Prot. *2019/3231*

Data 07/11/2019

Agli iscritti OPI Lecco
via PEC

23900 Lecco
Via Cantù 12
Tel. 0341/350102 Fax 351357
Cod. Fisc. 92028110135

Oggetto: Attacchi fraudolenti tramite email e PEC

Ordine delle Professioni Infermieristiche di Lecco

Giungono all'attenzione dello scrivente OPI le segnalazioni di ricezione di PEC dal contenuto ingannevole e fraudolento. La casella PEC, pur essendo uno strumento generalmente sicuro, non è purtroppo immune da tentativi di attacchi informatici, pertanto invitiamo a prendere tutte le accortezze necessarie per prevenirli. Nel caso delle attivate da questo Ordine è bene sapere che vengono fornite dal provider Aruba. Ad oggi ci è stato segnalato un testo in cui sono presenti i loghi di Aruba che richiedono di inserire i propri dati per regolarizzare il pagamento previsto per la casella PEC. A tal proposito ricordiamo che la casella è fornita gratuitamente dall'OPI-Lecco ed è l'ente stesso che fa da "interlocutore" con Aruba, pertanto suggeriamo di non cliccare e non fornire nessun dato ed informarci. Un'altra PEC di cui ci è giunta segnalazione contiene invece l'invio di un file immagine. Qualora non aspettiate di ricevere una PEC da un professionista, invitiamo a dubitare del contenuto. Gli indirizzi fraudolenti segnalatici sono: posta-certificata@aruba.pec.it e rembolso@landesonline-supporting.com. Tramite una rapida ricerca web è possibile vedere che si associano a diversi tentativi di phishing, ossia "furto di dati". Sperando di fare cosa gradita, riportiamo di seguito una lista di consigli utili:

- Prestare attenzione all'indirizzo, spesso differente rispetto al nome che compare come mittente. Esempio se compare "Servizio Clienti Aruba" e l'indirizzo è rembolso@landesonline è chiaro che ci troviamo di fronte una mail fraudolenta
- È possibile verificare l'esistenza e la proprietà di un indirizzo PEC sul sito https://www.inipec.gov.it/cerca-pec/-/pecs/companies. Si possono cercare sia imprese che professionisti
- L'indirizzo PEC di una Pubblica Amministrazione può essere invece verificato su https://www.indicepa.gov.it/documentale/index.php
- Non salvare e non aprire allegati da mittenti sconosciuti
- Non aprire nessun link, prima di aver verificato l'attendibilità della mail
- Non inserire mai informazioni personali, in particolare su siti che sono http: e non https:
- Controllare l'ortografia: spesso i messaggi falsi contengono errori grossolani, oppure sono traduzioni approssimative da altre lingue
- Minacce irrealistiche da eventuali hacker, vincite di concorsi a cui non abbiamo partecipato, notifiche di infrazioni che non abbiamo commesso, offerte commerciali non richieste, promesse di facili guadagni devono sempre farci dubitare

Rimaniamo a disposizione per qualsiasi chiarimento.
Cordiali saluti.

Il Presidente
Dott. Fabio Fedeli