Ingineria sociala

Istorie si prezent

De fapt, cat de vechi este conceptul?

Ce intelegem prin inginerie sociala?

- Phishing/spearphishing - in general un atac lansat prin e-mail, mesagerie, SMS sau alte forme scrise de a insela un utilizator
- Vishing - in general un atac lansat prin comunicare directa cu userul - in general telefon
- Baiting - in general campanii de genul “too good to be true”
- Quid pro quo - in general un atacator care impersoneaza o persoana legitima si cere informatii personale in schimbul unei actiuni in aparenta legitima
- Tailgating/pretexting - in general o persoana care obtine acces in zone fizice fara autorizatie

Sa deconspiram conspiratii

1. Nu e Rusia - ei prefera tinte mult mai mari
2. China doar te spioneaza, nu vrea banii tai
3. Probabil ca esti atacat mai degraba pentru ca esti mediocru decat pentru ca esti special
4. Nu este o oculta mondiala care se ocupa de asta
5. Nici un adolescent intr-un beci
6. De obicei sunt grupuri numeroase, care functioneaza ca orice organizatie comerciala

Campanii cunoscute - international
(si un video senzational pe subiect)

Facebook si Google - 2013-2015 - peste 100 mil USD

Crelan Bank, Belgia - 2016 - 75 mil EUR

JP Morgan - 2017 - 50 mil USD

Dar de ce?
Simplu. Bani

Economia digitala subterana este evaluata la peste 3 TRILIARDE de dolari. Da, 3000 de miliarde de dolari. Anual.

Asta include:

- Dezvoltarea si revanzarea de software malitios
- Dezvoltarea si revanzarea campaniilor de colectare a datelor personale si a datelor personale
- Dezvoltarea de echipament hardware si revanzarea datelor financiare
- Tranzactii cu produse si servicii ilegale in economia reala
- Piata de contractare (da, contractare) a serviciilor malitioase digitale

PIB-ul Romaniei este 300 de miliarde, adica de 10 ori mai putin

Cum ma pot proteja?

1. Exploreaza si invata cu incredere setarile de siguranta ale platformelor folosite in mod uzual: google, facebook, instagram, microsoft, etc
2. Instaleaza cat mai repede update-urile de pe toate dispozitivele si aplicatiile pe care le folosesti - majoritate update-urilor au si setari de securitate
3. Activeaza autentificarea in 2 factori pe toate platformele care au aceasta functionalitate
4. Fii suspicios daca o platforma nu are aceasta functionalitate
5. Stai la curent cu ultimele campanii: de exemplu, urmareste DNSC pe platformele sociale

Ramai vigilent!