SINTESI DI

Raccomandazioni e Indicazioni per la Sicurezza

del Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri

Il CSIRT emette preallarmi, allerte, bollettini e divulga informazioni alle parti interessate in merito a rischi e incidenti, al fine di supportare le attività di sensibilizzazione, prevenzione e gestione del rischio cyber.

In data 05 luglio, il CSIRT ha predisposto delle Raccomandazioni per la Sicurezza Informatica, che il Ministero dell'Istruzione ha poi inoltrato a tutte le scuole.
Il presente documento ha lo scopo di fare una sintesi degli aspetti fondamentali di cui l'utente deve tener conto, raccomandando comunque di visionare attentamente gli allegati qui sintetizzati.
Allegati del CSIRT:

- Sicurezza della Postazione di Lavoro Utente
- Raccomandazioni Sicurezza Posta Elettronica

Raccomandazioni e Indicazioni per la Sicurezza

Il CSIRT ha rilevato nell'ultimo periodo un flusso di email phishing (messaggio fraudolento creato in modo da sembrare autentico/verosimile) indirizzate a caselle di posta istituzionali; allo stesso modo, partono da caselle di posta istituzionali email spam (messaggi indesiderati e non autorizzati) all'insaputa dell'utente titolare dell'account.

USO DI PASSWORD E DISPOSITIVI*

Al proposito, il CSIRT ribadisce alcune raccomandazioni:

- Effettuare periodicamente una **scansione antivirus** e ricerca **malware**
- Avere un **sistema operativo aggiornato**
- Dotare il pc di un **sistema antivirus aggiornato**
- Scegliere **password complesse**, **non facilmente individuabili**, **diverse per ogni servizio** ed **evitare di aggiornarle facendo solo piccole modifiche** (ed es. modificando solo un numero o un carattere)
- **Non usare l'account di lavoro** per **registrarsi a siti di uso personale**
- **Non memorizzare le password** nel **browser di navigazione**
- **Non lasciare incustodita** la **postazione di lavoro**
- Usare con cautela **supporti esterni** (usb, hard disk) ed **effettuare una scansione** al momento della connessione
- **Eseguire un backup periodico** di tutti i dati ad uso lavorativo

GESTIONE POSTA ELETTRONICA*

- **Non aprire** file non attesi e/o di dubbia provenienza
- **Non installare software** sulla propria postazione da **collegamenti non sicuri** (link di accesso ad altre pagine o di esecuzione file)
- **Non dare seguito** alle **richieste incluse nei messaggi sospetti**
- **Verificare attentamente** richieste provenienti dal personale tecnico dell'Amministrazione

***NOTE**

Consiglio: quando in una email o in un documento è presente un link, se andate sopra il link con il mouse SENZA cliccare, dovreste vedere in basso nell'angolo sinistro (o nei pressi del collegamento) dove punta quel link. Nel caso di collegamenti fraudolenti, quasi sicuramente vedrete un indirizzo strano e di dubbia attendibilità.

Le raccomandazioni di sicurezza sono da applicare sia per l'utilizzo di pc scolastici che di pc personali in caso di smart working.

Per le operazioni tecniche che l'utente non riesce ad attuare e/o che non rientrano nelle proprie competenze, rivolgersi ai rispettivi referenti informatici (assistenti tecnici, amministratore di sistema …) individuati dalla scuola.

Si raccomanda di seguire scrupolosamente le Raccomandazioni del CSIRT e tutte le altre indicazioni da noi fornite nel Manuale Privacy, raggiungibile al seguente link:

MANUALE PRIVACY

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'email 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.

Raccomandazioni 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.