Nota a cura della Commissione Informatica dell'Ordine degli Avvocati di Torino in merito alla diffusione dei nuovi virus informatici- ransonware e alle misure di prevenzione da adottare

Con la presente nota s'intende porre l'attenzione dei Colleghi sul virus informatico WannaCry, diffusosi a partire dal 12 maggio scorso.
Si tratta di un c.d. "ransomware", cioè un programma che cripta i file presenti sul computer, rendendoli cioè accessibili solo inserendo una password fornita dietro pagamento di una somma di denaro (con la precisazione che si dubita che tale password venga realmente fornita).

Poiché il virus sfrutta un bug del sistema operativo Windows, la sua diffusione può avvenire anche senza che l'utente compia alcuna azione (come invece nei ransomware tradizionali).

Chiarito quindi che il virus colpisce esclusivamente i computer con sistema operativo Microsoft Windows (non quindi gli altri sistemi operativi), si invitano gli iscritti che utilizzino tale sistema operativo, o abbiano nella propria rete computer con installato tale sistema operativo, a:
- assicurarsi che gli aggiornamenti del sistema operativo (Windows update) siano attivi e siano effettuati regolarmente;
- eventualmente, applicare manualmente l'aggiornamento di sicurezza di Windows del 14 marzo 2017 reperibile...
-- per i sistemi operativi ancora mantenuti da Microsoft, all'indirizzo:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
(basterà selezionare il sistema operativo interessato, scaricare l'aggiornamento, eseguirlo e attendere il completamento dell'installazione)
-- per le versioni di Windows considerate obsolete (come Windows XP o Windows Vista), all'indirizzo:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
(seguendo il link al paragrafo "Download localized language security updates")
- assicurarsi che anche collaboratori e colleghi di studio osservino le medesime cautele
- valutare soluzioni di backup periodico su supporti non collegati alla rete (ad esempio hard disk esterni);
- assicurarsi di avere software antivirus e antimalware regolarmente aggiornati (si rammenta che esistono anche prodotti gratuiti e open source).

In ogni caso si consigliano le medesime cautele utilizzate per difendersi dai normali ransomware (non aprire file eseguibili da fonti sconosciute o solo apparentemente conosciute) e, se si è dotati di assistenza sistemistica o di informatica, di valutare cautele ulteriori (quali la disattivazione dei servizi oggetto di attacco, se non utilizzati: vedasi le ultime righe dell'articolo pubblicato dalla Polizia di Stato a questo link).