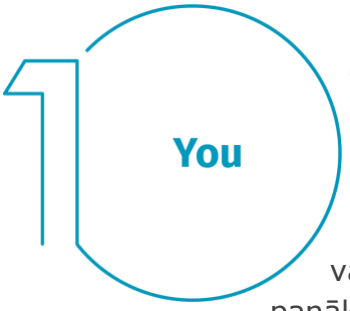
SANS SECURITY AWARENESS

5 galvenie soļi drošam darbam no mājām

Mēs saprotam, ka darbs no mājām dažiem no jums var būt kas neierasts un, iespējams, satraucošs, pielāgojoties jaunajai videi. Viens no mūsu mērķiem ir sniegt jums iespēju strādāt no mājām pēc iespējas drošāk. Tālāk ir aprakstītas piecas vienkāršas darbības drošam darbam. Vislabākais ir tas, ka visi šie pasākumi ne tikai palīdz aizsargāt jūs darba laikā, bet arī daudz labāk aizsargās jūs un jūsu ģimeni, nostiprinot kiberdrošību mājās.



Jūs: pirmkārt un galvenokārt, tehnoloģija vien nevar jūs pilnībā aizsargāt — jūs paši esat labākā aizsardzība. Uzbrucēji ir sapratuši, ka vienkāršākais veids, kā iegūt to, ko viņi vēlas, ir izvēlēties par mērķi tieši jūs, nevis datoru vai citas ierīces. Ja viņi vēlas iegūt jūsu paroli, darba datus vai kontroli pār jūsu datoru, uzbrucēji mēģinās apmānīt jūs, panākot, lai to nododat viņiem, bieži radot steidzamības sajūtu. Piemēram, viņi var jums piezvanīt, izliekoties par Microsoft tehniskā atbalsta dienesta pārstāvi, un apgalvot, ka jūsu dators ir inficēts. Vai varbūt viņi nosūtīs e-pasta ziņojumu, brīdinot, ka paku nevar piegādāt, un tādējādi liekot jums noklikšķināt uz kaitīgas saites. Visizplatītākie sociālās inženierijas uzbrukuma rādītāji ir aprakstīti tālāk.

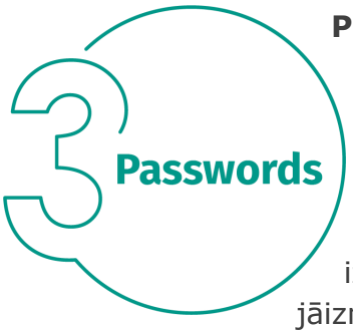
- Tas var būt kāds, kurš rada īpašu steidzamības sajūtu, bieži iedvešot bailes, iebiedējot, informējot par kritisku situāciju vai svarīgu termiņu. Kiberuzbrucēji labi prot izveidot pārliecinošus ziņojumus, kas, šķiet, nāk no uzticamām organizācijām, piemēram, bankām, valdības vai starptautiskām organizācijām.
- Uzbrukums var izpausties kā spiediens apiet vai ignorēt drošības politiku vai procedūras vai arī kā pārāk labs piedāvājums, lai būtu patiesība (nē, jūs neuzvarējāt loterijā!).
- Vai arī tā var būt ziņa, kas šķietami saņemta no drauga vai kolēģa, bet ziņas formulējums vai izteiksmes veids neatbilst šai personai.

Vislabākā aizsardzība pret uzbrukumiem esat jūs.

Mājas tīkls: gandrīz ikviens mājas tīkls sākas ar bezvadu (bieži dēvētu par Wi-Fi) tīklu. Tas ļauj visām jūsu ierīcēm izveidot savienojumu ar internetu bezvadu režīmā. Lielāko daļu mājas bezvadu tīklu kontrolē jūsu interneta maršrutētājs vai atsevišķs šim nolūkam izveidots bezvadu piekļuves punkts. Abas ierīces darbojas vienādi — pārraida bezvadu signālus, kuriem pievienojas mājas ierīces. Tas nozīmē, ka bezvadu tīkla drošība ir būtiska jūsu mājas aizsardzības sastāvdaļa. Lai nostiprinātu aizsardzību, mēs iesakām veikt tālāk minētās darbības.

- Nomainiet bezvadu tīklu kontrolējošās ierīces noklusējuma administratora paroli. Administratora konts ļauj jums konfigurēt jūsu bezvadu tīkla iestatījumus.
- Pārliecinieties, vai jūsu bezvadu tīklam var pievienoties tikai cilvēki, kuriem uzticaties. Dariet to, parūpējoties par spēcīgu aizsardzību. Tādējādi cilvēkiem būs nepieciešama parole, lai izveidotu savienojumu ar jūsu bezvadu tīklu, un pēc savienojuma izveidošanas viņu tiešsaistes darbības tiks šifrētas.
- Pārliecinieties, vai parole, ko cilvēki izmanto, lai pievienotos jūsu bezvadu tīklam, ir spēcīga un atšķiras no administratora paroles. Atcerieties, ka ikvienā no jūsu ierīcēm parole jāievada tikai vienreiz, jo tās saglabā un atceras paroli.

Vai nezināt, kā veikt šīs darbības? Pajautājiet savam interneta pakalpojumu sniedzējam, skatiet viņu tīmekļa vietni, dokumentāciju, kas bija pievienota jūsu bezvadu piekļuves punktam, vai arī apmeklējiet pārdevēja vietni.



Paroles: kad vietne lūdz jums izveidot paroli, izveidojiet spēcīgu paroli — jo vairāk rakstzīmju tā satur, jo spēcīgāka tā ir. Ieejas frāzes izmantošana ir viens no vienkāršākajiem veidiem, kā nodrošināt spēcīgu paroli. Ieejas frāze nav nekas vairāk kā parole, kas sastāv no vairākiem vārdiem, piemēram, "*bite medus balzams*". Unikālas ieejas frāzes izmantošana nozīmē, ka katrai ierīcei vai tiešsaistes kontam jāizmanto atšķirīga frāze. Tādējādi, ja viena ieejas frāze ir apdraudēta, visi pārējie konti un ierīces joprojām ir drošībā. Vai nevarat atcerēties visas ieejas frāzes?

Izmantojiet paroļu pārvaldnieku — specializētu programmu, kura droši glabā visas jūsu ieejas frāzes šifrētā formātā (un tai ir arī daudz citu lielisku iespēju!). Visbeidzot, iespējojiet divsoļu pārbaudi (dēvēta arī par daudzfaktoru autentifikāciju), kad vien iespējams. Šī metode izmanto jūsu paroli, bet arī pievieno otro soli, piemēram, uz viedtālruni nosūtītu kodu vai lietotni, kas jums ģenerē kodu. Divsoļu pārbaude, iespējams, ir vissvarīgākā darbība, ko varat veikt, lai aizsargātu savus tiešsaistes kontus, un tās lietošana ir daudz vienkāršāka, nekā varētu šķist.

Atjauninājumi: pārliecinieties, vai visos jūsu datoros, mobilajās ierīcēs, programmās un lietotnēs darbojas programmatūru jaunākās versijas. Kiberuzbrucēji pastāvīgi meklē jaunas ievainojamības problēmas programmatūrās, kuras izmantojat savās ierīcēs. Atklājot ievainojamības problēmas, viņi lieto īpašas programmas, lai šīs problēmas ļaunprātīgi izmantotu un uzlauztu jūsu izmantotās ierīces. Tikmēr uzņēmumiem, kas izveidojuši attiecīgās programmatūras, smagi jāstrādā, lai tās salabotu, izlaižot atjauninājumus. Nodrošinot, ka šie atjauninājumi tiek nekavējoties instalēti jūsu datoros un mobilajās ierīcēs, uzbrucējiem būs daudz grūtāk uzlauzt jūsu ierīces. Lai vienmēr izmantotu aktuālo versiju, vienkārši aktivizējiet automātisko atjaunināšanu, kad vien iespējams. Šis noteikums attiecas uz gandrīz jebkuru tehnoloģiju, kas tiek savienota ar tīklu, tai skaitā ne tikai jūsu darba ierīcēm, bet arī ar internetu savienotajiem televizoriem, mazuļu uzraudzības ierīcēm, drošības kamerām, mājas maršrutētājiem, spēļu konsolēm vai pat jūsu automašīnu.

Bērni/viesi: birojā jums visdrīzāk nav jāuztraucas, ka bērni, viesi vai citi ģimenes locekļi varētu izmantot jūsu darba klēpjdatoru vai citas darbam paredzētās ierīces. Pārliecinieties, vai ģimene un draugi saprot, ka viņi nedrīkst izmantot jūsu darbam paredzētās ierīces, jo viņi var nejauši izdzēst vai pārveidot informāciju vai arī, vēl sliktāk, nejauši inficēt ierīci.