Struttura e Relazione Tecnica Phishing (Social Engineering)

Da: supporto-it@azienda.it
A: “e-mail del dipendente” **ven 13/09/2024 17:00**

Oggetto: AZIONE RICHIESTA: Aggiornamento URGENTE credenziali di accesso

Gentile “Utente”,

Le scriviamo questa e-mail per avvisarla che causa di un recente intervento tecnico e relativo aggiornamento dei sistemi di sicurezza aziendale, Le chiediamo con estrema urgenza la verifica dei Suoi dati di accesso al portale aziendale e di agire, eseguendo un aggiornamento delle Sue credenziali per accedere al sistema dell’azienda.

Dopo un’analisi del sistema da parte del Team IT – Sicurezza Informatica, La informiamo di aver rilevato attività sospette sull’account, per agire tempestivamente e proteggere i Suoi dati, clicchi sul link che trova alla fine di questo avviso nelle prossime 24 ore.

Se non aggiorna le Sue credenziali di accesso entro le prossime 24 ore, il Suo account aziendale sarà sospeso.

Clicca e aggiorna

Grazie in anticipo,
Team Information Technology
supporto-it@azienda.it
Telefono: +39 02 12345678

AVVISO IMPORTANTE: Per motivi di sicurezza aziendale, si prega di non cancellare la soprascritta comunicazione.

Descrizione sulla struttura della e-mail

Il dipendente (**destinatario**) di una determinata azienda riceve sul suo PC Desktop o Laptop un'email che a primo impatto sembra provenire da un mittente attendibile, in questo caso, con inviata dal Team Information Technology dell’azienda in cui il dipendente lavora.
La e-mail inviata dalla sua “azienda” e ricevuta dal lavoratore, lo informa di verificare e di attuare un aggiornamento dei propri dati, in questo caso, le proprie credenziali di accesso al portale dell’azienda.

L'obiettivo del **Phishing** una delle Tecniche, appartenente al Social Engineering, è quello di ottenere le credenziali personali del dipendente, così da avere accesso al portale dell'azienda.

Relazione sulla struttura dell'e-mail "aziendale"

Nell'esempio illustrato sulla pagina precedente, viene descritta una situazione in cui un dipendente riceve una e-mail, dove gli viene richiesto di aggiornare con tempestività le proprie credenziali di accesso al portale aziendale da parte del Team IT – Sicurezza Informatica.
La richiesta di primo impatto sembra che provenga da una fonte (**mittente**) attendibile, dove al suo interno richiede un aggiornamento di sicurezza, urgente, una procedura di routine, spesso eseguita a livello aziendale, e che alla fine della e-mail, con una frase che tocca la psicologia del dipendente, chiede allo stesso di aggiornare al più presto le proprie credenziali, o che se non agirà tempestivamente, l'account sarà sospeso.

Indizi che possono allertare il dipendente, sulla possibilità che non sia una e-mail ricevuta da una fonte (**mittente**), attendibile, ma che al contrario, sia una e-mail di **Phishing**.

Di seguito elenco gli indizi di allerta del dipendente:

- **NOMINATIVO ASSENTE**: La e-mail non specifica il nome dell'utente (dipendente) e la mancanza della personalizzazione incrementa il dubbio sull'autenticità della e-mail.
- **URGENZA AGGIORNAMENTO CREDENZIALI**:
  - Le email legittime raramente richiedono azioni immediate con minacce di sospensione dell'account.
- **DESCRIZIONE LINK**:
  - A primo impatto può sembrare un link normale, ma in realtà potrebbe nascondere un attacco **Phishing**.
- **E-MAIL AZIENDALE ERRATA**:
  - L'indirizzo e-mail aziendale, nell'esempio, illustrato in precedenza, **supporto-it@azienda.it** a prima vista potrebbe essere corretto, ma se analizzato con maggiore attenzione da parte del destinatario (**dipendente**), potrà accertarsi che non è l'indirizzo dell'azienda in cui lavora.
- **NUMERO FISSO AZIENDALE ERRATO**:
  - Il numero di telefono fisso aziendale nell'esempio, illustrato, in precedenza, **+39 02 12345678** a prima vista potrebbe essere corretto, ma se analizzato con maggiore attenzione e magari con le giuste verifiche da parte del dipendente, lo stesso potrà accertarsi che il contatto telefonico, non corrisponde a tutti gli effetti all'azienda per cui lavora.

13/09/2024 **Christian Vagnoni**