**MINISTERO DELL'ISTRUZIONE**
**Istituto Comprensivo Statale "Ai nostri caduti"**
**Via Pietro Nenni 2 - 20056 Trezzo sull'Adda (Mi)**
Scuola dell'Infanzia Trezzo-Scuole Primarie Trezzo e Concesa-Scuola Secondaria di I Grado Trezzo
Cod.Fisc.: 91546630152 - Cod.Mecc.: MIIC8B2008 - Cod.Univ.Uff.: UFY1XJ
TEL.: 02.90933320 - MAIL: MIIC8B2008@istruzione.it - PEC: MIIC8B2008@pec.istruzione.it
WEB: www.ictrezzo.edu.it

Circ. n. 150

Trezzo sull'Adda, 31/12/2020

**AI DOCENTI**
**ALLA DSGA**
**AI COLLABORATORI SCOLASTICI**
**AL PERSONALE DI SEGRETERIA**

Oggetto: **S.O.S. PHISHING PER CASELLE POSTA ELETTRONICA SCUOLA**

A questo tribolato 2020 mancava, per il mondo della Scuola, il botto finale: il comportamento riprovevole di coloro che stanno mettendo in atto **azioni di PHISHING** [*un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale]* **ai danni delle caselle di posta elettronica in ambito scolastico**.

**Riporto integralmente l'articolo di "ORIZZONTE SCUOLA" del 23 DICEMBRE SCORSO, a firma di FRANCESCA CAROTENUTO**, nel quale vengono fornite le opportune *informazioni* e indicate le più efficaci *precauzioni* per non essere coinvolti in questo disdicevole fenomeno.

Vi invito a prenderne visione.

## False mail che si fingono il Ministero dell'Istruzione, sono virus. Alcune raccomandazioni contro queste azioni di phishing

Il CSIRT MI [*Computer Security Incident Response Team-Ministero Istruzione*] ha reso noto di un'intensa azione di phishing rilevata ai danni del Miur [*Ministero dell'Istruzione*].
Si tratta dell'invio di messaggi di posta inviati a caselle istituzionali, provenienti da mittenti "verosimili", interni o esterni all'Amministratone e rispetto ai quali, nei testi, si richiede di scaricare o aprire file che sono in realtà virus in grado di recare grave infezione alle postazioni di lavoro utilizzate e, a cascata, pregiudizio sull'infrastruttura tecnologica del Miur.

Per quanto i mittenti possano essere noti, il messaggio può dunque essere malevolo. Si può riscontrare tale evidenza passando il puntatore del mouse sul nome dello stesso mittente e verificando eventuali anomalie nell'indirizzo mail visualizzato (si noterà un disallineamento con il nome visualizzato, stringhe alfanumeriche complesse o non interpretabili nel nome utente, dominio estero, ecc).
Non si devono assolutamente aprire tali file in allegato.
Qualora ciò fosse stato fatto, occorre procedere immediatamente alla scansione della postazione di lavoro utilizzata e, subito dopo, provvedere al cambio delle credenziali di tutti gli account utilizzati a fini lavorativi (la stessa posta elettronica, accesso al sistema informativo dell'istruzione, ecc).

In alcuni casi, si potrebbe avere già certezza della mail malevola, sempre da non considerare assolutamente o darvi seguito, qualora si ritrovasse in allegato un file di testo denominato 'Malware Alert Text.txt'; tale riscontro significherebbe che i sistemi di protezione del sistema informativo del Ministero sono riusciti ad intercettare l'attacco.
Non solo nella situazione della segnalazione in oggetto, bensì sempre, qualora doveste incorrere in messaggi mail del suddetto tipo, allo scopo di limitare l'occorrenza di incidenti di sicurezza, si devono seguire le seguenti raccomandazioni:
-non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
-non installare software sulle proprie postazioni di lavoro, soprattutto se a seguito di sollecitazioni via e-mail;
-non dare seguito alle richieste di e-mail sospette;
-nel caso in cui la richiesta provenga da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: l'e-mail era attesa? le frasi sono scritte con grammatica corretta? il software da installare ha un fine specifico? eventuali link nell'e-mail puntano a siti conosciuti? il mittente è corretto?
Inoltre si ricorda di scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi utilizzati per lavoro.
Nel caso di utilizzo del PC personale per telelavoro/smart working assicurarsi periodicamente:
-che il sistema operativo della propria postazione di lavoro sia aggiornato;
-che la propria postazione di lavoro sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
-che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti, e che, al momento della modifica, non siano apportate solo piccole modifiche (come ad esempio numerazioni progressive …).

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: Area Riservata> Computer Security Incident Response Team > Security Awareness) sono presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.
È fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

Per completezza, si allegano le Raccomandazioni dello CSIRT MI per la sicurezza.
Inoltre, ai fini tutela delle informazioni riservate di lavoro, ivi inclusi i dati personali propri e di terzi, si raccomanda fortemente di non lasciare mai il personal computer di lavoro incustodito o comunque non sotto il proprio diretto controllo.

<u>Raccomandazioni di sicurezza per l'Utente (smart working)</u>

Si fa raccomandazione agli Utenti, per quanto concerne il proprio PC di casa usato in telelavoro, di assicurarsi periodicamente:
-Che il sistema operativo della propria workstation sia aggiornato;
-Che la propria workstation sia dotata di antivirus e che questo sia aggiornato;
-Che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive, ecc.;
-Di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa.
Si consiglia inoltre di evitare di iscriversi a siti internet non riconducibili alla sfera lavorativa, ovvero utilizzando la casella di posta istituzionale; tali siti potrebbero infatti

essere poco sicuri nella protezione dei dati personali, con eventuali ripercussioni in violazioni all'interno della propria operatività lavorativa.

Raccomandazioni di sicurezza per l'Utente

Allo scopo di limitare l'occorrenza di incidenti di sicurezza si rappresentano le seguenti raccomandazioni:
-Non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungono da caselle di posta non note;
-Non installare software sulla propria postazione di lavoro gestita, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzione file;
-Non dare seguito alle richieste di e-mail sospette;
-Nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificare attentamente il contesto: ovvero se l'e-mail fosse attesa, le frasi siano scritte con grammatica e sintassi corretta, se il software di cui si richiede l'installazione abbia un fine specifico, se eventuali link nell'e-mail puntino a siti conosciuti, se il mittente fosse noto e/o corretto. In caso di dubbi rispetto a quanto sopra rivolgersi sempre conferma ai rispettivi referenti informatici.

**In Internet, cercando sotto la voce *phishing*, sono disponibili anche dei video-tutorial che offrono ulteriori strumenti conoscitivi e di prevenzione-contrasto del fenomeno.**

Grazie per l'attenzione. Un cordiale saluto.

IL DIRIGENTE SCOLASTICO
Dott.ssa Patrizia Santini

Atto firmato digitalmente ai sensi della Legge 82/2005

Documento informatico conservato all'interno del registro protocollo AOO/ufficio protocollo.


***un tempo nuovo, di giorno in giorno meno ostile e più amico AUGURI***