WELCOME

To The Net

Ovvero
sopravvivere alla rete
ed altre storie incredibili

Ingegneria Sociale

“Ingegneria sociale significa **utilizzare il proprio ascendente** e le capacità di persuasione per ingannare gli altri e manovrarli, convincendoli che l'ingegnere sociale è quello che non è.
Di conseguenza l'ingegnere sociale può **usare le persone per ottenere informazioni**, con o senza l'ausilio di strumenti tecnologici.”

Kevin Mitnick

L’ingegneria sociale è quindi l’arte di farsi dare dalle persone, informazioni che normalmente non divulgherebbero.

Ingegneria Sociale

Con il passare degli anni, i sistemi informatici hanno fatto della sicurezza uno degli elementi più complessi e solidi, rendendo i tentativi di intrusione sempre più elaborati e tortuosi.

Quindi perché, volendo attaccare un'infrastruttura, dovremmo tentare un approccio così complesso, quando la persona che sta dietro lo schermo rappresenta **l'anello debole**?

Ingegneria Sociale

Le basi di un attacco di ingegneria sociale, **si fondano sull'inganno** e fanno leva su tecniche psicologiche, come infondere un senso di autorità, indulgenza, colpa o panico, oppure sfruttando i punti deboli del bersaglio, quali ignoranza, desiderio fisico ed avidità.

Autorità: un messaggio spedito da forze dell'ordine, banche o enti governativi, assume automaticamente una certa importanza e l'utente sarà spronato a seguire le richieste del comunicato, abilmente compilato dall'ingegnere sociale.

Ingegneria Sociale

Colpa: una persona che si sente in colpa per una determinata situazione, cercherà di porvi rimedio al più presto, per sentirsi meglio ed evitare provvedimenti disciplinari.
Questo potrebbe spingerla ad eseguire azioni inconsuete pur di rimettere tutto a posto.

Panico: ancora meglio della colpa, una persona in panico compie azioni stupide.
Una situazione di emergenza, che rischia di peggiorare in tempi brevissimi e la cui colpa può essere data al target, genera panico; una soluzione rapida, per quanto inusuale, può essere adottata senza troppa riluttanza.

Ingegneria Sociale

Ignoranza: un problema tecnico o un messaggio di errore indecifrabile possono scatenare due reazioni.
Ammettere l'ignoranza ed affidarsi all'ingegnere, oppure dimostrare falsa competenza, assecondando comunque i consigli dell'ingegnere, pur di non sembrare poco preparati.

Desiderio: contenuti pornografici o promesse di incontri con belle ragazze possono invogliare il target a compiere azioni inusuali per non lasciarsi sfuggire la "preda".
Questa tecnica è particolarmente efficace con gli utenti di sesso maschile

Ingegneria Sociale

Avidità: offerte imperdibili e guadagno facile sono la base per questo tipo di attacco, dove il bersaglio, pur di non lasciarsi sfuggire l'occasione, segue i procedimenti segretissimi e particolari forniti dall'ingegnere sociale.

Compassione: per quanto sembri strano, la maggior parte delle persone sono portate ad aiutare qualcuno in difficoltà, specialmente se c'è qualche elemento che le accomuna. Questa tecnica è molto efficace con i bersagli femminili.

Ingegneria Sociale

A seconda di come viene condotto l'attacco, distinguiamo tre tipi principali di ingegneria sociale:

- **Umana**: si basa sul carisma dell'attaccante e viene condotto di persona o telefonicamente.
  E' sicuramente l'attacco più complesso e "classico", che se condotto bene può dare grossi risultati.

- **Digitale**: sfrutta canali digitali come mail, finestre di popup, chat e social network. In alcuni casi,
  come ad esempio la chat, si assumono molti elementi della modalità umana

- **Mobile**: specializzazione della digitale, sfrutta link ed app per accedere ai dati memorizzati in uno smartphone.
  Per questo motivo verificare le fonti di un app può essere di fondamentale importanza.

Ingegneria Sociale

Alcuni esempi delle tecniche più usate e che sono diventate famose nel tempo:

- **Truffa rayban su facebook**: canale digitale - avidità;
- **Truffa “Polizia Postale”**: canale digitale - autorità e panico;
- **Popup “Computer infetto da virus”**: canale digitale - ignoranza e panico;
- **Richieste di sesso in cam su Facebook (e-whoring)**: canale digitale - desiderio;
- **Sondaggio Ikea con premio da 500€**: canale digitale - avidità;
- **Telefonate informative su contratti o programmi aziendali**: canale umano - autorità o compassione;
- **Furto dati dalle “applicazioni torcia” android**: canale mobile - ignoranza.

Ingegneria Sociale

Come è possibile quindi proteggersi da attacchi di ingegneria sociale?

Mobile: specialmente nel caso di smartphone windows ed android ma anche Apple con jailbreak, è buona norma non installare mai app delle quali non possiamo **verificare la fonte** ed anche in tal caso, valutare bene i permessi da concedere.

Ingegneria Sociale

Digitale: mantenere aggiornato l'antivirus è sicuramente la base ma alcuni accorgimenti aggiuntivi sono doverosi.

- Prestare attenzione agli **URL** dei siti
- Diffidare di **mail che richiedono informazioni** quali numeri di conto, PIN ecc…
- Prestare attenzione al **phishing**
- Diffidare di **offerte incredibili** e metodi segreti per diventare milionari in un pomeriggio
- Diffidare di modelle di Victoria's Secret improvvisamente **innamorate di noi** su Facebook

Ingegneria Sociale

Umana: la prevenzione da un contatto “diretto”, quindi di persona o tramite telefono passa per semplici punti.

- Seguire sempre le **procedure di sicurezza**;
- Se un’autorità chiede l’accesso a dati sensibili, **richiedere un riconoscimento** ed effettuare una verifica prima di acconsentire;
- Non effettuare procedure che **esulano dai normali iter**;
- Diffidare da offerte e **proposte straordinarie** e valutare sempre in maniera oggettiva;
- **Non violare le politiche aziendali** facendosi muovere da compassione;
- Nel dubbio, **chiedere consiglio** ad un collega o ad un superiore prima di effettuare procedure inusuali.

Ingegneria Sociale

"Le forze dell'ordine non possono proteggere i consumatori.
Le persone devono essere più consapevoli dei rischi e deve esserci maggiore informazione sui furti d'identità.
Siate più attenti e anche un po' più furbi, non c'è nulla di male nell'essere diffidenti.
Viviamo in un mondo dove se qualcuno ha l'occasione di truffarti, sicuramente lo farà**"**

Frank William Abagnale