Gentile utente,

negli ultimi tempi si stanno verificando campagne massive di attacchi perpetrati per mezzo della posta elettronica, anche certificata, che sono principalmente volte alla diffusione di malware, in particolare “ransomware” in grado di rendere inutilizzabili le postazioni di lavoro e di causare la perdita dei propri dati.

Anche per gli utenti del dominio @istruzione.it la numerosità e la frequenza di tali attacchi è significativa.

Le tecniche utilizzate per ingannare l’utente ed inoculare il malware sono sempre più raffinate, presentano messaggi “verosimili” e si basano fondamentalmente sull’apertura di allegati infetti, anche spesso veicolati da caselle PEC precedentemente compromesse, o sulla selezione di link malevoli.

A questo proposito si ricorda che non è possibile applicare il controllo Antispam ai messaggi di posta elettronica certificata perché comporterebbe il rischio di considerare come Spam messaggi desiderati (lo scopo principale di un servizio di Posta Elettronica Certificata è quello di garantire l’invio e la consegna di un messaggio di posta prescindendone dal contenuto).

La prevenzione è l’arma più importante per contrastare tale fenomeno che sfrutta soprattutto la distrazione o la fretta degli utenti nell’apertura delle email e dei suoi allegati, pertanto si raccomanda:

· di prestare la massima cautela quando si ricevono email (normali o PEC) di provenienza sospetta o da mittenti sconosciuti;

· di diffidare dei messaggi che richiedono una nostra azione urgente circa situazioni importanti, ad esempio notifiche di procedimenti giudiziari piuttosto che comunicazioni urgenti di gestori telefonici, fornitori di servizi, aziende di spedizioni o agenzie ed enti statali come Agenzia delle entrate, enti di riscossione tributaria ecc…;

· di attendere anche 48 ore prima di aprire un allegato se non si è sicuri della provenienza del messaggio, per dare modo all'antivirus di aggiornarsi circa l'esistenza di nuove minacce. Prima di aprire l’allegato, scaricarlo in una directory locale e sottoporlo alla scansione antivirus;

· di evitare, nel caso di documenti Office all’apparenza legittimi, l’esecuzione delle macro;

· di prestare attenzione ai file in formato compresso (ZIP);

· di evitare di selezionare link contenuti nel corpo del messaggio a meno di essere sicuri dell'identità del mittente;

· di controllare che le connessioni proposte nei link contenuti nel corpo del messaggio siano di tipo HTTPS e conducano a siti noti, verificando che all'apertura della pagina il sito sia effettivamente quello "ufficiale";

· di non utilizzare la casella di posta istituzionale (@istruzione.it) per attività non inerenti l'ambito lavorativo;

· di eseguire backup regolari dei dati più importanti avendo cura di utilizzare dispositivi per il backup non infetti e che non contengano altri file non attendibili;

· di interrompere quanto prima il collegamento di rete nel caso di sospetta o certa infezione;

· di procedere ad un costante aggiornamento del proprio antivirus e alla verifica che l'aggiornamento automatico sia attivo e funzionante.

Altre raccomandazioni valide per aumentare il livello di sicurezza dei propri dati ed utili a contrastare gli attacchi di tipo "phishing" (frode informatica realizzata tramite invio di email contraffatte volte a carpire dati dell'utente) sono:

· non condividere i propri dati o i dati istituzionali con interlocutori non "certi" (verificando che il mittente della mail sia chiaro e noto);

· non inserire credenziali utente (utenza e password) in risposta a mail provenienti da banche e/o compagnie "ufficiali"; in genere queste aziende non chiedono mai informazioni del genere via mail; eventualmente verificare la veridicità della mail telefonando all'azienda;

· utilizzare password robuste (almeno di 14 caratteri) e cambiarle con frequenza

· non utilizzare MAI la stessa password per diversi servizi

Ministero dell'Istruzione, dell'Università e della Ricerca

D.G. Contratti, Acquisti, Sistemi Informativi e Statistica