Brescia, lì 20.02.2025

OGGETTO: CYBER SICUREZZA – INDICAZIONI PER RIDURRE LA POSSIBILITA' DI ATTACCHI HACKER

Gentili Clienti,

sebbene non attinente alla nostra professione, poiché ultimamente si stanno verificando parecchi casi di frode informatica, pensando di fare cosa gradita si tramettono alcune indicazioni relative ai controlli da svolgere, in particolar modo, sulle e-mail ricevute:

a) Porre attenzione al mittente, non fidarsi anche se la mail apparentemente arriva da un indirizzo conosciuto. Prima di procedere all'apertura della mail, controllare, utilizzando l'anteprima del riquadro di lettura, che dietro l'indirizzo e-mail o la "descrizione dell'indirizzo mail" conosciuto, non si nasconda un account sconosciuto e potenzialmente pericoloso.

Per fare questa verifica si può:

- controllare se dopo la "descrizione dell'account" è riportato un indirizzo conosciuto e coerente con la descrizione;

- controllare se, passando con il mouse senza cliccare, sulla "descrizione dell'account" è visualizzato un indirizzo conosciuto e coerente con la descrizione;

b) Porre attenzione alla presenza, nel testo della mail, di evidenti errori di punteggiatura o in generale di grossolani errori di scrittura;

c) Non farsi mai spaventare dal tono di urgenza o di minaccia della mail, aprendola senza prima aver fatto le dovute verifiche preliminari;

d) Porre attenzione agli allegati, non aprirli se non si è più che sicuri della loro provenienza e della loro attendibilità;

e) Porre attenzione ai link presenti, non cliccarci sopra se non si è più che certi della loro genuinità. Per verificare l'autenticità del link, passare con il mouse senza cliccare, sopra il link stesso e controllare se l'indirizzo, a cui si verrebbe inviati, sia attendibile e sicuro;

f) Porre attenzione anche alle e-mail recapitate nella cartella "posta indesiderata" di Outlook, prima di indicarle come attendibili;

g) Se si elimina una mail non attendibile, svuotare la cartella "posta eliminata" di Outlook;

h) Nel caso vengano cancellati file sospetti, in precedenza erroneamente salvati sul disco fisso del computer, svuotare sempre il "cestino".

Si consiglia in ogni caso di confrontarsi con il tecnico informatico di riferimento della vostra società, al fine di stabilire la procedura da adottare prontamente in caso di attacco hacker.

Si coglie l'occasione di porgere cordiali saluti

Studio Dott. Begni & Associati