite a completare nessuna delle due procedure sopra riportate, contattate il referente tecnico se è un dispositivo dell’Ateneo o il vostro servizio di assistenza se è un dispositivo personale.

In ogni caso non inserite credenziali di alcun tipo nel *form* che presumibilmente verrebbero memorizzate dall’attaccante e usate per altri attacchi e non chiamate il numero indicato.

Ricordiamo infine di mantenere aggiornato il vostro antivirus e di effettuare periodicamente scansioni complete del vostro PC; al link seguente è possibile scaricare l’antivirus di Ateneo:

https://work.unimi.it/servizi/servizi_tec/6562.htm

Sperando di avervi fornito indicazioni utili, vi ringraziamo per la vostra attenzione.

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