

IT DROŠBAS APMĒCĪBAS UN SOCIĀLĀ INŽENIERIJA



VEICINĀSIM DARBINIEKOS IZPRASTI!

Datorlietotāju apmācības ir svarīga loma kopējā IT drošības nodrošināšanā jebkurā organizācijā, jo neuzmanīgs un neinformēts darbinieks, kas publiski atstāj pieejamu savu lietotāja paroli, ir tikpat bīstams kā hakeru uzbrukums organizācijai.

Ikviens darbinieks var kļūst par uzbrukuma upuri, kļūstot par vienu no galvenajiem IT drošības draudiem organizācijā, un tikai izglītots un pienācīgi informēts organizācijas IT lietotājs nekļūst par ieroci krāpnieku rokās, jo:



Pratīs izveidot drošus paroli, neatstājot to publiski pieejamu un saprotot, kādi ir regulārie jomains.



Izpats un ievieš organizācijā noteiktos drošības tehniskus un informācijas sistēmu lietošanas noteikumus.



Atbildīgi un droši veidlieto mobilās ierīces un sociālos tīklus internetā.



Spēj identificēt „aizdomīgus” e-pastus, tīrumus un atbilstoši uz tiem reaģēt.



Apzināsies, ka pat spersonāli ir viens no potenciālajiem krāpnieku uzbrukumu mērķiem.

MĀSPĒDIĀM

1

Veikt IT drošības apmācības apvienojumā ar sociālo inženieriju, iekaujot:



Sagatavošanās interviju ar IT vai uzņēmuma vadītāju par aktualitāti, specifiskiem klienta riskiem, noteikumiem u.c. jautājumiem.



Lietotāju apmācības un pārbaudes - sociālo inženierijas demo uzbrukumu/testu.



Mācību materiālus katram apmācībū dalībniekam.

Izmaksas

1395 EUR + PVN par vienas grupas (līdz 25 cilvēkiem) nodarbu un testu. Katram grupas dalībniekam: 245 EUR + PVN*.

*Vairāk par 5 grupām ir individuāli piedāvājums.

IT DROŠBAS APMĒCĪBAS UN SOCIĀLĀ INŽENIERIJA



2

Veikt IT drošības apmācības programmu, iekaujot tādā maskā:



Ikviens ir mērķis - iemesli, kādēļ jebkurš no darbiniekiem var kļūt par uzbrukuma upuri.



Sociālā inženierija - izplattās metodes, kas uzbrucēji spēj manipulēt ar cilvēkiem.



Paroles - droša parolu lietošana. Demonstrācijas un piemēri, kā pareizi veidot un glabāt paroles.



Drošības incidents - kā identificēt un rīkoties, ja datorā ir iekļuvis hakeris, vīrusi vai aunprātīga programmatūra.

Izmaksas

790 + PVN par vienas grupas (līdz 25 cilvēkiem) nodarbību. Katrai nākamajai grupai: 245 EUR + PVN*.

*Vairāk par 5 grupām ir individuāls piedāvājums.

3

Veikt kļūdu no sociālās inženierijas testa /uzbrukuma veidiem, piemēram:



Pa ceļam publiski pieejamā informācijas analīzes, **veikt telefona zvanu**, iegūstot privāto organizācijas vai darbinieka informāciju.



Viltuse-pasta izsūtīšanu ar saiti uz viltus lapu (phishing, jeb pikšķeršana).



Fizisko piekļuves zonu pārbaudi, piemēram, armēri iegūst pieeju datortīkla pieslēgvietai vai datu centram.



Inficēt USB, CD-ROM «izplatīšanu».



Atkritumu inspicēšanu (dumpster diving), u.c. uzbrukuma veidus.

Izmaksas

900 EUR + PVN par vienu uzbrukumu vai testu*.

*Vairāk par 5 grupām ir individuāls piedāvājums.