MINUTKA

ZA VARNOST IN ZASEBNOST

1/2022

Zlata pravila:

1.

Uporabljajte močna gesla in jih redno spreminjajte.

2.

Ne klikajte na nenavadne povezave ali pojavna okna.

3.

Bodite previdni pri odpiranju e-pošte, če ne poznate pošiljatelja.

4.

Bodite pozorni na svoje objave na družbenih omrežjih.

5.

Če je mogoče službenih naprav ne uporabljajte za osebne namene.

Top 3 grožnje

september 2022

1. Izsiljevalski virus

2. Phishing

3. Zloraba osebnih podatkov

Kaj je novega?

Google je v začetku meseca oktobra izdal posodobljene različice mobilnega operacijskega sistema Android, ki vsebujejo ključne varnostne popravke. Med drugim posodobitev krpa ključno varnostno luknjo, ki bi napadalcem lahko omogočila popoln nadzor nad vašim mobilnim telefonom.

Nasvet: *Poskrbite, da so vse vaše naprave posodobljene na zadnjo dostopno različico!*

Hrvaški »Informacijski pooblaščenec« je centru za socialno varstvo prepovedal objavo seznama delavcev, v katerem je za vsakega od njih naveden preostali letni dopust, na oglasni deski centra.

Nasvet: *Preden se odločite za objavo osebnih podatkov na oglasni deski (še posebej, če je ta javno dostopna), preverite če to smete storiti in katere podatke smete objaviti.*

Vozite Toyoto, mlajšo od 5 let? Iz avtomobilskega velikana Toyote, so sporočili, da je iz njihove aplikacije T-Connect odteklo več kategorij podatkov skoraj 300.000 uporabnikov. Večinoma gre za e-poštne naslove in interne številke uporabniških računov.

Nasvet: *Bodite pozorni na to v katerih izpostavljenih bazah podatkov se nahajajo vaši osebni podatki. Kombinacija vašega e-poštnega naslova in informacije o znamki vašega avtomobila, lahko spletnim napadalcem ponudi osnovo za pripravo spletne prevare.*

Tema tedna: *Kako prepoznati lažne e-poštne naslove*

E-pošta je ena izmed najpogostejših vstopnih točk spletnih kriminalcev za izvedbo kibernetskega napada. Poleg neposrednih vdorov v e-poštni predal, so posamezniki največkrat tarča zlonamernih e-poštnih sporočil.

Zlonamerna e-poštna sporočila imajo najpogosteje dva tipa škodljivih elementov - povezavo na zunanjo spletno stran ali priponko, ki se predstavlja kot običajen dokument, vsebuje pa škodljivo programsko kodo.

Kako prepoznamo zlonamerno e-poštno sporočilo? Namigov je več. Včasih so jasni kot beli dan, včasih pa skoraj povsem nevidni. Prvi namigi se navadno skrivajo v e-poštnem naslovu, najpogosteje v domeni.
Domena je drugi del e-poštnega naslova, nahaja se za @. Domena v e-poštnem naslovu janez@microsoft.com je microsoft.com.

1. Neznana domena: Ko prejmemo sumljivo e-poštno sporočilo, velja najprej preveriti domeno. Pozorni moramo biti predvsem na: neznana imena domen, generične e-poštne domene (*gmail*, *yahoo*, *hotmail*, *outlook*, ...), ter domene sestavljene iz zaporedja naključnih znakov.

2. Ena najpogostejših taktik napadalcev je sprememba v črkovanju domene. Poglejmo primer: janez@micsoroft.com. Janez seveda ne dela za Microsoft, nepozorne posameznike pa zna hitro prepričati, da “obnovijo” naročnino na njihove izdelke.

3. Napadalci uporabljajo prilagojeno verzijo resnične domene. Gre za tehniko, ki jo je najtežje prepoznati, saj predvsem pri večjih podjetjih ne poznamo različnih variacij e-poštnih naslovov.

janez@microsoft-support.com je lahko resničen naslov, janez@microsoft-support.net pa lažen. V tem primeru je najbolje, da e-poštni naslov vnesete v spletni iskalnik in preverite pravilno obliko domene.

Ne pozabite:

1. znana domena

2. pravilno črkovanje

3. pravilna oblika domene

13.10.2022

SGB varnostno svetovanje InfoHiša