REGOLE AZIENDALI PER IL TRATTAMENTO SICURO DELLE INFORMAZIONI

Finalità: messaggi chiave per la gestione delle informazioni ricevute da o fornite per conto di Lilly, di seguito denominate Informazioni.

Perché è importante?

- La tua organizzazione e il suo personale sono preziosi collaboratori di Lilly e le azioni che intraprendete sono parte della prima e migliore linea di difesa contro la compromissione delle Informazioni.
- La protezione delle Informazioni è essenziale per Lilly e per i pazienti che serviamo.

I messaggi chiave seguenti, che sono basati sulle migliori pratiche del settore, tra cui il NIST Cybersecurity Framework, devono essere integrati nelle pratiche correnti per continuare a ridurre il rischio durante la gestione delle Informazioni.

In generale:

- Evitare di creare duplicati elettronici o copie cartacee di documenti contenenti Informazioni a meno che non sia assolutamente necessario.

Archiviazione elettronica dei dati:

- I file elettronici che includono Informazioni devono essere archiviati in modo sicuro. I dispositivi di archiviazione rimovibili come dischi rigidi esterni e USB non possono essere utilizzati senza l'approvazione di Lilly.
  - Per concedere l'accesso ai file deve essere applicato il principio del minimo privilegio (ovvero, l'accesso alle Informazioni deve essere accordato solo a coloro che hanno l'esigenza di sapere, in misura non superiore al necessario e soltanto per il tempo richiesto). L'accesso deve essere riesaminato proporzionalmente al livello di sensibilità. Ciò include gli spazi di archiviazione gestiti da te e quelle gestiti dai tuoi subappaltatori.
  - Occorre disattivare tempestivamente l'accesso non appena una persona lascia l'azienda o non ha più l'esigenza aziendale di accedere alle Informazioni.
- Le Informazioni NON devono essere archiviate nei seguenti mezzi senza l'approvazione di Lilly:
  - Dispositivi personali dei dipendenti come laptop, iPad, ecc.
  - Servizi o siti di archiviazione esterni.

Trasferimento elettronico dei dati:

- I file elettronici che includono Informazioni devono essere trasferiti in modo sicuro. Rivolgersi al referente Lilly per definire il metodo preferito per il trasferimento delle Informazioni. I dispositivi di archiviazione rimovibili come dischi rigidi esterni, CD/DVD e USB non possono essere utilizzati senza l'approvazione di Lilly.
- Le informazioni NON devono essere trasferite tramite:
  - Posta elettronica non protetta (a meno che il livello di sensibilità non lo consenta).
  - Dispositivi di archiviazione esterni, come disco rigido esterno o USB (senza l'approvazione di Lilly).
  - E-mail personale.

Teleconferenze/riunioni online:

- Utilizzare i servizi per le riunioni approvati da Lilly per programmare e condurre riunioni sulle attività aziendali. Rivolgersi al referente Lilly in caso di domande relative a teleconferenze/riunioni online.
- Prestare attenzione al contesto in cui ci si trova e agire con cautela quando si parla di Informazioni.

Sicurezza fisica:

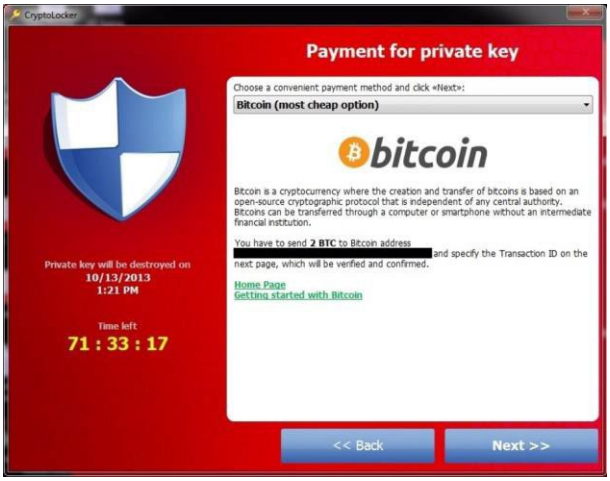
- Mantenere uno spazio di lavoro sicuro:
  - Bloccare l'accesso ai propri dispositivi OGNI volta che ci si allontana da essi.
  - I dispositivi devono essere collocati in un armadietto con serratura, bloccati tramite cavo o portati con sé quando si deve stare fuori per l'intera giornata, fare un viaggio di lavoro o andare in ferie.
  - Chiudere a chiave la scrivania, i mobiletti e l'armadietto/ufficio quando si deve stare fuori per l'intera giornata, fare un viaggio di lavoro o andare in ferie.
  - Non lasciare copie cartacee sulle stampanti.
  - Eliminare in modo riservato le Informazioni (ad esempio, con un dispositivo distruggi-documenti).

Messaggi istantanei ed SMS:

- Utilizzare uno strumento approvato da Lilly per scambiare messaggi istantanei ed SMS a fini aziendali. Rivolgersi al referente Lilly in caso di domande relative alla messaggistica istantanea o agli SMS.

Segnalazione di incidenti relativi alla sicurezza delle Informazioni:

- Segnalare tempestivamente gli incidenti al referente Lilly. Gli incidenti possono comprendere, tra l'altro, i seguenti casi:
  - Un messaggio e-mail contenente Informazioni è stato inviato accidentalmente a un destinatario sbagliato.
  - Un laptop, disco rigido o dispositivo di archiviazione rimovibile che contiene Informazioni è stato smarrito o rubato.
  - Un subappaltatore con accesso alle Informazioni avvisa l'azienda di un incidente.
  - Si riceve un ransomware, un tipo di software dannoso concepito per bloccare l'accesso al dispositivo fino al pagamento di una somma. Vedere l'esempio sotto. L'esecuzione immediata dei seguenti passaggi può aiutare a ridurre il rischio:
    - Scollegare il cavo di rete o disabilitare l'adattatore wireless.
    - Impostare la modalità di ibernazione.



Prestare attenzione all'ingegneria sociale *(ad esempio, Phishing, Vishing, SMiShing)*:

- L'ingegneria sociale consiste nell'utilizzare l'inganno per manipolare le persone affinché divulghino informazioni riservate o personali che possono essere utilizzate per scopi fraudolenti. I truffatori si fingono una fonte attendibile nel tentativo di rubare identità o recuperare Informazioni, come password, dati bancari, numeri di carte di credito, ecc.

- **Phishing** (e-mail)
  - Un tentativo di phishing è un messaggio inatteso che può avere le seguenti caratteristiche:
    - Una richiesta di azione urgente (ad esempio, un pagamento con carta di credito è in ritardo).
    - Un elemento temporale (ad esempio, una scadenza entro due giorni).
    - Una conseguenza (ad esempio, è necessario risolvere questo problema altrimenti succederà qualcosa di brutto).
    - Testo sgrammaticato o con errori di ortografia.
    - ED è sempre presente qualcosa su cui "fare clic", come un collegamento o un allegato
  - Se si fa clic su un allegato o un collegamento sconosciuto all'interno di un messaggio e-mail, il computer e l'intera rete potrebbero subire danni.

- **Vishing** (telefonate o messaggi vocali)
  - Un tentativo di vishing (phishing vocale) è una telefonata inattesa che:
    - Cerca conferma di Informazioni o richiede Informazioni.
    - Può essere utilizzata in combinazione con un attacco di phishing.
- **SMiShing** (messaggi di testo SMS)
  - Un tentativo di SMiShing è un testo inatteso che:
    - Cerca conferma di Informazioni o richiede Informazioni.
    - Può essere utilizzata in combinazione con un attacco di phishing.
    - In genere contiene qualcosa su cui "fare clic", come un collegamento o un allegato.

- **Chiunque abbia un indirizzo e-mail Lilly** parteciperà al programma di formazione sul phishing di Lilly.
  - Le persone che hanno fatto clic ripetute volte saranno segnalate alla terza parte e dovranno presumibilmente sottoporsi a un coaching di follow-up. Rivolgersi al referente Lilly per qualsiasi domanda relativa al programma di formazione sul phishing di Lilly.
  - Se si utilizza un account e-mail Lilly o365, segnalare i messaggi sospetti tramite il pulsante "Report Phishing" (Segnala phishing) nella barra multifunzione "Home" di Outlook.

  - Se si è connessi alla rete interna Lilly tramite VPN o virtual.lilly.com, segnalare i messaggi sospetti tramite cyber@lilly.com.

- **Fermarsi e controllare. Usare il proprio intuito:**
  - Se un messaggio e-mail sembra sospetto, fermarsi un istante ed esaminarlo con attenzione.
  - Non fare clic su link e non aprire allegati che non attendevi.
  - Se non si dispone di un indirizzo e-mail Lilly e si fa clic su un collegamento o si apre un allegato in un messaggio che si ritiene sospetto, occorre segnalarlo tramite la procedura del proprio datore di lavoro.

In caso di domande o dubbi:

- Rivolgersi al referente Lilly per domande o dubbi relativi a uno qualsiasi degli aspetti trattati sopra.
- Queste informazioni sono disponibili anche sul Supplier Portal (portale dei fornitori) in Operating Responsibility (Responsabilità operativa) nella sezione Supplier Resources (Risorse per fornitori).