Truffe via Business Email Compromise

Avvisi di sicurezza da parte del fornitore.

MSD prende molto seriamente le truffe e la protezione dei dati.

Il fatto di affidarci sempre più alla comunicazione virtuale sta facendo aumentare l'incidenza di attacchi Business Email Compromise (BEC). I BEC utilizzano la posta elettronica e le altre comunicazioni elettroniche per impersonare un dirigente, un dipendente o un'altra persona di un ente.
Questi attacchi avanzano infatti richieste di pagamento o di accesso alle buste paga o ai CUD dei dipendenti per conto di un'azienda.

Cosa dovresti sapere
MSD si impegna a proteggere i dati aziendali e bancari. In conformità con il nostro Dipartimento per la privacy globale e i nostri processi e linee guida in materia di Information Technology, oltre che nel rispetto delle

normative locali e regionali, il nostro personale qualificato applica processi e controlli rigorosi alla raccolta, validazione e cattura dei dati, con punti di controllo multipli e audit regolari delle nostre pratiche e procedure.

Per meglio proteggere la tua azienda:

- Utilizza i canali secondari o l'autenticazione a due fattori per verificare in modo indipendente le richieste di modifica dei dati del tuo account.
- Assicurati che gli URL riportati nelle e-mail siano associati all'azienda da cui dicono di provenire.
- Fai attenzione ai collegamenti ipertestuali che contengono errori di ortografia nell'effettivo nome di dominio.
- Verifica l'indirizzo di posta elettronica utilizzato per inviare le e-mail abbinandolo al mittente, soprattutto se utilizzi un dispositivo mobile o palmare.
- Crea filtri nel sistema di rilevamento delle intrusioni per contrassegnare le e-mail con estensioni che sembrano e-mail aziendali. Ad esempio, l'e-mail legittima di ceo@abc_company.com viene contrassegnata come e-mail fraudolenta da ceo@abc-company.com.
- Controlla regolarmente i conti finanziari per eventuali irregolarità, come ad esempio versamenti mancanti.
- Mantieni tutte le patch del software accese e tutti i sistemi aggiornati.
- Assicurati che le impostazioni sui computer dei dipendenti consentano di visualizzare le estensioni complete delle e-mail.
- Trova i contatti del Centro assistenza (Resolution Center) preposto a livello locale, avvisandone il personale se ritieni di essere vittima di un attacco BEC rispetto a MSD; in caso contrario, contatta le autorità locali.

Ci chiamiamo MSD ovunque, tranne negli Stati Uniti e in Canada dove siamo conosciuti come Merck & Co Inc, Rahway, NJ USA.