Istituto Comprensivo Statale
"BOCCADIFALCO - TOMASI DI LAMPEDUSA"
Via Dogali – 90135 Palermo - Tel. 091.6760335/6762490
C.F. 80028350827 - Codice IPA: UFAHZI
paic85600t@istruzione.it - paic85600t@pec.istruzione.it

CIRC. N.319 DEL 12.04.2023

I.C."BOCCADIFALCO-LAMPEDUSA"
Prot. 0003454 del 12/04/2023
I-1 (Uscita)

All'Animatore Digitale
Al team per l'innovazione digitale
Al personale docente
Al personale ATA
Ai genitori/tutori degli/lle alunni/e
Agli/lle alunni/e
Al DSGA
Sito – Sezione privacy

Oggetto: CSIRT-MI: raccomandazioni e indicazioni per la sicurezza

Le pubbliche amministrazioni sono sempre più oggetto di campagne miranti alla diffusione di malware attraverso l'utilizzo di posta ordinaria (PEO) e posta certificata (PEC) che costituiscono dei canali attraverso i quali sono condotti attacchi informatici anche di rilevante gravità. Anche per le PA le principali e più diffuse minacce sono rappresentate da eventi di phishing e distribuzione di vari tipi di malware, come i ransomware e i trojan, specializzati nel carpire dati ed altre informazioni sensibili tra cui le credenziali d'accesso ai diversi servizi telematici.

Con lo scopo di prevenire questo tipo di attacchi CERT-PA (Computer Emergency Response Team – Pubblica Amministrazione) ha diffuso nel novembre del 2019 il bollettino B006-191119 con le raccomandazioni per limitare la proliferazione dei maleware nei sistemi informatici delle PA.

La gravità del problema è oggi evidenziata anche dal CSIRT-MI (Computer Security Incident Response Team – Ministero dell'Istruzione) che il primo Aprile 2021 ha diffuso una nota con raccomandazioni ed indicazioni per la sicurezza informatica. In essa viene evidenziato come l'utente finale rappresenta la migliore barriera per bloccare una possibile minaccia e come, viceversa, l'inosservanza delle buone prassi di sicurezza da parte delle persone permette invece l'avvio della catena di infezione del malware.

Le buone prassi di sicurezza

La nota CSIRT-MI riporta in due allegati quelle che sono le buone prassi di sicurezza cui tutto il personale scolastico deve attenersi:

- 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'email puntino a siti conosciuti, se il mittente fosse noto e/o corretto;
- scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi che accedono alla Posta Elettronica;

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.

CERT-PA – raccomandazioni di sicurezza

Cogliamo l'occasione per ricordare le raccomandazioni di sicurezza che aveva invece impartito CERT-PA con il suo bollettino B006-191119

1. Modificare le credenziali delle caselle, con cadenza trimestrale, adottando requisiti di complessità;
2. Non ignorare eventuali attività sospette rilevate, in ingresso o in uscita, dalle caselle;
3. Al manifestarsi di una sospetta anomalia o attività legata ad accessi non autorizzati in una casella, provvedere subito a cambiare la password del servizio, quindi allertare il supporto tecnico di riferimento;
4. Utilizzare la protezione di un antivirus accertandosi che sia sempre attivo ed aggiornato e non ignorando la presenza di avvisi di sicurezza;
5. Eseguire periodicamente una scansione antivirus della propria postazione/dispositivo ed in particolare degli allegati che si desidera aprire;
6. Se si ritiene di aver aperto un allegato non sicuro, eseguire una scansione AV completa quindi utilizzare, per ulteriore accertamento, un antivirus esterno come i "rescue disk" che permettono di sfruttare un'unita CD, DVD, USB per esaminare il sistema dall'esterno;
7. Accertarsi che il sistema operativo abbia tutti gli aggiornamenti di sicurezza rilasciati e che siano attivi gli "Aggiornamenti Automatici", in modo da garantire l'applicazione delle correzioni di sicurezza non appena disponibili;

8. Evitare di cliccare su un link quando punta su destinazioni non note (posizionando il puntatore del mouse sul link senza cliccare dà in genere la possibilità di vedere l'indirizzo contenuto nel link stesso);
9. Non aprire allegati e file provenienti da mittenti sconosciuti senza gli opportuni controlli del caso;
10. In genere, diffidare da comunicazioni che richiedono l'esecuzione di azioni non richieste o che invitano ad inserire credenziali di accesso, o altre informazioni sensibili, all'interno di form online in quanto, con altissima probabilità, si tratta di pagine fasulle appositamente predisposte per catturare le informazioni.
11. Verificare regolarmente sul sito del CERT-PA l'emergere di campagne o attacchi attivando, ove rilevato un caso analogo, le contromisure suggerite.

CSIRT-MI ha anche realizzato un video di 6 minuti per illustrare in modo semplice i pericoli del phishing: https://www.youtube.com/watch?v=oggknseErEU&t=23s

La Dirigente Scolastica
Rosaria Corona
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2 del D.L.vo 39/93