OUCH! 2024 - 01

Ikmēneša informācijas drošības izdevums tev

QR kodi jeb kvadrātkodi

Pārskats

Vai esat kādreiz aizdomājušies, kas ir tie punktu kvadrāti vai svītras, ko sauc par "kvadrātkodiem"? Jūs, visticamāk, esat tos redzējuši izvietotus tīmekļvietnēs, uzdrukātus uz plakātiem, izmantotus kā mobilās biļetes vai uz restorānu galdiem. Kā tie darbojas, un vai ir kādi riski, par kuriem vajadzētu uztraukties? Skatāmies.

Kvadrātkods, kas norāda uz "SANS OUCH" tīmekļvietni.

Kā darbojas kvadrātkodi?

Kvadrātkods nozīmē "ātrās atbildes kods", un tas ir mašīnlasāms kods, kas parasti sastāv no melnu un baltu kvadrātu matricas (tie var būt arī citās krāsās un saturēt fona attēlus). Šos kvadrātus var viegli izveidot, izmantojot kvadrātkodu ģeneratorus, un tos izmanto, lai kodētu informāciju, piemēram, tīmekļvietnes URL, e-pasta kontaktinformāciju vai cita veida datus. Domājiet par kvadrātkodiem kā par svītrkodiem, bet daudzpusīgākiem. Lielākā daļa mobilo ierīču kameru atpazīst un atšifrē kvadrātkodā kodēto informāciju. Citiem vārdiem sakot, kad mēģināsiet nofotografēt kvadrātkodu ar ierīces kameru, tā atšifrēs kvadrātkodu un jautās, vai vēlaties rīkoties ar tajā ietverto informāciju, piemēram, atvērt saiti uz tīmekļvietni.

Kādi draudi pastāv?

Kvadrātkodus cilvēki var nespēt viegli interpretēt, tāpēc kiberuzbrucējiem ir vieglāk iekodēt informāciju, kas varētu būt ļaunprātīga vai nodarīt kaitējumu. Piemēram, kvadrātkods var nosūtīt jūs uz ļaunprātīgu tīmekļvietni, kas mēģina iegūt jūsu personisko informāciju, piemēram, paroles vai kredītkaršu numurus, vai, iespējams, pat mēģina instalēt jūsu ierīcē ļaunprātīgu programmatūru. Turklāt kvadrātkodi var veikt papildu darbības, piemēram, pievienot kontaktpersonu jūsu kontaktu sarakstam vai izveidot e-pasta vēstuli jūsu vārdā. Kvadrātkods pats par sevi nav drauds, taču apdraudējums var būt informācija vai darbība, ko tas izraisa.

Piemēram, jūs atrodaties pilsētā vai lidostā, un pie sienas ir plakāts, kas reklamē jūs interesējošu produktu. Uz plakāta ir kvadrātkods, ko varat izmantot, lai ātri iegūtu plašāku informāciju. Jūs neapjaušat, ka kāds ir pārklājis plakāta kvadrātkodu ar cita kvadrātkoda uzlīmi. Aplūkojot plakātu, jūs tam uzticaties, nenojaušot, ka kvadrātkods uz plakāta ir aizstāts ar noziedzīgu kodu. Kad skenējat kvadrātkodu, lai uzzinātu vairāk par produktu, jūs tiekat novirzīts uz noziedznieka kontrolētu tīmekļvietni, kurā tiek sākts uzbrukums.

Ko darīt, lai būtu drošs?

- Esiet uzmanīgi, pirms uzticaties kvadrātkodam un skenējat to. Vispirms pajautājiet sev: Vai varat uzticēties avotam? Vai uzticaties plakātam, restorānam vai tīmekļvietnei, kurā parādīts kvadrātkods? Ja kāds uz jūsu automašīnas būtu atstājis izdales materiālu ar kvadrātkodu, vai varat tam ticēt?
- Pēc kvadrātkoda skenēšanas ierīce pirms jebkādu darbību veikšanas jautās, vai vēlaties rīkoties ar nolasīto informāciju. Piemēram, ja kvadrātkods ir saite uz tīmekļvietni, jūsu ierīce pirms došanās uz šo vietni jums jautās, vai vēlaties to apmeklēt. Atvēliet laiku, lai pārskatītu aicinājumu veikt darbību vai pašu saiti un pārliecinātos, ka jums ir droši to apmeklēt.
- Pārliecinieties, ka jūsu mobilās ierīces vienmēr ir atjauninātas un tajās darbojas jaunākā operētājsistēmas versija. Tas nodrošina, ka tajā ir jaunākās drošības funkcijas. Visvienkāršākais veids, kā to izdarīt, ir aktivizēt ierīces automātiskos atjauninājumus.
- Lai atšifrētu kvadrātkodus, nav nepieciešams instalēt īpašas mobilās lietotnes, jums vajadzētu būt iespējai vienkārši izmantot ierīcē iebūvēto kameru. Ja tīmekļvietnē ir nepieciešams lejupielādēt specializētu kvadrātkodu skenēšanas lietotni, visticamāk, tā ir viltota vai neīsta.
- Padomājiet divreiz, pirms sniedzat konfidenciālu vai personisku informāciju jebkurai tīmekļvietnei, kurā esat nokļuvis, izmantojot publiski redzamu kvadrātkodu.

Kvadrātkodi ir ērts veids, kā piekļūt dažāda veida jaunai informācijai un iespējām. Veicot dažus vienkāršus pasākumus, varat tos izmantot maksimāli droši.

Viesredaktors

Abdulmadžīds AlAbdulhadi (Abdulmajeed AlAbdulhadi) ir Saūda Arābijas Aramko IT/OT sistēmu konsultants ar vairāk nekā 27 gadu darba pieredzi. Viņš ir sertificēts informācijas sistēmu auditors (CISA) un sertificēts informācijas drošības vadītājs (CISM), un ASV patentu birojs viņam ir piešķīris kiberdrošības patentu (10,693,906).

Resursi

Teksta paziņojumu / smikšķerēšanas uzbrukumi: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Vikšķerēšana — tālruņa zvanu uzbrukumi un krāpniecība: https://www.sans.org/newsletters/ouch/vishing
Mobilo ierīču pasargāšana: https://www.sans.org/newsletters/ouch/securing-mobile-devices/

Tulkojums: CERT.LV