SPIEGAZIONE DELLE DINAMICHE

Per questo attacco ho scelto un manager molto importante di un’azienda di moda, la scelta del settore moda non è casuale come tutti sappiamo nel mondo della moda si ha a che fare con molte donne dalle varie mansioni, dalle modelle (spesso molto giovani) alle segretarie. Le informazioni che abbiamo sul nostro manager sono che ha moglie e figlie quindi faremo leva sulla sua integrità di marito e padre. La sua email personale l’abbiamo presa direttamente dal sito della sua azienda con strumenti di OSINT per accelerare il processo, e con una semplice ricerca su Facebook abbiamo scoperto nome e cognome di moglie e figlie in modo da avere tutto pronto per creare il nostro bait. Per iniziare abbiamo raccolto foto da varie prospettive del nostro manager dal suo account facebook, per poi aprire i book fotografici delle varie modelle che lavorano per l’azienda dal loro sito ufficiale, abbiamo proceduto ad allenare un modello di IA che genera foto DeepFake (Generative Adversarial Networks). Ora che il modello è allenato e pronto a generare qualsiasi tipo di foto con un catalogo intero delle varie modelle (giovanissime) e del nostro manager prepariamo la nostra email di Phishing, ora colleghiamo tutti i punti di questa premessa. Divideremo la truffa in ben 2 email!

EMAIL PHISHING 1

Gentile [Nome del Manager],

Mi scuso per il disturbo, ma mi vedo costretto a contattarla per un problema estremamente delicato che richiede la sua attenzione immediata.

Durante una recente verifica di sicurezza informatica, abbiamo rilevato una serie di immagini e materiali che sembrano essere stati reinvenuti a suo nome e associati al suo profilo pubblico. I contenuti, seppur probabilmente manipolati digitalmente, sono di natura compromettente e potrebbero causare danni alla sua immagine personale e professionale.

A tutela della Sua privacy, questi materiali non sono stati ancora divulgati. Tuttavia, abbiamo ricevuto una richiesta anonima che minaccia di inviare tali contenuti ai membri della sua famiglia e ai suoi contatti professionali, a meno che non venga effettuato un pagamento entro le prossime 48 ore.

Se desidera evitare l'escalation di questa situazione, La invitiamo a seguire le istruzioni indicate nel documento allegato, dove troverà il dettaglio delle modalità per risolvere la questione.

Scarichi il documento qui:
[Link_fittizio.docx](http://example-malicious-link.com)

Ci auguriamo che lei capisca la delicatezza di questa situazione e agisca con tempestività.

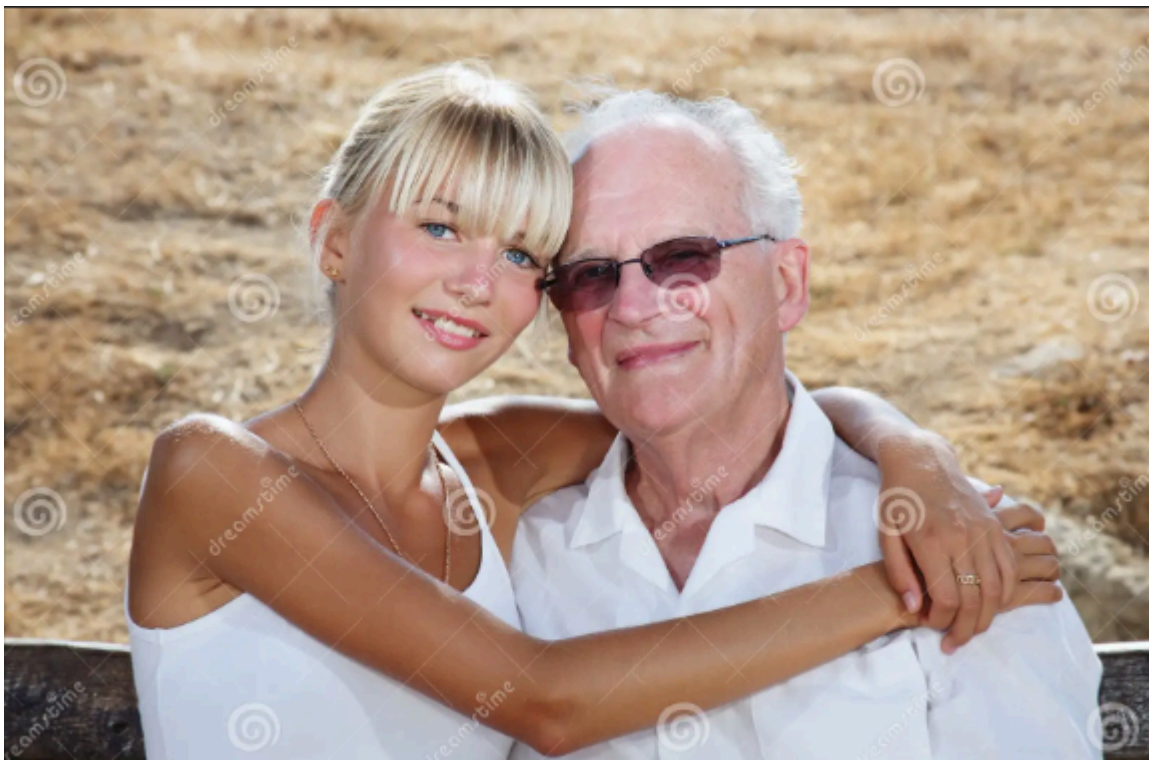
Cordiali saluti,
Ufficio Sicurezza Digitale
[Nome azienda simulata]

SECONDA FASE EMAIL

Gentile [Nome del Manager],

Come già anticipato nella nostra precedente comunicazione, siamo in possesso di materiale digitale compromettente associato al suo profilo. Per dimostrare la nostra serietà, Le inviamo in allegato una **singola immagine** come prova dell’autenticità dei dati in nostro possesso. Si tratta solo di una frazione del materiale completo, che include anche video.

[Allegato fittizio: *anteprima.jpg*]



Qualora non venga presa una decisione entro le prossime **24 ore**, procederemo con la divulgazione completa dei contenuti, inviandoli a:
- La Sua famiglia ([Lista generica, es.: moglie e figli])
- I Suoi colleghi ([Lista generica, es.: dipendenti del Suo dipartimento])
- I media ([generico, es.: principali testate di settore])

Per evitare questa situazione, può trovare le istruzioni dettagliate nel documento allegato.

Scarichi il documento qui:
[Link_fittizio.docx](http://example-malicious-link.com)

Non sottovaluti questa comunicazione. Una volta iniziata la divulgazione, non sarà più possibile fermarla.

Cordiali saluti,
Ufficio Sicurezza Digitale
[Nome azienda simulata]