



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 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.