SIMULAZIONE PHISHING CON CHATGPT:

Il compito di oggi consiste di creare una mail di phishing credibile scegliendo un contesto e un obbiettivo.

Il contesto che ho scelto, è una situazione che purtroppo è molto reale ad oggi, ho deciso che il mittente in questione sarà un fornitore di energia elettrica che invia una mail ad un cliente/destinatario nella quale richiede il pagamento urgente di una fattura che risulta insoluta del valore di 100 euro entro i 5 giorni utilizzando il qr code allegato.

Per fare questa simulazione mi sono aiutata con chatGPT il quale ha formulato un esempio come possiamo vedere nell'immagine sottostante:

Oggetto: Urgente: Fattura Insoluta da Saldare

Da: supporto@fornitoreenergia.it

A: cliente@esempio.com

Gentile Cliente,

La informiamo che abbiamo riscontrato un saldo insoluto sulla sua fattura recente. Per evitare l'interruzione del servizio, è necessario saldare l'importo di 100 euro entro e non oltre 5 giorni dalla ricezione di questa email.

Per procedere al pagamento, la invitiamo a utilizzare il QR Code allegato, che la guiderà al nostro sistema di pagamento sicuro.

![QR Code Allegato]

Se ha già effettuato il pagamento, la preghiamo di ignorare questa comunicazione. In caso contrario, clicchi sul QR Code per regolarizzare la sua posizione.

La ringraziamo per la collaborazione.

Cordiali saluti,
Servizio Clienti
Fornitore di Energia Elettrica

Come possiamo vedere la mail ad una persona che non ha competenza in materia potrebbe risultare credibile in quanto il testo è scritto in maniera veritiera, abbiamo un indirizzo email credibile di un fornitore x e un qr code allegato.

Allo stesso tempo una persona che è preparata noterebbe subito che non c'è un logo riconoscibile del fornitore, saprebbe che difficilmente un fornitore può richiedere in questo modo un pagamento, dovrebbe esserci un documento con la fattura allegato, dove possiamo riscontrare il codice cliente o i dati dell'azienda del fornitore. Inoltre come abbiamo imparato oggi, una persona formata, potrebbe accertarsi della veridicità della mail cliccando su "mostra originale", e li possiamo vedere se sono presenti o meno i parametri SPF, DKIM e DMARC o meno. Se questi parametri non sono presenti sicuramente non è una mail vera. Anche ananlizzando il codice potremmo controllare i passaggi effettuati, ad esempio, fornitore elettrico-google e google-cliente con i rispettivi indirizzi IP, in questo caso possiamo essere sicuri sull'autenticità del mittente e del contenuto.