Aina osavamalt koostatud õngitsuskirjad – kuidas vältida nende ohvriks langemist?

2 aastat tagasi - 18.06.2024 Autor: AM

Tänapäeval puutuvad kõik kokku õngitsuskirjadega – pettur püüab ohvrit kavalate nippide abil manipuleerida oma andmeid jagama. Kuidas neid e-kirju ära tunda?

Õngitsuskirjad on laialt levinud ja petturid lähevad nende koostamisel aina teadlikumaks. “Õngitsuskirja iseloomustab üleskutse millelegi klõpsata, näiteks mõnel kahtlasel lingil või manusel,“ selgitab Riigi IT Keskuse IT-abi vanemspetsialist Merle Kappak petuskeemi olemust.

Eksperdi sõnul on linkide puhul enamasti tegemist mõne veebisaidi võltsversiooniga, kus inimest üritatakse suunata sisestama oma kasutajanime ja parooli või muud isiklikku teavet, et siis seda infot ära kasutada. “Õngitsuskirjadele manustatud failid on aga peaaegu alati ründevara,” lisab ta ning toob mõned näiteid, kuidas õngitsuskirja ära tunda või hoopis selle ohvriks langemisel edasi käituda.

Õngitsuskirjade ohvriks võib langeda igaüks

IT eksperdi sõnul on tuleb tähelepanelik olla nii tööalaste meilide kui ka isiklike aadresside ja kontodega. Näiteks alles hiljuti puutus Kappak kokku juhtumiga, kus asutuse töötajaid said kirja justkui tuttavalt portaalilt, kuid saatja aadressi lõpus oli domeeni ".ee" asemel ".eu".

“Õngitsuskirjade saatjaks võib näiliselt olla kodupank, mõni avalik ametiasutus, tuttav teenusepakkuja või mõni üldtuntud ettevõte nagu Microsoft või Amazon,“ toob Kappak näiteid levinumatest võtetest. “Võidakse minna isegi nii kaugele, et üritatakse kehastada teie ülemust, kolleegi, sõpra või isegi pereliiget,“ lisab ta. Seetõttu tasub Kappaku sõnul alati veenduda saatja aadressi õigsuses ja olla tähelepanelik ebatavalise kirjastiili, kirjavigade ja tavapäratute soovide osas.

Kuidas kontrollida kirja autentsust?

“Vähimagi petukirja kahtluse puhul tuleks kirja saatjat mitu korda kontrollida ja mitte mingil juhul klõpsata linkidel või laadida alla manuseid. Julgustan kasutama veebiportaale, mis aitavad õngitsusi ja viiruseid sisaldavad lingid ja manused ära

tunda - üheks selliseks on näiteks virustotal.com," räägib Kappak ning juhendab, et postkasti jõudnud lingi puhul on heaks nipiks viia hiir selle kohale, nägemaks lingi tegelikku aadressi. Kui tegemist on tõesti tuttava saidiga, soovitab ekspert lingile klikkimise asemel võimalusel otsest navigeerimist ametlikule veebilehele.

Samuti toob ta välja, et kui meilis palutakse jagada isiklikke või tundlikke andmeid, nagu paroole või pangainfot, siis on üsna tõenäoliselt tegemist pettusega. "Ükski pank, ametiasutus ega usaldusväärne ettevõte ei palu paroole meili teel saadetud lingi kaudu jagada," rõhutab RITi IT-abi vanemspetsialist. Seetõttu soovitab kahtluse korral küsida täiendavat kinnitust kas saatja ametliku telefoni või veebilehe kaudu.

Kui meilile tehakse erakordne pakkumine

"Mõnel juhul kehtib ka lihtne talupojatarkus – kui miski tundub liiga hea, et tõsi olla, siis see enamasti ei vasta tõele," ütleb aga Kappak meilile saabunud ebatavaliselt ahvatlevate pakkumiste kohta.

Tema sõnul leidub õngitsuskirjades enamasti üsna lihtsalt tuvastatavaid vihjeid, mis pettusele viitavad. "Oleme ju kõik kohanud kirjakesi uskumatust pärandusest või juhuslikult süllekukkunud investeeringust, mida tahetakse laiali jagada. Enamasti annab juba üle võlli ja grammatiliselt ebakorrektne keelekasutus selge vihje, et tegemist on lihtlabase petukirjaga," räägib Kappak.

Surve kiirelt tegutsemiseks on ohumärk

"Viimasel ajal on saadetud sõnumeid telefonile, mis näevad välja nagu need oleks kullerfirma või mõne muu tuntud ettevõtte poolt, kus rõhutakse emotsioonile ja palutakse kiirelt lingile vajutada ja oma andmed sisestada, et pakk kätte saada," toob RITi IT-abi vanemspetsialist näite levinud petuskeemist ning selgitab lisaks, et läbi ajaloo on petuskeemid tuginenud ohvri psühholoogia ja käitumisharjumuste tundmisele.

"Mõtle enne, kui tegutsed. Ära allu kiireloomulistele nõudmistele, võta aega olukorra hindamiseks ja vajadusel konsulteeri usaldusväärse asjatundjaga," rõhutab ekspert vajadust alati kontrollida, kas õngitsuskirjas esitatud kiire nõue on üldse tõepärane.

Pahalane võib andmeid kasutada alles palju hiljem

Kappaku sõnul on inimeste levinud eksiarvamuseks veel see, et lingile vajutades või manust avades ei juhtunud midagi. “Manusesse saab peita kahtlaseid koodijuppe, mis hakkavad andmeid lugema,“ ütleb ta.

Pärast ettevaatamatut klõpsamist tuleks alati teha arvutile viirusetõrje ja kõik oma paroolid vahetada,” sõnub Kappak ja lisab, et seda on oluline teha nii tööga seotud kui ka isiklikel kontodel, sest õngitsejad panustavad paroolide ristkasutamise peale. Tööarvutite puhul tuleks kindlasti pöörduda ka oma IT-abi poole, et olukord parimal viisil lahendada. “Ei tasu tunda valehäbi ja võimalusel tasuks spetsialistide käest uurida taustainfot kirja kohta juba ennetavalt, enne klõpsamist,” lisab RITi IT-abi vanemspetsialist.

- Lahendused
- Turvalisus

Pilt

