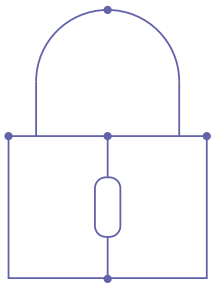
dots.

IT drošības apmācības un sociālā inženierija

Veicinām darbiniekos izpratni!

Datorlietotāju apmācībai 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 organizācijas datorsistēmām!

Ikviens darbinieks var kļūt 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.



dots.

Mēs iemācīsim:

Izveidot drošu paroli, neatstājot to publiski pieejamu un saprotot, kādēļ tā ir regulāri jāmaina.

Izprast un ievērot organizācijās noteiktos datortehnikas un informācijas sistēmu lietošanas noteikumus.

Atbildīgi un drošā veidā lietot mobilās ierīces un sociālos tīklus internetā.

Identificēt „aizdomīgus" e-pasta sūtījumus un atbilstoši uz tiem reaģēt.

Apzināties, ka pats personīgi ir viens no potenciālajiem krāpnieku uzbrukumu mērķiem.

Kādi ir pakalpojuma veidi?

IT drošības apmācības, apvienojot sociālo inženieriju.

Sagatavošanās intervija ar IT vai uzņēmuma vadītāju par aktualitātēm, specifiskiem klienta riskiem, normatīvajiem u.c. jautājumiem.

Lietotāju apmācības un pārbaude - sociālās inženierijas demo uzbrukums/tests.

Mācību materiāli katram apmācību dalībniekam.

1 999,99 EUR + PVN

par vienas grupas (līdz 25 cilvēkiem) nodarbību un testu. Katra nākamā grupa: 375 EUR + PVN. Katrs nākamais grupas dalībnieks virs 25 cilvēkiem: 15 EUR + PVN.

Sociālās inženierijas testa vai viens uzbrukuma veids.

Pēc publiski pieejamās informācijas analīzes, veiksim telefona zvanu, iegūstot privāto organizācijas vai darbinieka informāciju.

Viltus e-pasta izsūtīšana ar saiti uz viltus lapu (phishing, jeb pikšķerēšana).

Fizisko piekļuves zonu pārkāpšana, piemēram, ar mērķi iegūt pieeju datortīkla pieslēgvietai vai datu centram.

Inficētu USB, CD-ROM «izplatīšana».

Atkritumu inspicēšana (dumpster diving) vai kāds cits uzbrukuma veids.

1 600,00 EUR + PVN

par vienu uzbrukuma veidu

IT drošības apmācības par šādām tēmām:

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

Sociālā inženierija - izplatītākās metodes, kā uzbrucēji spēj manipulēt ar cilvēkiem.

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

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

780,00 EUR + PVN

par vienas grupas (līdz 25 cilvēkiem) nodarbību un testu. Katra nākamā grupa: 375 EUR + PVN. Katrs nākamais grupas dalībnieks virs 25 cilvēkiem: 15 EUR + PVN.

dots.

Ieguvumi

Izglītoti
un informēti darbinieki neradīs draudus organizācijas datortīklam un tajā esošajai sensitīvajai informācijai.

Izpratīs
un ievēros organizācijā noteiktos datoru izmantošanas noteikumus.

Spēs
pamanīt «aizdomīgus» e-pasta sūtījumus un adekvāti uz tiem reaģēt.

Izveidos
drošu paroli, izprotot, kādēļ tā ir regulāri jāmaina

Apzināsies
ka arī viņš/viņa ir viens no potenciālajiem uzbrukuma mērķiem.

Atbildīgi
lietos sociālos tīklus un mobilās ierīces.

WeAreDots, SIA
Elizabetes iela 75, Rīga
Latvija LV-1050

+371 67509912
info@wearedots.com