**OBIETTIVO DEL PHISHING:** Rubare credenziali di accesso alla banca ad un cliente.

**E-MAIL**

**Oggetto**: URGENTE: Conferma delle informazioni sul tuo conto bancario

Gentile Cliente,

Abbiamo notato un accesso insolito al tuo account bancario e, per proteggere i tuoi dati personali, ti chiediamo di confermare alcune informazioni importanti. È essenziale per garantire la tua sicureza e prevenire potenziali atività non autorizzate.

**Attività sospetta rilevata:**

* Data: 01/11/2024
* Ora: 09:47
* Località: Milano

**Azioni richieste:**

Per evitare la sopensione temporanea del tuo conto, ti invitiamo a confermare entro 24 ore i tuoi dati. È possibile completare la verifica seguendo il link sottostante:

[**Clicca qui per verificare il tuo conto bancario**](http://link-falso.com)

Al termine della verifica, ti chiederemo di fornire i seguenti dettagli per confermare la tua identità:

* Numero del conto corrente
* Codice IBAN
* Codice fiscale
* PIN di accesso online

Queste informazioni ci permetteranno di autenticare la tua identità e garantire che non ci siano attività sospette sul tuo conto.

Se non completi questa procedura di verifica entro il tempo indicato, il tuo conto verrà temporaneamente bloccato per motivi di sicurezza e sarà necessario contattare il servizio clienti per la riattivazione.

**Nota**: Questo messaggio è inviato automaticamente, per favore non rispondere a questa email. Per ulteriori chiarimenti, contattaci al numero verde: 800-123-456.

Grazie per la collaborazione,  
Servizio di Sicurezza Bancaria  
Banca BPM

In questa mail, l’idea è quella di rubare i dati di accesso bancari ad un cliente, in questo caso banca BPM. L'email sembra credibile perché utilizza diverse tecniche di messaggio reali e induce il destinatario a rispondere rapidamente senza pensarci troppo. Ecco i principali elementi che aumentano il grado di persuasione:

1. **Uso formale e professionale**: L'email è scritta in uno stile formale, simile a quello che potrebbe utilizzare una banca o un'istituzione finanziaria affidabile. Frasi come "Gentile Cliente" e "Servizio di Sicurezza Bancaria" sono comuni nelle comunicazioni ufficiali, e l’assenza di errori grammaticali o sintattici dà un’impressione di autenticità.
2. **Riferimento a una "attività sospetta"**: L’idea di una possibile attività sospetta è pensata per creare urgenza e preoccupazione. È una tattica psicologica: le persone sono più propense a rispondere immediatamente se pensano che i loro dati o denaro siano a rischio.
3. **Scadenza temporale**: Dare un limite di tempo ("confermare entro 24 ore") aumenta il senso di urgenza e riduce il tempo di riflessione della vittima. Temono di perdere l'accesso al conto e quindi agiscono in fretta, senza pensare troppo o verificare la veridicità dell'email.
4. **Chiamata all'azione chiara e diretta**: Link come "Clicca qui per verificare il tuo conto bancario" sono progettati per essere facili da trovare e cliccare, portando l'utente direttamente a una pagina falsa. Una chiamata all’azione esplicita sembra legittima e rassicura che tutto si risolverà facilmente tramite il link.
5. **Richiesta di informazioni personali "per la sicurezza"**: Questo è il punto cruciale. L'email chiede informazioni come numero del conto, IBAN, codice fiscale e PIN, tutte informazioni sensibili che una banca legittima non richiederebbe mai tramite email. Tuttavia, il richiamo alla sicurezza inganna, poiché fa apparire queste richieste come una misura di protezione.
6. **Dettagli di contatto generici**: L'indicazione "non rispondere a questa email" e un numero verde fittizio danno un’ulteriore parvenza di autenticità, in quanto molte email ufficiali spesso contengono informazioni simili.
7. **Assenza di un destinatario specifico**: Anche se alcune email di phishing potrebbero utilizzare il nome del destinatario per aumentare l'illusione, l'uso di "Gentile Cliente" è comune nelle email di servizio, e quindi non fa necessariamente sorgere sospetti.

Nelle e-mail di phishing è normale trovare errori grammaticali, evidenziati nella mail, così come link sospetti e chiamate urgenti all’azione. È molto importante controllare prima di tutto il link. Passandoci sopra col mouse è possibile verificare che l’URL combaci con quello della banca, inoltre quest’ultima non chiederà mai i tuoi dati di accesso come PIN o IBAN tramite mail.