«Social Engineering» Informazione e prevenzione

Come si presentano i possibili attacchi di social engineering?

- Una persona si presenta come un tecnico (per es. di una società telefonica o di fornitura di elettricità) e tenta di introdursi in casa vostra o nella sede della vostra impresa.
- Ricevete un'e-mail che vi invita ad aprire un link ed effettuare l'accesso su un sito Web, o a fornire informazioni personali (phishing).
- Una persona vi telefona e afferma di voler condurre un sondaggio. L'obiettivo è quello di ottenere informazioni sensibili (per es. sul reddito, sulle misure di sicurezza, ecc.).
- Alla vostra postazione di lavoro si presenta una persona che si spaccia per un tecnico e vi fa credere di dover eseguire dei lavori di manutenzione sul vostro PC.

Tutti questi attacchi mirano a strapparvi informazioni personali o riservate (come dati di accesso, password, ecc.) per utilizzarle poi illecitamente.

Social Engineering

Il social engineering è un metodo diffuso per l'acquisizione di informazioni riservate, tutte riguardanti i singoli individui. Per raggiungere questo obiettivo vengono spesso sfruttate la buona fede e la disponibilità – così come l'insicurezza – delle persone. Dalle telefonate fittizie alle persone che si spacciano per qualcun altro, agli attacchi di phishing, non c'è limite alla varietà.

In generale è sufficiente una dose «sana» di sfiducia. Spesso è utile chiedersi che tipo di informazioni si rendono pubbliche su di sé e a chi.

Proteggetevi così:

- comunicate il minor numero possibile di informazioni personali su di voi. Sui siti di social networking come Facebook, Xing, ecc., in particolare, è opportuno agire con grande cautela nella pubblicazione di informazioni.
- in generale le password non vanno MAI comunicate a un'altra persona. Nemmeno a un amministratore di sistema o al vostro capo. Una password appartiene SOLO E SOLTANTO a voi!
- non fidatevi delle richieste pervenute via e-mail. Anche le e-mail di mittenti conosciuti (amici) possono essere falsificate.

In caso di dubbio informate il vostro istituto finanziario

In caso di sospetti sul servizio e-banking non comunicate nulla e informate immediatamente il vostro istituto finanziario. I recapiti si trovano su http://www.ebankingmasicuro.ch.

Ulteriori informazioni: www.ebas.ch/socialengineering

«eBanking – ma sicuro!» presenta utili informazioni sulla sicurezza per gli utenti dei servizi e-banking

eBanking ma sicuro!

Sul sito Internet gratuito **www.ebankingmasicuro.ch** si trovano ulteriori informazioni pratiche sui provvedimenti necessari e le regole di comportamento per un uso sicuro delle applicazioni di e-banking.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz