OUCH! 2024.gada oktobris

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Lejupielādes briesmas: kā pārspēt ļaunprātīgas mobilās lietotnes

Noslēpumainā lietotne: Īss brīdinošs stāsts

Kādā laiskā svētdienā Sāra sociālajos tīklos uzdūrās jaunas fotoattēlu rediģēšanas lietotnes "PiksPerfect" reklāmai. Ieintriģēta par tās satriecošajiem filtriem, viņa bez vilcināšanās to lejupielādēja. Sākotnēji lietotne darbojās lieliski, taču drīz vien viņas tālruņa darbība kļuva lēna, un sāka parādīties dažādas reklāmas. Pēc dažām dienām Sāra saņēma zvanu no savas bankas par aizdomīgiem darījumiem, kuru kopējā summa bija tūkstošiem dolāru. Panikā viņa pārbaudīja savu bankas lietotni un atklāja, ka viņas uzkrājumi ir gandrīz pilnībā iztērēti. Pēc ziņošanas par krāpšanu un konta iesaldēšanas viņa burtiski sabruka – apjukusi un sarūgtināta.

Viņas tehniski zinošais draugs atklāja patiesību: mobilā lietotne bija viltojums, kas nozaga viņas personisko informāciju, tostarp bankas datus. Pagāja vairāki mēneši, līdz Sāra atguva zaudējumus, taču kļuva piesardzīgāka un pirms instalēšanas izpētīja mobilās lietotnes. Tagad viņa dalās savā stāstā, lai brīdinātu citus, saprotot, ka neuzmanības mirklis var radīt tālejošas sekas.

Kā zināt, kuras lietotnes ir drošas?

Mobilās lietotnes ir ērtas un jaudīgas, ļaujot mums ar vienu pogas pieskārienu izdarīt gandrīz visu, kas attiecas uz mūsu dzīvi. Tomēr kibernoziedznieki to izmanto, radot viltotas vai ļaunprātīgas mobilās lietotnes. Ja lejupielādējat kādu no šīm lietotnēm, tās var pārņemt jūsu tālruni un uzraudzīt visu, ko darāt. Lai sevi pasargātu, galvenais ir pārliecināties, ka jūsu ierīcēs instalētās mobilās lietotnes ir īstas un drošas.

Pirmkārt un galvenokārt, lejupielādējiet mobilās lietotnes tikai no oficiāliem veikaliem, kuros pārdevēji pārbauda mobilās lietotnes, piemēram, "Apple App Store" vai "Google Play Store". Tas palīdz samazināt risku lejupielādēt ļaunprātīgu mobilo lietotni. Trešo personu lietotņu veikaliem bieži vien nevar uzticēties, un tos var pat pārvaldīt kibernoziedznieki. Taču, pat izmantojot uzticamu mobilo lietotņu veikalu, ir jābūt uzmanīgiem. Piedāvājam dažus papildu pasākumus, ko varat veikt, lai pārliecinātos, ka lejupielādējat īstas un drošas mobilās lietotnes.

1. **Pārbaudiet izstrādātāja nosaukumu**: Kad meklējat konkrētu mobilās lietotnes programmu, ko izveidojis konkrēts uzņēmums, pārliecinies, ka lejupielādējamo lietotni ir izveidojis šis uzņēmums. Izplatīts krāpnieku triks ir radīt mobilās lietotnes, kas izskatās ļoti līdzīgas labi zināmām lietotnēm. Pārbaudiet izstrādātāja nosaukumu– vai tas ir tas pats uzņēmums vai labi zināms izstrādātājs, vai arī lietotni ir izstrādājis kāds, par kuru jūs nekad neesat dzirdējis? Vēl viena iespēja ir apmeklēt lietotnes vai izstrādātāja oficiālo tīmekļa vietni, lai atrastu tiešas saites uz mobilo lietotni lietotņu veikalā. Tas nodrošina, ka lejupielādējat oficiālo lietotni.

2. **Izlasiet atsauksmes un vērtējumus**: Aplūkojiet lietotāju atsauksmes un vērtējumus. Īstai lietotnei būs ievērojams skaits pozitīvu atsauksmju un augsti reitingi. Uzmanīgi izturieties pret lietotnēm, kurām ir maz atsauksmju, daudz negatīvu atsauksmju vai pārāk pozitīvas atsauksmes, kas izklausās viltotas.

3. **Izpētiet lejupielāžu skaitu**. Īstām lietotnēm parasti ir liels lejupielāžu skaits. Lietotne ar mazu lejupielāžu skaitu var būt kā sarkanais karogs.

4. **Pārbaudiet atļaujas**: Pirms lejupielādes pārskatiet lietotnes pieprasītās atļaujas. Īstas programmas pieprasīs tikai tās funkcionalitātei nepieciešamās atļaujas. Uzmanīgi izturieties pret lietotnēm, kas pieprasa pārāk daudz vai nebūtisku atļauju. Vai mobilā tālruņa lietotnei tiešām būtu jāzina jūsu atrašanās vieta un vajadzīga piekļuve jūsu kontaktiem?

5. **Pārbaudiet programmatūras atjaunināšana**: Īstas lietotnes tiek regulāri atjauninātas, lai novērstu kļūdas un uzlabotu veiktspēju. Pārbaudiet lietotnes atjauninājumu vēsturi, lai pārliecinātos, ka tā bieži tiek atjaunināta.

6. **Esiet piesardzīgi ar jaunām lietotnēm**: Pret jaunām lietotnēm, kurām nav atsauksmju vai vērtējumu, jāizturas ar piesardzību. Ja lietotne ir īsta, tā laika gaitā, visticamāk, iegūs pozitīvas atsauksmes un vērtējumus.

Pēc mobilās lietotnes lejupielādes iespējojiet automātisko atjaunināšanu. Mobilo lietotņu kodā un konfigurācijās pastāvīgi tiek atrastas jaunas kļūdas un ievainojamības. Vienmēr pārliecinoties, ka izmantojat jaunāko mobilo lietotņu versiju, varat būt droši, ka šīs ievainojamības ir novērstas un ka jums ir pieejamas jaunākās drošības funkcijas. Turklāt, ja vairs neizmantojat mobilo lietotni, dzēsiet to no tālruņa.

Viesredaktors

Daniela Strimbu (Danielle Strimbu) ir "Travel Minds Digital Agency" tehnisko projektu vadītāja, kurai ir pieredze tehnoloģiju un darbības vadībā. Kā "WiCyS" Kolorādo filiāles pasākumu priekšsēdētāja viņa cenšas organizēt saistošus pasākumus, lai palīdzētu veicināt sieviešu attīstību kiberdrošības jomā. Viņai ir maģistra grāds informācijas sistēmu drošībā un diploma sertifikāts kiberdrošības vadībā.

Resursi

Trīs izplatītākie veidi, kā kiberuzbrucēji vēršas pret jums: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Informācija, kas jums jāzina par papildus datiem: https://www.avast.com/c-what-is-background-data#

Tulkojums: CERT.LV