L'Ordine della Professione di Ostetrica di Ravenna con sede legale in Ravenna (RA), Piazza Bernini, n. 2, C.F. 80008190391 e-mail: ostetriche.ravenna@gmail.com intende adottare la presente policy avente riguardo le regole da seguire nell'utilizzo e gestione della posta elettronica istituzionale al fine di evitare il configurarsi di situazioni di phishing, ossia una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'invio di messaggi di posta elettronica (ordinaria e/o PEC) ingannevoli.

1. PRESTARE ATTENZIONE AL MITTENTE

Quando il mittente della e-mail risulta essere sconosciuto, occorre prestare attenzione e interrogarsi sulla ragione di tale contatto, evitando di aprire l'e-mail inviate da contatti non noti, da un'istituzione pubblica non familiare o da un ente bancario.

2. FARE ATTENZIONE ALLA GRAMMATICA DEL TESTO

Se l'indirizzo email del mittente è noto e/o non appare sospetto, prestare attenzione alle modalità di dialogo ed allertarsi se le stesse sono diverse da quelle utilizzate usualmente dall'interlocutore.
In particolare, occorre analizzare il testo della mail, ponendo attenzione, soprattutto, sui seguenti elementi:

- messaggio inatteso;
- testo generico;
- testo pieno di errori di battitura o sintassi;
- testo tradotto da un'altra lingua;
- richiesta di informazioni personali;
- contenuto istituzionale o ufficiale proveniente da una banca, Poste Italiane, società di carte di credito, Google, PayPal etc.;
- contenuto riguardante sanzioni, multe o addirittura richiesta di riscatti che chiedono di aprire un allegato o di inviare immediatamente i propri dati personali;
- testo troncato, senza una frase di chiusura;
- testo minaccioso che mette ansia al lettore;
- contenuto entusiasmante che promette premi, vincite o occasioni della vita con un limite di tempo ristretto per poterlo ricevere.

Generalmente, queste e-mail contengono un tono intimidatorio e allarmante. Altre volte, invece, promettono premi e vincite. Altre ancora, non identificano in modo certo il destinatario, ma utilizzano un linguaggio generico, quale, ad esempio, "Gentile utente" o "Gentile cliente". In linea generale, è necessario diffidare sempre da email che per contenuto risultano essere sospette e/o inusuali rispetto a quelle tipicamente ricevute.
Spesso, il cyber criminale individua informazioni che riguardano la vita personale, quotidiana e lavorativa del destinatario per incardinare il messaggio proprio con specifiche informazioni che richiameranno la Sua attenzione, come ad esempio, elementi contabili, informazioni inerenti al corriere utilizzato, fatture di un fornitore reale, dati relativi a un servizio cloud realmente utilizzato, etc.
In ogni caso, è importante non fornire mai le informazioni richieste tramite la compilazione di un form, o scaricando un allegato o cliccando sul contenuto della mail.
In caso di dubbio sul fatto che l'e-mail sia stata correttamente indirizzata, contattate il mittente via telefono per accertarsi della veridicità del messaggio.

3. NON FORNIRE MAI INFORMAZIONI RIGUARDANTI CODICI E PASSWORD VIA MAIL.
Una buona prassi è quella di non fornire mai codici personali o password via mail. Inoltre, si consiglia di non fornire indicazioni attinenti alle credenziali bancarie, anche quando il messaggio sembra provenire da società bancarie note.
Generalmente, i cyber criminali si avvalgono della medesima grafica, testo, colori, temi e persino URL e indirizzi web simili al sito originale, contenenti comunicazioni legate a problematiche di malfunzionamento del sistema, come, ad esempio:

- problema con un pagamento;
- fattura o nota non pagata;
- abbonamento scaduto;
- multa da pagare;
- blocco del servizio.

Qualora risulti necessario, occorre verificare la veridicità del mittente, utilizzare gli strumenti all'uopo predisposti e chiamare preventivamente l'istituto bancario per accertarsi della richiesta.

4. FARE ATTENZIONE AGLI ALLEGATI
Spesso le e-mail phishing contengono allegati, in questi casi è necessario prestare la massima attenzione nell'apertura dei medesimi e non scaricarli se sussistono uno degli elementi sopra meglio descritti.

5. FARE ATTENZIONE AI LINK PRESENTI NEL TESTO DELLA E-MAIL
Se la mail contiene link sospetti, passare il mouse sopra l'URL senza cliccarci sopra, in modo tale da verificare la voce del link e un'eventuale corrispondenza con quanto contenuto nel resto del messaggio. In ogni caso, è consigliato evitare di cliccare sui link contenuti nei messaggi di testo mail, soprattutto se sussistono gli elementi sopra riportati.

6. NON INOLTRARE LA MAIL SOSPETTA
In caso di ricezione di una mail ritenuta sospetta, la stessa non deve assolutamente essere inoltrata ad altro contatto. È però possibile procedere con un l'invio di uno screenshot all'eventuale consulente tecnico IT per rappresentare il problema e chiedere supporto.

7. NON TENERE IL SEGRETO
In caso di attacco di phishing informare immediatamente l'eventuale consulente tecnico IT, il referente privacy dell'Ordine e il DPO.

8. ATTENZIONE ALLA PEC
La PEC non è necessariamente un sistema di comunicazione elettronica sicura: la sua gestione segue, pertanto, le regole sopra riportate per l'e-mail.

Ravenna, 09/10/2025

ORDINE DELLA PROFESSIONE DI OSTETRICA di RAVENNA

La Presidente
Gasperoni Oriana