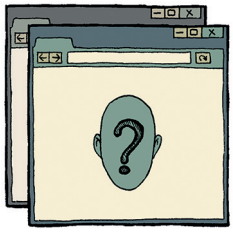
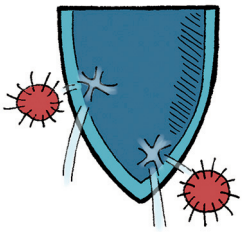
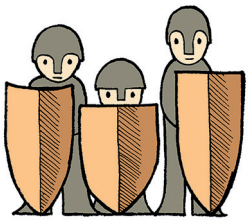


Privātais logs



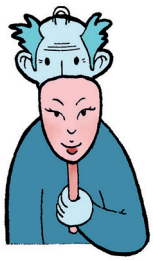
Antivīruss

CAPTCHA



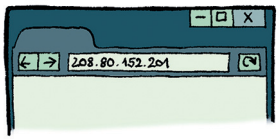
CSIRT

Digitālā pēda



Uzmākšanās tiešsaistē

Urķis

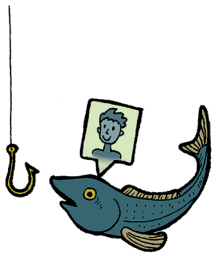


IP adrese

Kiberterors

Nomofobija

Drošības ielāps



Pikšķerēšana

Pirātisms

Šifrējošie izspiedējvīrusi

Maršrutētājs

Ķēdes vēstules

Pexeso

Spēlētāju skaits: 2 un vairāk
Spēlētāju ieteicamais vecums: 3-99 gadi

2 × →

Drukāšanai: uz abām pusēm (*duplex*)
Mērogs: reālais izmērs (100%)

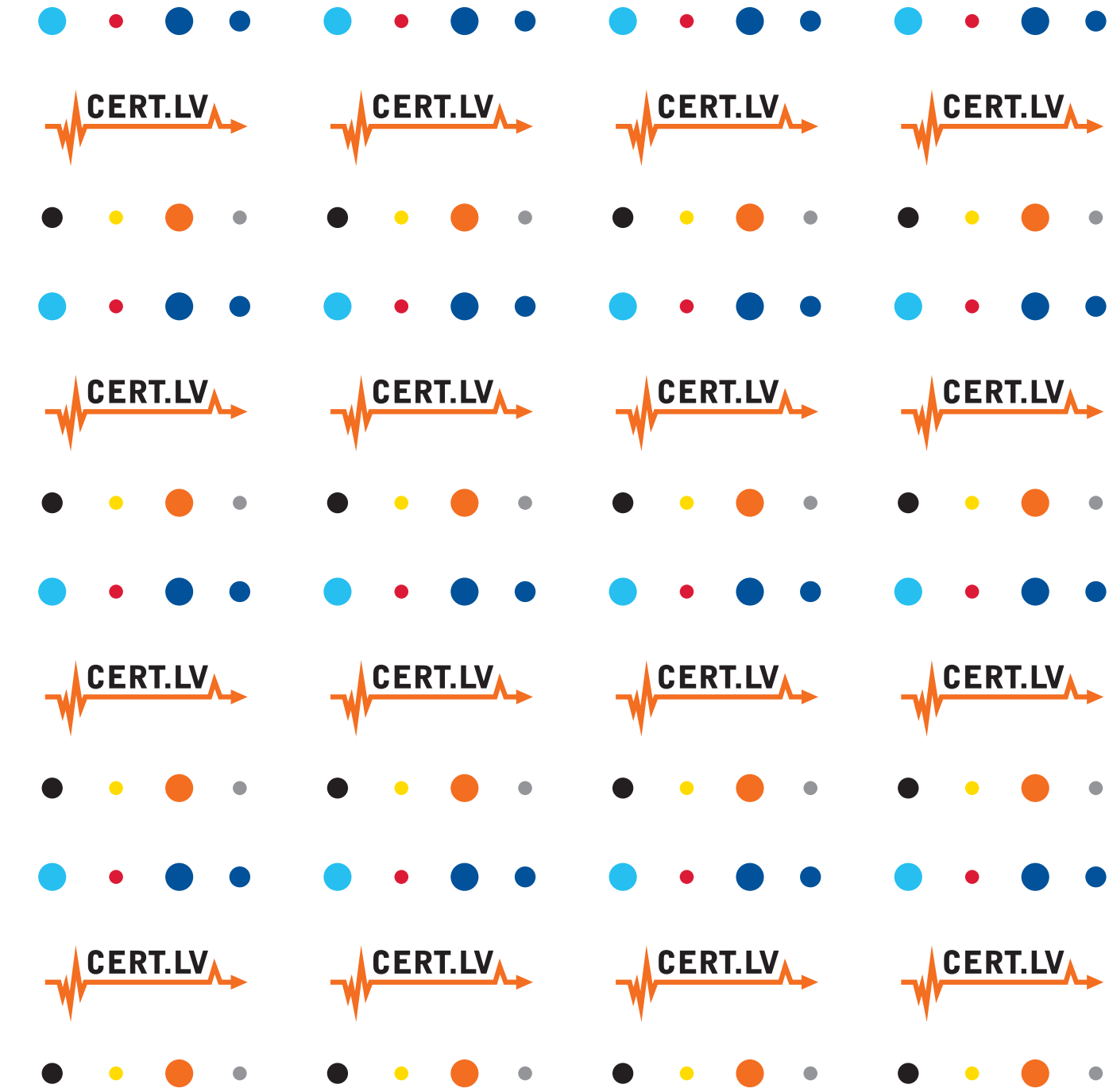
Spēles noteikumi:
Vispirms sajauciet kārtis, tad izkārtojiet tās pamīšus ar zīmējumu uz leju tā, lai neviens no spēlētājiem neredzētu attēlus. Pēc tam spēlētāji rindas kārtībā izvēlas 2 kārtis un apgriež tās, visiem redzot, otrādi – ar attēliem uz augšu. Ja abi attēli sakrīt, tad spēlētājs abas kārtis patur sev, un izvēlas nākamo kartīšu pāri. Ja attēli uz abām kārtīm nesakrīt – spēlētājs tās novieto atpakaļ ar zīmējumu uz leju, un spēli turpina nākamais spēlētājs. Spēle beidzas, kad visi attēlu pāri ir atrasti. Spēles uzvarētājs ir tas, kuram ir izdevies savākt visvairāk pāru.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CZ.NIC | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

Materiāls latviešu valodā tulkots sadarbībā ar CERT.LV.

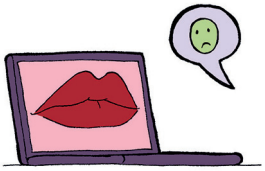


CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

cz.nic | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

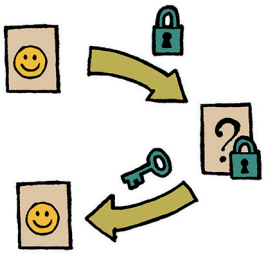
Dalīšanās



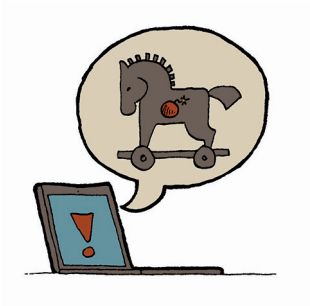
Sekstings

Privātums

SPAM

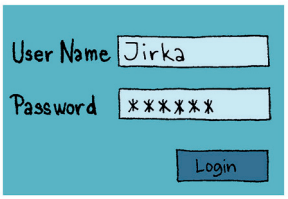


Kriptogrāfija

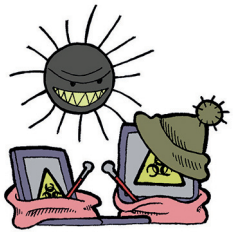


Trojas zirgs

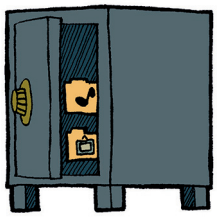
Uzbrukums



Lietotājvārds / parole



Vīruss



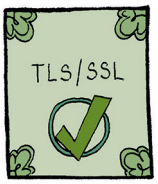
Datu rezerves kopija

"Zombiju" datori

DNSSEC

Urķuslazds

Kibernoziegums



TLS / SSL sertifikāts

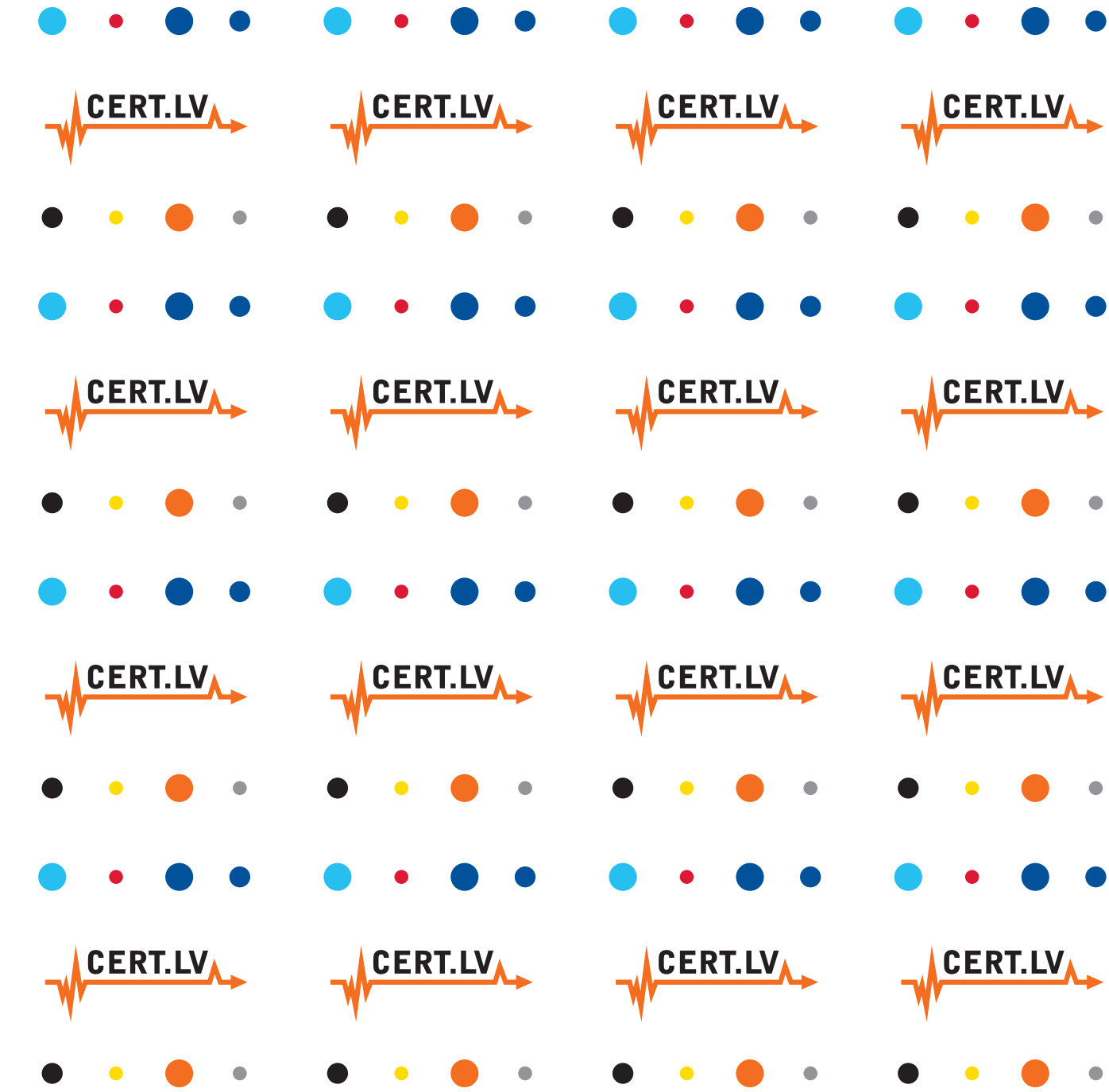
Wi-Fi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

cz.nic | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

Materiāls latviešu valodā tulkots sadarbībā ar CERT.LV.



CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

cz.nic | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

Antivīruss

Tā ir datorprogramma, kas darbojas līdzīgi kā mūsu vecāki – mēģinot mūs pasargāt no saslimšanas. Vecāki var rīkoties divējādi. Viņi mūs aizved pie daktera, ja esam jau sākuši klepot, lai noskaidrotu, cik nopietni tas ir un vai esam saķēruši kādu vīrusu, kā arī viņi neļauj mums spēlēties ar draugu, kurš ir apslimis, lai arī mēs nesaslimtu.. Antivīrusa programma strādā līdzīgi. Tā pārbauda mūsu datoru, lai noskaidrotu, kāds ir tā veselības stāvoklis. Tāpat programmatūra cenšas mūsu iekārtu pasargāt no vīrusiem ar ko aplipušas citas programmas vai iekārtas, piemēram, pārbaudot vai datorspēlē, ko gribam lejupielādēt, arī nav kāds vīruss.

Uzbrukums

Tāpat kā mēs regulāri apmeklējam zobārstu, lai pārbaudītu zobu veselību, tāpat mums regulāri vajadzētu veikt arī pārbaudes mūsu datoram, telefonam un planšetei. Iekārtas remonts varētu būt tikpat sāpīgs, kā ielaists caurums zobā. Ja mēs regulāri neuzstādīsim atjauninājumus, un lejupielādēsim programmas no neoficiālām vietnēm, mēs padarīsim savas iekārtas viegli pieejamas uzbrucējiem. Veiksmīga uzbrukuma gadījumā ļaundaris var izmantot mūsu iekārtu, lai izsūtītu citiem mēstules, lai padarītu mūsu iekārtu nelietojamu, kā arī, piemēram, lai uzlauztu mūsu skolas mājaslapu vai izzagtu naudu no vecāku bankas konta. Lai tas nenotiktu, mums jāseko līdzi mūsu iekārtu veselībai, regulāri jāuzstāda atjauninājumi un jāizvairās lejupielādēt programmas no neoficiālām mājaslapām. Tāpat vajadzētu rūpēties arī par antivīrusa programmas atjauninājumiem.

Datu rezerves kopija

Datu rezerves kopija nozīmē saglabāt informāciju, kas atrodas mūsu datorā, telefonā vai kur citur, uz citām ārējām un drošām iekārtām. Tas mums palīdzēs gadījumos, ja kāds ļaundaris mums draudēs izdzēst visu mūsu datorā saglabāto informāciju – bildes, referātus, mūziku u.c. (līdzīgi kā aprakstīts šifrējošā izspiedējvīrusa gadījumā). Tas pasargās arī gadījumos, ja mūsu dators vienkārši saplīsīs. Tiešsaistes servisi, jeb tā dēvētie mākoņpakalpojumi, piemēram, Failiem.lv, Mozy, Dropbox, Carbonite, Google Drive - ir viens no labākajiem risinājumiem, kur uzglabāt mazāk svarīgu informāciju. Noderīgi, ka šiem mākoņpakalpojumiem mēs varam piekļūt no jebkuras vietas. Slepenu un mums svarīgu informāciju (piemēram, personas datus) vajadzētu glabāt uz ārējiem cietajiem diskiem, kas aizsargāti ar paroli.

CAPTCHA jeb cilvēktests

Hakeri var izstrādāt programmas, kas nenogurstoši izmēģina dažādas paroļu kombinācijas, lai piekļūtu svešai informācijai. Šīs programmas dēvē arī par „botiem" vai „zirnekļiem". Botu izmantošanai kiberuzbrukumos ir daudz priekšrocību, salīdzinot ar cilvēkresursiem, bet arī viens liels trūkums. Boti atpazīst tikai perfekti uzrakstītas rakstzīmes un burtus. Tāpat tie nespēj sazīmēt, kā izskatās, piemēram, koki, ziedi vai dzīvnieki. Cilvēks, atšķirībā no botiem, atpazīs „B" burtu arī tad, ja tam trūks kāda maza detaļa, vai tas būs uzrakstīts šķībi, kā arī cilvēkam nebūs problēmu attēlā atpazīt ziedus, cilvēkus, kokus un citas detaļas. Boti šobrīd to vēl nespēj. CAPTCHA palīdz atšķirt botus no cilvēkiem. Līdz ar to CAPTCHA bieži tiek izmantota mājaslapās kā papildu drošības līdzeklis, lai boti nevarētu „atšifrēt" lietotāju paroles un piekļūt viņu kontiem.

Ķēdes vēstules

Ļoti ticams, ka ar šo jūs esat jau saskārušies. Piemēram, jūs saņemat interesantu ziņu no kāda drauga, sākat lasīt un tad pēkšņi parādās tāda frāze kā „Nosūti šo ziņu tālāk, savādāk Tava veiksme Tevi pametīs!". Jo biežāk uz šādiem stāstiem reaģēsiet, jo biežāk tādus saņemsiet. Ķēdes vēstules, diemžēl ir arī lielisks veids, kā masveidā izplatīt viltus ziņas, piemēram, par bērniem, kuriem šķietami nepieciešama līdzcilvēku palīdzība, vai kucēniem, kurus draud iemidzināt. Ja ziņas jums šķiet ļoti interesantas vai neparastas, vispirms pārbaudiet to ticamību – vai tās nav pilnībā vai daļēji izgudrotas pasaciņas. Ja papildu informācija nekur citur vairāk nav pieejama, vislabāk būt piesardzīgiem un ar saņemto informāciju tālāk nedalīties.

CSIRT

CSIRT ir saīsinājums: Cyber Security Incident Response Team, kas apzīmē speciālistu komandu, kas ir atbildīga par drošību, līdzīgi kā policija. Tikai atšķirībā no policijas, CSIRT speciālisti rūpējas par drošību kibertelpā, - par datoriem un serveriem, kas pievienoti internetam. Gadījumos, kad kibertelpā notiek incidents – CSIRT komanda strādā pie tā, lai noteiktu incidenta cēloni un par to laicīgi informētu citas CSIRT komandas citās valstīs, kuras arī varētu būt apdraudētas. Tādā veidā CSIRT komandas mēģina izvairīties no potenciāliem incidentiem visā pasaulē. Līdzīgi kā policija neapsargā katru gājēju pāreju, arī CSIRT komanda nevar visur atrasties vienlaicīgi. Līdz ar to ir svarīgi arī katram pašam rūpēties par savu drošību digitālajā vidē. Latvijā CSIRT komanda ir CERT.LV.

Emocionālā vardarbība internetā (arī kiberterors)

Ja kāds salauzīs mūsu pildspalvu vai saplēsīs mūsu T-kreklu, mūsu vecāki to noteikti pamanīs un atpazīs kā pāri darījumu un noteikti palīdzēs šo situāciju risināt. Taču, ja kāds pret mums vērš emocionālo vardarbību internetā –vecākiem ir daudz grūtāk vai pat neiespējami to pamanīt. Emocionālā vardarbība var izpausties, piemēram, kā kaitinošas ziņas nakts vidū, vai ļaunu klasesbiedru / nepazīstamu cilvēku mēģinājumi mūs sāpināt internetā, - sūtot šausminošas bildes, piespiežot mūs darīt lietas, ko nevēlamies, vai arī vienkārši smejoties par mums. Ja jūtam, ka nevaram atrast risinājumu paši, vai arī nevēlamies to lūgt ne vecākiem, ne skolotājiem – pastāv iespēja lūgt palīdzību anonīmi. To var paveikt, atverot interneta pārlūkā Latvijas Drošāka interneta centra mājas lapu https://drossinternets.lv/lv/questions, kurā var lūgt palīdzību, vai zvanot uz uzticības tālruni 116111 – uzticības tālruņa konsultācijas ir anonīmas. Ja tā jutīsies drošāk, meklējot informāciju internetā izmanto incognoto režīmu.

Kibernoziegums

Diemžēl, ir iespējams nodarīt pāri citiem, izmantojot tikai datoru. Bieži cilvēkus mēdz apbēdināt ar sliktām ziņām, biedējošām fotogrāfijām vai draudiem. Ar datora palīdzību un interneta pieslēgumu mūsdienās var nozagt naudu no citu cilvēku banku kontiem. Ikviena darbība internetā, kas nodara pāri citiem, var tikt saukta par kibernoziegumu. Ar šīs atmiņas spēles palīdzību vēlamies jūs iepazīstināt ar kibernoziegumu dažādajām sejām: izspiedējvīrusiem, datorvīrusiem, Trojas zirgiem, sekstingu, kiberterorismu vai "zombiju" datoriem. Ir ļoti svarīgi cīnīties pret šādiem uzbrukumiem, piemēram, ziņojot par tiem CERT.LV.

Digitālā pēda

Informācijas publicēšanu internetā varētu salīdzināt ar šīs informācijas (piemēram fotogrāfijas) neskaitāmu kopiju izdrukāšanu un izdalīšanu cilvēkiem lidostā. Pēc tam lidostas apmeklētāji katrs ar savu kopiju iekāpj dažādās lidmašīnās un aizlido katrs uz savu pasaules malu. Ir tikpat kā neiespējami prognozēt, kur šī informācija beigās nonāks, kurš to izlasīs,vai tā jebkādā veidā tiks izmainīta un kā tā tiks izmantota tālāk. Ja mēs uzrakstītu savu adresi uz katras no šīm kopijām, agrāk vai vēlāk kāds pie mūsu durvīm var arī pieklauvēt un pieprasīt mūsu uzmanību, - jo svešiniekam var šķist, ka pēc iepazīšanās ar izplatīto informāciju, viņš mūs pazīst. Mums ir jāpatur prātā, ka visu, ko mēs publicējam internetā, izmantojot telefonu, datoru vai planšeti – nekad nevarēsim vairs izdzēst. Informācija tīmeklī paliks mūžīgi, un pat vecāki nespēs palīdzēt.

Domēna vārdu sistēmas drošības paplašinājums jeb DNSSEC (*Domain Name System Security Extension*)

Zvanot mammai, mēs diez vai no galvas atceramies viņas telefona numuru. Tā vietā telefona kontaktu sarakstā mēs atrodam apzīmējumu „Mamma" un paļaujamies uz to, ka telefons zinās mammas numuru. Līdzīgi strādā DNS. Pateicoties DNS mēs varam interneta pārlūka adrešu laukā rakstīt mamma.lv, nevis tā vietā vietnes pilno IP adresi: 95.173.213.36. Dators pārtulkos mamma.lv cipariskā formātā, sauktā par IP adresi, un parādīs mums mūsu izvēlēto mājas lapu. Laikā, kad tika radīts DNS, internets bija drošāka vieta, bet, pieaugot interneta lietotāju skaitam, drošība pakāpeniski samazinās. DNSSEC sniedz garantiju, ka, ierakstot interneta vietnes adresi mamma.lv, jūs sasniegsiet vēlamo mājas lapu, un nevis kādu citu krāpniecisku vai inficētu vietni.

Kriptogrāfija

Datu šifrēšana jeb kriptogrāfija apraksta procesu, kad saprotama informācija tiek ar nolūku pārveidota nesaprotamā. Nošifrētā informācija atkal var tapt salasāma, ja lasītājs zina pareizo atslēgu. Mēs varam nošifrēt sev svarīgu informāciju gan uz cietā diska, gan uz tādām pārvietojamām

CERT.LV Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CZ.NIC | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

ierīcēm kā zibatmiņa. Tāpat mēs varam šifrēt arī visu mūsu tiešo komunikāciju – ziņas un e-pastus. Vēl viens šifrēšanas ceļš ir izmantot virtuālo privāto tīklu (VPN - virtual private network), ko mēs varam salīdzināt ar tuneli, ko zina tikai tie, kas to lieto. Šifrēšana tiek izmantota arī mājas lapās. Mājas lapas, kas šifrē lietotāju ievadīto datu plūsmu ir tās, kurām vietnes adrese sākas ar https, nevis – http, kā arī interneta pārlūkprogrammā, pie adreses sākuma, redzama zaļa slēdzene.

Uzmākšanās tiešsaistē

Kāds izveido kontaktu ar iepriekš izvēlētu personu internetā, un pēc tam, kad izveidota šķietama draudzība tiešsaistē, tiks ierosināts satikties arī dzīvē, piemēram, lai kopā uzspēlētu video spēles vai apskatītu kucēnus. Var tikt ierosināti visdažādākie iemesli, lai satiktos. Klātienē ļaundaris var fiziski ietekmēt upuri, uzņemt bildes ar viņu vai arī censties pārliecināt pievienoties teroristu vai cita veida ekstrēmistu grupējumam. Tie ir tikai daži no apdraudējumiem. Tādēļ vienmēr, pirms tiecies ar kādu internetā iepazītu personu, noteikti par to pastāsti saviem vecākiem, draugiem vai kādai citai uzticības personai. Svarīgi ar sev tuvajiem cilvēkiem sazināties arī uzreiz pēc satikšanās ar internetā iepazīto svešinieku. Esi piesardzīgs, tādēļ nekad nepiekrīti tikties nomaļā vietā vai pie svešinieka mājās.

Hakeris (arī Urķis)

Hakeri var salīdzināt ar zagli, tikai viņš neielaužas mājās un bankās, vicinādams ieroci, bet gan datoros un serveros, izmantojot programmas. Ir neskaitāmi veidi, kā hakeris var iekļūt mūsu iekārtās. Līdzīgi kā zaglis, kurš var durvis atslēgt ar viltus atslēgu, ierāpties dzīvoklī caur logu, vai arī izdomāt ticamas pasaciņas, lai mājas īpašnieks pats viņu uzaicinātu iekšā, arī hakeris var izmantot dažādus ceļus, lai piekļūtu jūsu datoram. Viņi izmanto vīrusus, Trojas zirgus, pikšķerēšanas lapas, izgudroja stāstus, ko izsūta rakstiskā formā (SMS, e-pasts u.c.), un citas metodes, kas klasificētas kā kibernoziegums. Hakeri nav tikai ļauni, ir arī „baltie hakeri", kas strādā plecu pie pleca ar labajiem spēkiem, piemēram, ar CERT.LV. Sliktos hakerus kiberpasaulē mēdz dēvēt arī par „uzlauzējiem".

Urķuslazds (*Honeypot*)

Kad mums sāk traucēt bišu un lapseņu uzmanība, kad to dēļ vairs pat nevaram mierīgi notiesāt saldējumu, mēs varam izmantot salīdzinoši vienkāršu risinājumu – tuvumā novietot podu ar medu, kas pievilinās bites un lapsenes, tādā veidā novirzot to uzmanību prom no mums. Internetā urķuslazdi strādā līdzīgi. Uzbrucēji regulāri izgudro jaunas ļaunatūras, tikmēr labie spēki nepārtraukti cenšas mūsu iekārtas no tām pasargāt. Tiklīdz tiek atklāta jauna ļaunatūra, tiek izlaists arī tās ielāps vai jauna / uzlabota programmas versija. Urķuslazdu uzdevums ir šīs jaunās ļaunatūras noķert, lai labie spēki var tās pēc iespējas ātrāk izpētīt un atrast tām „zāles".

Privātais logs (*Incognito Window*)

Izmantojot privāto logu jeb „Incognito Window", lietotājs nodrošina sev lielāku privātumu internetā. Piemēram, šajā režīmā interneta pārlūkprogrammma nesaglabā informāciju par lietotāja veiktajiem vaicājumiem un apmeklētajām tīmekļa vietnēm. Gadījumā, ja vēlies saviem vecākiem internetā atrast dzimšanas dienas dāvanu, taču nevēlies, lai pēc meklēšanas procesa Tevi vajā uzlecošas reklāmas par šīm dāvanām, Tev nepieciešams uzklikšķināt uz izvēles pogas labajā augšējā stūrī interneta pārlūkprogrammā (trīs punkti vai trīs strīpiņas, atkarībā, kādu pārlūku izmanto) un tad izvēlēties „Incognito Window". Tu vari izmantot arī klaviatūras piedāvātos īsceļus: Ctrl + Shift + N Google Chrome un Opera interneta pārklūkporgrammās, un Ctrl + Shift + P Internet Explorer un Mozilla Firefox interneta pārlūkprogrammās.

IP adrese

IP adrese ir kā mūsu drauga vai vecāku telefona numurs. Katrai personai ir savs, un mēs, protams, nevaram no galvas atcerēties visus. Šie numuri satur vairākus datu blokus, piemēram, pēc tiem var noteikt valsti, kurā mobilā telefona numurs reģistrēts un kuru sakaru operatoru izmanto. Cilvēka atmiņa nespēj iegaumēt visus numurus, taču gribam zināt gan kas mums zvana, gan kam mēs varam piezvanīt atpakaļ. Mēs arī necenšamies draugu numurus iegaumēt, jo vieglāk taču ir saglabāt tos telefonā un nosaukt drauga vārdā vai iesaukā. Šie vārdi ir līdzīgi arī interneta vietņu nosaukumiem. Lai dators zinātu, kur atrast datus un informāciju par pieprasīto vietni, tāpat kā telefonu numuru gadījumā tam ir jāatpazīst valsts, izmantotais Interneta pakalpojuma sniedzēja operators un jāsazīmē vieta, kur dati ir noglabāti utt.

Nomofobija

Mūsdienās daļai cilvēku izveidojusies atkarība no viedierīcēm un patstāvīgas būšanas tiešsaistē. Šiem cilvēkiem piedēvē „nomofobiju" jeb bailes palikt bez viedtālruņa. Cilvēki, kuri ir atkarīgi no viedierīcēm, parasti vienmēr ir pieejami un gandrīz momentā atbild uz mūsu ziņām, labprāt komunicē ar mums, izmantojot telefonu, cik ilgi vien mēs to vēlamies, tāpat arī pārspīlēti regulāri publicē bildes un ziņas savos sociālajos tīklos. Protams, ir lieliski visu laiku būt tiešsaistē un pieejamam, taču šie cilvēki parasti neievēro sev tuvos līdzcilvēku reālajā pasaulē. Ar nomofobiju sirgstošie atsakās doties uz pasaules skaistākajām vietām, ja pastāv iespēja palikt bez zonas vai interneta pieslēguma.

Pikšķerēšana

Termina „pikšķerēšana" izcelsme saistīta ar angļu valodas vārdu „zveja" (phishing). Idejiski uzbrucējs tiek salīdzināts ar „zvejnieku", bet interneta lietotāji ar „zivīm". Ja mēs vēlamies nodegustēt kaut ko jaunu un iepriekš nebaudītu, tad vispirms mums vajadzētu to kārtīgi pārbaudīt un izķidāt, lai saprastu, vai iekšā nav paslēpts kāds „āķis". Un ja gadījumā, mēs neesam līdz galam pārliecināti, tad būtu ieteicams vērsties pie kāda ar lielāku pieredzi. Tādēļ ir svarīgi e-pastā saņemtos pielikumus lejupielādēt tikai no sev tuviem un pazīstamiem cilvēkiem, kam uzticamies. Tāpat vajadzētu izvairīties ievadīt savas paroles vietnēs, kas parādās vai „uzlec" pēkšņi un izskatās aizdomīgas. Ievadot savas paroles internetā, mums vienmēr vajadzētu vispirms pārliecināties, vai pārlūkā redzamā adrese sakrīt ar to, kuru vēlējāmies apmeklēt, it īpaši, ja tas ir tiešsaistes veikals, kurā vēlamies izdarīt kādu pirkumu.

Pirātisms

Lielākā daļa sabiedrības uzskata, ka nelegāla filmu un spēļu lejupielāde ir pieņemama. Bet tā nav. Iztēlosimiessituāciju - esam uzzīmējuši skaistu bildi, un skolotāja apgalvo, ka varam to pārdot par 1000 EUR mākslas darbu izstādē pēc nedēļas. Tas ir mūsu darbs, mēs esam tā autori un mums vienīgajiem ir tiesības to tālāk pārdot. Tikmēr mūsu klasesbiedrs šo darbu veiksmīgi nokopē un piedāvā to pārdot tikai par 500 EUR. Kad tiekam līdz izstādei, neviens vairs nevēlas mūsu darbu iegādāties, jo visi to jau ir nopirkuši par daudz lētāku cenu. Tas nav pareizi. Ja šāda situācija nav patīkama mums, tā nebūs patīkama arī citiem. Risinājums ir atturēties lejupielādēt filmas un spēles, kas publicētas internetā bez oriģinālā autora atļaujas. Izvēloties nelegālu saturu mēs apzogam paši sevi, jo oriģinālajiem darbu (mūzikas, filmu, spēļu) autoriem, netiks paredzētā atlīdzība un viņiem vairs nebūs līdzekļu jauna, oriģināla satura radīšanai.

Privātums

Pat ja varētu šķist, ka mūsu datorā notiekošo neviens neredz, tā īsti nav taisnība. Mūsu e-pasti, bildes un cita veida dati bieži vien tiek glabāti uz citiem serveriem, kur tiem var piekļūt citi cilvēki. Nodrošināt privātumu iekārtai, kas pievienota internetam, ir diezgan sarežģīti. Jo vairāk šķēršļu hakerim būs jāpārvar, jo sarežģītāk un grūtāk būs piekļūt mūsu datiem. Ir svarīgi neizmantot nepārbaudītus servisus privātu datu glabāšanai, ir svarīgi atjaunot mūsu īpašumā esošās iekārtas, t.sk. arī maršrutētājus, kā arī izmantot drošas paroles (piemēram, paroļu frāzes u.tt.). Ne mazāk svarīgi ir pievērst uzmanību informācijai, ko par sevi publicējam internetā, jo tā var atklāt gan mūsu atrašanās vietu, mūsu ikdienas gaitas, gan mūsu pārdzīvojumus, ko kāds var izmantot savā labā.

Šifrējošie izspiedējvīrusi

Gadījumā, ja ievadam trīs reizes nepareizi PIN kodu savā telefonā, mūsu SIM karte tiek bloķēta un, lai to atbloķētu, mums jāievada garš un sarežģīts numurs (PUK), taču parasti tas mums ir pieejams vai arī varam to iegūt no sava mobilā telefona operatora. Šifrējošais izspiedējvīrus ir daudz ļaunāks, jo tas var nobloķēt pieeju visiem mūsu datiem gan telefonā, planšetē, gan datorā, bet atslēga pieejama tikai ļaundariem, kas par to prasa bargu samaksu. Tādā veidā mēs varam pazaudēt visas mūsu ziņas, attēlus un citus datus. Katru reizi, kad internetā saskaramies ar izspiešanas mēģinājumu vai draudiem, mums par to ir pēc iespējas ātrāk jāziņo saviem vecākiem, jāuzņem ekrānšāviņš ar draudu vēstuli un jāinformē par to arī CERT.LV un Valsts policija. Nekādā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CZ.NIC | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

Materiāls latviešu valodā tulkots sadarbībā ar CERT.LV.

gadījumā nemaksājiet ļaundariem, to nevajadzētu darīt arī jūsu vecākiem. Vienmēr ir labāk atdzīt, ka esat apmeklējis neatļautas vietnes, nekā maksāt ļaundariem.

Maršrutētājs

To varētu salīdzināt ar kasti, kas ļauj mums pieslēgties internetam no mūsu telefona, planšetes un datora. Ja mēs šo „kasti" atstājam ilgi bez uzraudzības, tā var „saslimt", jo tāpat kā mūsu dators, arī tā var būt ievainojama, un tāpēc regulāri nepieciešams veikt tās programmatūras atjauninājumus. Ne tikai mēs, lietotāji, bieži piemirstam parūpēties par „kastes" veselību, to piemirst arī tās ražotāji. Tas ir diezgan izplatīti, ka „kastēm" tiek atklātas ievainojamības, taču atjauninājumi tā arī nav pieejami. Šādas „kastes" var būt pilnas ar vīrusiem un inficēt mūsu mobilos telefonus, datorus un citas iekārtas, par kurām mēs, iespējams, rūpējamies. Lai izvairītos no šādām situācijām, mēs varam lūgt saviem vecākiem iegādāties tikai tādus maršrutētājus, kam regulāri iznāk atjauninājumi, piemēram, MikroTik.

Drošības ielāps

Kad mēs ieplēšam miltu iepakojumu, pa tā plaisu laukā sāks birt milti. Līdzīgi notiek ar datoriem. Ja datorā kaut kas ir saplīsis – var sākt birt laukā mūsu dati, piemēram, paroles, bildes, ziņas, ar kurām apmaināmies un cita svarīga informācija. Kad tas notiek, datoram pēc iespējas ātrāk ir nepieciešams drošības ielāps. Tas nozīmē ražotājam radīt un lietotājam instalēt jaunu programmatūras daļu, kas aizlāpa vecajā programmā atrasto caurumu. Šo procesu sauc par „atjaunināšanu". Drošības ielāps tiek ievietots datorā, telefonā vai planšetēkonkrētām programmām, tai skaitā arī operētājsistēmām. Lai drošības ielāps pēc iespējas ātrāk sasniegtu savu mērķi, mums ir nepieciešams regulāri lejupielādēt un instalēt jaunākās programmatūru / lietotņu versijas.

Sekstings

Sekstings ir lielisks piemērs mūsu „digitālajam pēdu nospiedumam", kas var izrādīties diezgan postošs. Daži cilvēki sūta saviem draugiem vai mīļotajiem bildes, kurās redzami apakšveļā vai pat bez tās. Šīs bildes atgūt ir tikpat kā neiespējami un bieži tās tiek bez atļaujas parādītas tālāk arī plašākam cilvēku lokam – citiem draugiem, klases biedriem utt. Sūtot šādas bildes, lielākā daļa cilvēku pat neaizdomājas, ka tās var nonākt arī svešās rokās. Bet brīdī, kad tas notiek, sūtītāju var pārņemt tik liela kauna izjūta, ka ideja par palīdzības lūgšanu netiek pat apsvērta. Ja gadījumā kādam ir sanācis šādi kļūdīties, un tālāk šis cilvēks tiek par to izsmiets un pazemots, to sauc par emocionālo vardarbību vai "kiberteroru". Vēl vairāk – bildes publicēšana bez mūsu atļaujas skaitās nelikumīga, tādēļ pastāv iespējas sevi arī oficiāli aizstāvēt, par ko vairāk varat uzzināt, sazinoties ar Drossinternets.lv. Tomēr labākais risinājums vēl joprojām ir tiešsaistē publicēt tikai tādu informāciju, ar kādu mēs būtu gatavi dalīties ar visu klasi.

Dalīšanās

Mēs bieži vēlamies dalīties ar saviem dzīvestāstiem. Tas, protams, ir normāli, taču, to darot internetā, ir jārēķinās ar to, ka citi var sākt uzdot jautājumus. Mēs varam tikt arī izsmieti savas publicētās informācijas dēļ. Ja mēs nevēlamies, lai tā notiek, tad būtu ieteicams dalīties ar informāciju tikai ar tiem cilvēkiem, kuriem patiesi uzticamies. Mēs varam publicēt ziņas privātajā režīmā, kur tās varēs izlasīt tikai tie, kuriem būsim to atļāvuši. Tāpat mēs varam savas bildes un failus, ar ko vēlamies dalīties, ievietot speciāli tam izveidotā mapītē, kas aizsargāta ar paroli. Paroli tālāk dodam tikai tiem cilvēkiem, kam uzticamies.

Surogātpasts (SPAM)

Tā ir kaudze nevajadzīgas un liekas informācijas, kuru saņemam internetā vai caur īsziņām, un kuru nevēlamies redzēt. Pateicoties surogātpastam, ir viegli apmaldīties pašiem savā e-pastā un palaist garām svarīgu informāciju. Lai izvairītos no surogātpasta, mums jābūt uzmanīgiem, akceptējot vai piekrītot dažādiem noteikumiem internetā utt. Vienmēr ir svarīgi iepazīties ar noteikumiem un nosacījumiem, kurus grasāmies apstiprināt. Jā, mēs zinām, ka parasti šie noteikumi un nosacījumi var būt pat 100 lappuses gari, taču, pat, ja nelasi visu informāciju - atrodi noteikumos sadaļu, kas attiecas uz privāto datu aizsardzību un pārbaudi vai tajā minēts, ka tavi dati tiks izpausti trešajām personām, kā tie tiks aizsargāti un vai tiem var piekļūt vēl kāds.

TLS / SSL sertifikāts

Šie akronīmi ir saistīti ar kodēšanu, proti, vietņu šifrēšanu. Vietni, kurā datu plūsma tiek šifrēta, var atpazīt pēc tās interneta adreses, kas sākas ar „https" nevis vienkārši „http". Līdztekus tam, ka "https" protokols nodrošina drošāku datu ievadīšanu vietnē, tas arī ļauj pārbaudīt, vai vietne, kuru gribējām apmeklēt, patiešām ir tā, uz kuru mēs vēlējāmies doties. TLS / SSL sertifikāti var novērst dažādus pikšķerēšanas uzbrukumus, kas cenšas mūs ievilināt savās lamatās. SSL sertifikāts vienmēr tiek izmantots gadījumos, kad interneta pārlūkprogramma un serveris apmainās ar sensitīvu informāciju, piemēram, lietotājvārdu un paroli.

Trojas zirgs

Trojas zirgs bija liels, no koka veidots zirgs senajā Grieķu mitoloģijā, kurā bija paslēpti karavīri, kas vēlāk uzbruka un ieņēma Trojas pilsētu. Līdzīgu taktiku internetā izmanto arī ļaundari. Tie cenšas mūs pārliecināt, ka tas, ko viņi piedāvā, ir kaut kas noderīgs, interesants un mums nepieciešams. Lejupielādējot viņu atsūtīto failu uz mūsu datora un aiz tā ugunsmūra, mēs paši savā datorā ielaižam slēptu un krāpniecisku programmu, kuras mērķis ir atdarīt durvis ļaundarim un ielaist viņu mūsu iekārtā. Lai izvairītos no šādas muļķības, ko pieļāva arī trojieši, lejupielādējiet failus tikai no oficiālām interneta vietnēm un neatbalstiet pirātismu internetā.

Lietotājvārds / parole

Lietotājvārds un parole kalpo līdzīgi kā mūsu mājas atslēgas, un šīs atslēgas izmantošanu dēvē arī par autentifikācijas procesu. Savos lietotāju kontos mēs glabājam visdažādāko informāciju, kā arī šos kontus izmantojam saziņai ar saviem draugiem. Tādēļ ir svarīgi rūpēties par to drošību, lai tie netiktu nozagti. Kontu piekļuves parolēm vienmēr vajadzētu saturēt gan burtus, gan ciparus, kā arī speciālās rakstzīmes, piemēram – zvaigznīti. Paroles nevajadzētu pierakstīt uz papīra un glabāt iekārtas tuvumā, kā arī katram kontam vajadzētu savu, unikālu paroli. Kontiem, kas mums tiešām ir svarīgi, būtu ieteicams izmantot divfaktoru autentifikāciju, ko ir daudz sarežģītāk uzlauzt salīdzinājumā ar parolēm.

Vīruss

Kad esam slimi, viss ko vēlamies, ir palikt gultā, - mēs esam pārāk noguruši, lai apģērbtos, staigātu vai pat padzertos. Datoriem ir līdzīgi. Kad dators ir inficēts ar vīrusu, tā darbība var mainīties. Tie var būt lēnāki vai arī izpildīt komandas, kuras neesam tiem devuši. Inficēts dators var „aplipināt" arī citus datorus, dodot iespēju hakeriem uzbrukt lielākām organizācijām, tādām kā skolas, veikali, sabiedriskā transporta vietnes utt. Vīrusi var pārsūtīt hakeriem mūsu autentifikāciajs datus un citu informāciju par mūsu darbībām iekārtā, t.sk. privātas ziņas vai e-pastus. Lai no šādiem vīrusiem izvairītos, ir nepieciešams uz iekārtām aktivizēt un regulāri atjaunināt antivīrusa programmu.

Wi-Fi

Lielveikalos, restorānos, kafejnīcās, kā arī daļā autobusu un vilcienu ir iespējams pieslēgties bezvadu internetam, pazīstamam arī kā Wi-Fi. Publiskais Wi-Fi tīkls tiek veidots iespējami draudzīgs lietotājam, jo to ikdienā izmanto lielas ļaužu masas. Līdz ar to var arī loģiski secināt, ka drošība tam nav augstākajā līmenī. Gandrīz jebkurš prasmīgs hakeris var redzēt visu, ko darām publiskajā Wi-Fi tīklā - kādas vietnes apmeklējam, kādus kontus pārvaldām, un galu galā – kādas paroles un lietotājvārdus izmantojam. Tādēļ vajadzētu būt īpaši uzmanīgiem, pieslēdzoties publiskajam Wi-Fi tīklam, - sekojam līdzi, kādās vietnēs ievadām savus autentifikācijas datus, un ko sūtam, izmantojot šo tīklu.

"Zombiju" datori

„Spoku" datori atšķiras no normāliem datoriem ar to, ka tos savā pakļautībā tur ļaunie spēki, līdzīgi kā filmās par zombijiem. Hakeris ar ļauniem nolūkiem, izmantojot vīrusu, Trojas zirgu vai citu metodi, mūsu datorā var augšupielādēt programmu, kas pilnībā var pārņemt mūsu iekārtu savā kontrolē, mums to nezinot. Tas nozīmē, ka hakeris no mūsu iekārtas var sūtīt SPAM vēstules, izmantot to, lai izplatītu vīrusus, pelnītu ar reklāmām vai arī vienlaicīgi no vairākiem „spoku" datoriem apmeklēt kādu konkrētu vietni, pilnībā pārslogojot serveri un padarot vietni nepieejamu (to sauc par DDoS uzbrukumu).

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CZ.NIC | CZ DOMAIN REGISTRY

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

Materiāls latviešu valodā tulkots sadarbībā ar CERT.LV.