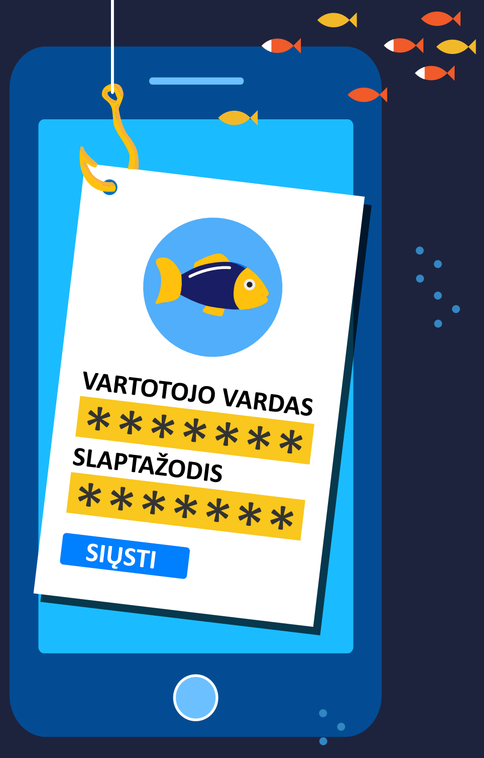
SU INTERNETU SUSIJĘ PAVOJAI

PATIKRINKITE KELIS KARTUS PRIEŠ SPAUSDAMI

Įrenginiui nustojus veikti, galite prarasti savo pinigus, asmeninę informaciją ir net saugomus duomenis. Neužkibkite!



KAIP TAI GALĖJO NUTIKTI?

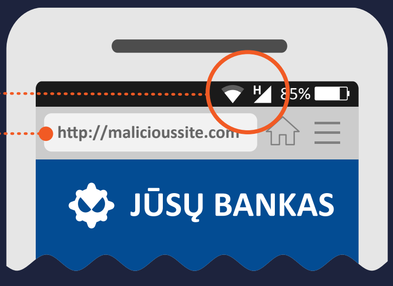
„FIŠINGO“ ATAKOS: Apsimetę patikimu subjektu jie priverčia naudotojus pasidalyti savo asmenine informacija. Tokios atakos vykdomos el. paštu, teksto žinutėmis ar per socialinių tinklų platformas.

NARŠYMAS SVETAINĖSE: Jūsų mobilusis įrenginys gali pasigauti virusą jums tiesiog apsilankius nesaugioje svetainėje.

FAILŲ PARSISIUNTIMAS: El. laiške gali būti kenksmingų nuorodų ar priedų.

KODĖL TAI VEIKSMINGA?

Mobilieji įrenginiai YRA NUOLATOS PRISIJUNGĘ prie interneto.



Pagrindinė priežastis yra MAŽESNIS ĮRENGINIO EKRANAS. Mobiliosios naršyklės rodo URL adresą riboto dydžio ekrane, todėl sunku pamatyti, ar domenas yra tikras.

BESĄLYGINIS NAUDOTOJŲ PASITIKĖJIMAS mobiliojo įrenginio asmeniškumu.

KĄ GALITE PADARYTI?

Būkite budrūs, jei įmonė atsiunčia jums SMS žinutę arba skambina prašydama asmeninės informacijos. Žinutės ir (arba) skambučio tikrumą galite patikrinti paskambinę įmonei jos oficialiu telefono numeriu.

https://

Naršydami internete per savo mobilųjį įrenginį įsitikinkite, kad jūsų ryšys apsaugotas jungiantis HTTPS protokolu. Tai visada galite patikrinti pažiūrėję į URL adreso pradžią.

Niekada nespauskite nuorodos ar priedo nepageidaujamame el. laiške ar SMS žinutėje. Nedelsdami juos ištrinkite.

^BE:%}
W@RY
*)Z#$=

Būkite budrūs, jei svetainės, kurioje apsilankėte, tekste yra daug gramatinių ar rašybos klaidų, taip pat jei svetainės rezoliucija yra labai maža.

Jei įmanoma, įdiekite mobiliesiems įrenginiams skirtą saugumo programėlę, kuri įspės jus apie bet kokią įtartiną veiklą.

EUROPOL EC3 European Cybercrime Centre

cert·lt

#MobileMalware