I.I.S. Alessandro Lombardi
Largo Capone, 82011 Airola (BN)
Indirizzi: Liceo Classico – Liceo Scientifico – Liceo Musicale - ITE – IPIA – Moda
Presidenza: Tel. 0823711296, Segreteria Tel. Fax 0823-711263
E-Mail: bnis00800r@istruzione.it sito web: www.iislombardi.edu.it

CSIRT
Computer Security Incident Response Team
Ministero dell'Istruzione

Raccomandazioni e Indicazioni per la Sicurezza

01 Aprile, 2021

Gentile Utente,

anche in questo ultimo periodo stiamo rilevando il blocco di mail di phishing indirizzate al personale ministeriale da parte dei sistemi di sicurezza del MI; tali messaggi sono indirizzati a caselle di posta elettronica istituzionali, provenendo da mittenti 'verosimili' e rispetto ai quali nei testi si richiedono azioni di accesso a pagine web/download file che in realtà possono recare problemi alla postazione di lavoro e, a cascata, all'infrastruttura tecnologica del MI.

Con la stessa frequenza inoltre, si rileva anche attività anomala da parte di alcune caselle di posta istituzionali che inviano mail di spam all'insaputa dell'Utente titolare del account, la cui compromissione il più delle volte è dovuta ad infezioni da virus sulle postazioni di lavoro o sui dispositivi utilizzati per l'accesso.

La causa delle suddette situazioni risiede sicuramente in un'intensa e sempre più sofisticata attività da parte dei cyber attaccanti in internet, interessati a carpire informazioni riservate e sensibili, personali e/o dell'Organizzazione, ma anche e soprattutto in comportamenti da parte delle persone non sempre in linea con le buone prassi di sicurezza e le indicazioni in tal senso da parte dell'Amministrazione.

Si ribadisce allo scopo quindi di:

- **scansionare periodicamente per la ricerca virus le postazioni di lavoro ed i dispositivi utilizzati per lavoro;**
- nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:

- che il sistema operativo 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 di posta e strumenti di lavoro 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).

- **non usare l'account di lavoro per registrarsi in internet per fini non riconducibili alla sfera di lavoro ed evitare di salvare le password nel browser di navigazione Internet;**

CSIRT-MI

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.

CSIRT-MI

Raccomandazioni di Sicurezza Posta Elettronica

Allo scopo di limitare l'occorrenza di incidenti di sicurezza sulla casella di Posta Elettronica si rappresentano le seguenti raccomandazioni:

1. non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
2. non installare software sulla propria postazione, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzione file.
3. non dare seguito alle richieste di e-mail sospette;
4. 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;
5. di scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi che accedono alla Posta Elettronica;

nel caso di utilizzo del PC personale (telelavoro/smart working) si raccomanda di assicurarsi periodicamente:

6. che il sistema operativo della propria workstation sia aggiornato;
7. che la propria workstation sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
8. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale.
9. al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc...;
10. di eseguire il backup periodico dei dati elaborati nell'ambito della sfera lavorativa.

Si consiglia inoltra 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.