

Phishing

Obiettivo del phishing: Ottenere le credenziali di accesso del cliente (username e password) per accedere al suo conto bancario online.

Scenario

Ho immaginato un cliente di una banca che riceve un'email apparentemente da parte della sua istituzione bancaria. L'email informa il cliente di un presunto problema con il suo conto, richiedendo un'azione immediata per evitare il blocco dell'account. Utilizza un linguaggio formale e professionale, cercando di instillare un senso di urgenza.

Esempio di Email di Phishing

Oggetto: Avviso Importante: Verifica Urgente del Tuo Conto

Da: Servizio Clienti Banca
servizioclienti@DeutscheBank.com

A: Edoardo Mucci

Data: [Data di oggi]

Gentile Edoardo Mucci,

Ti informiamo che abbiamo rilevato un'attività sospetta sul tuo conto corrente. Per proteggere i tuoi fondi e garantire la sicurezza del tuo account, ti chiediamo di effettuare una verifica immediata delle tue informazioni.

Clicca sul link sottostante per accedere al tuo profilo e completare il processo di verifica:

192.168.1.184

Ti preghiamo di effettuare questa operazione entro 48 ore per evitare la sospensione del tuo accesso online. Grazie per la tua attenzione a questa questione importante. Siamo qui per assisterti.

Cordiali saluti,
Il Team di Assistenza Clienti
DeutscheBank

Avviso Importante: Verifica Urgente del Tuo Conto

edoardo.edowork@gmail.com

Avviso Importante: Verifica Urgente del Tuo Conto

Da: Servizio Clienti Banca servizioclienti@DeutscheBank.com

A: Edoardo Mucci

Data: 31/10/2024

Gentile Edoardo Mucci,

Ti informiamo che abbiamo rilevato un'attività sospetta sul tuo conto corrente. Per proteggere i tuoi fondi e garantire la sicurezza del tuo account, ti chiediamo di effettuare una verifica immediata delle tue informazioni.

Clicca sul link sottostante per accedere al tuo profilo e completare il processo di verifica:

[Verifica il tuo conto](#)

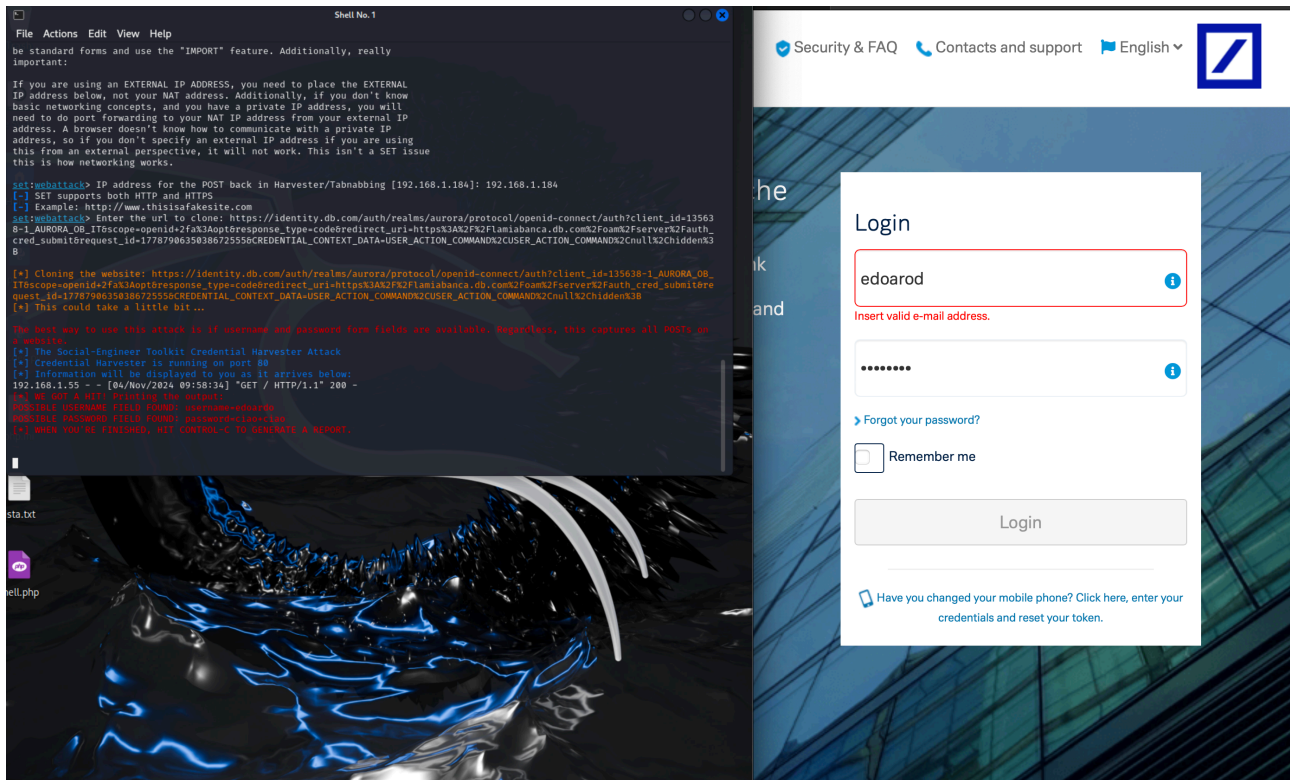
Ti preghiamo di effettuare questa operazione entro 48 ore per evitare la sospensione del tuo accesso online.

Grazie per la tua attenzione a questa questione importante. Siamo qui per assisterti.

Cordiali saluti,
Il Team di Assistenza Clienti
Deutsche Bank

Con lo strumento SET, nella macchina di Kali Linux, ho simulato un attacco phishing clonando la pagina di login della banca Deutsche Bank.

PROGETTO S5/L5



Conclusioni

Le email di phishing possono sembrare autentiche e convincenti, sfruttando tecniche di ingegneria sociale per indurre le vittime a rivelare dati sensibili.

È cruciale essere vigili e adottare misure preventive, come verificare attentamente l'indirizzo email del mittente, evitare di cliccare su link sospetti e soprattutto educare se stessi e gli altri su queste minacce per navigare in sicurezza.