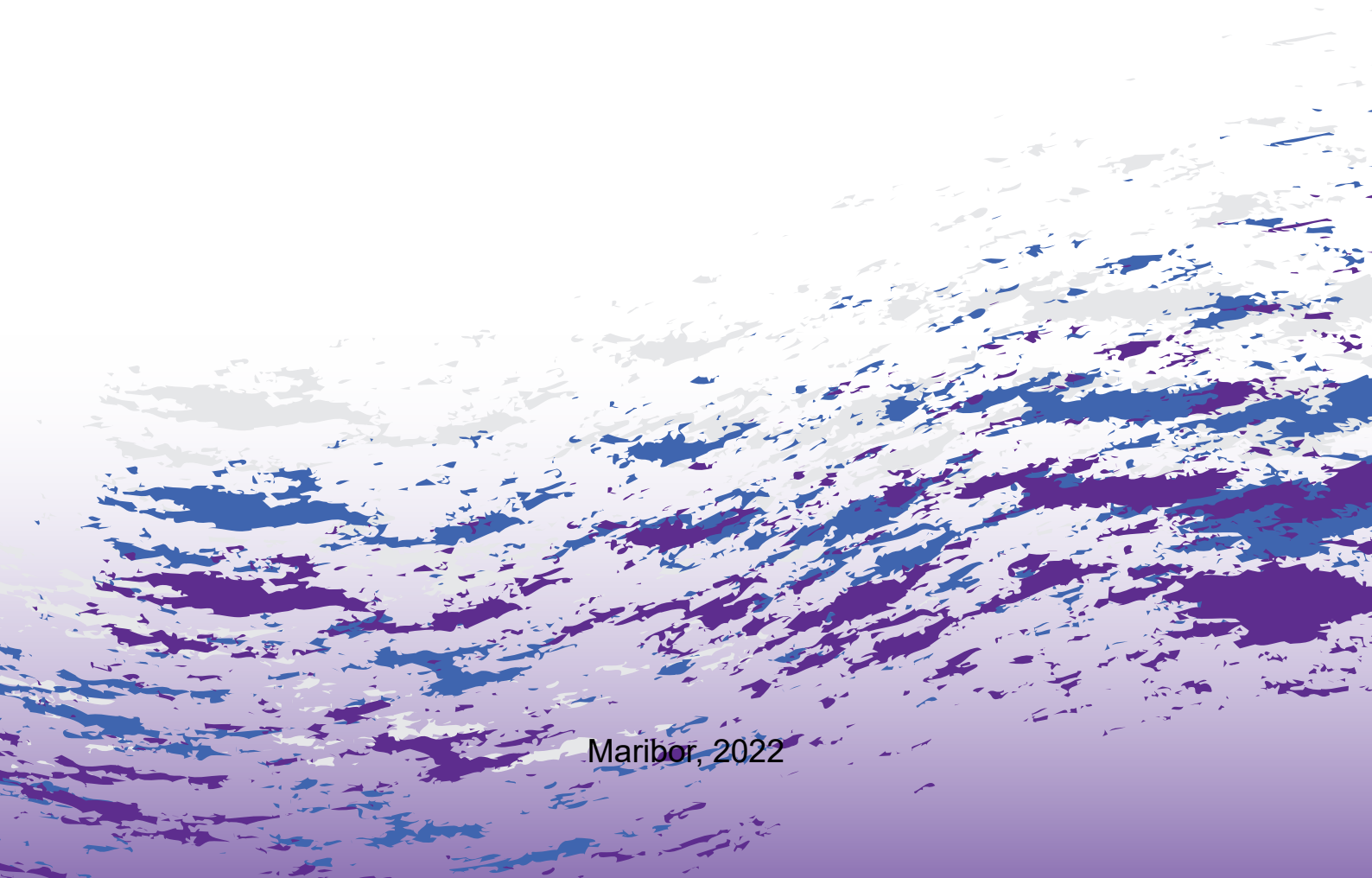
PAM Pokrajinski arhiv Maribor

Moderna arhivistika

Časopis arhivske teorije in prakse
Journal of Archival Theory and Practice

Letnik 5 (2022), št. 1 / Year 5 (2022), No. 1



Maribor, 2022

Prejeto / Received: 28. 06. 2022

1.04 Strokovni članek *1.04 Professional article*

https://doi.org/10.54356/MA/2022/CEZB3255

VARNOST KOMUNIKACIJ IN APLIKACIJ

Boštjan ŠPEHONJA
specialist informacijske varnosti, direktor v podjetju Go-lix d.o.o., Šempeter pri Gorici, Slovenija
bostjan.spehonja@golix.si

Sanja GERDAK
vodja sektorja priprave dela, Mariborski vodovod, d.o.o., Maribor, Slovenija
sanja.gerdak@mb-vodovod.si

Izvleček:

Varnost komunikacij in aplikacij je v sodobni digitalni družbi vse pomembnejša, tako na poslovnem kot zasebnem področju. Glede na trenutne nepredvidljive razmere, na območju Evropske unije in v svetu, pa se stopnja tveganja za kibernetski napad vsak dan povečuje. V prispevku bo predstavljena varnost elektronskih komunikacij in tistih aplikacij, ki jih poslovni svet najpogosteje uporablja. To so elektronska pošta, protokoli za oddaljen dostop pri delu od doma in ostali komunikacijski protokoli. Dotaknili pa se bomo tudi aplikacij z zasebnega področja, kot so Whatsup, Viber, Messenger, Zoom ter podobne. Vsem komunikacijskim kanalom je skupno, da uporabljajo šifrirane protokole, vendar tudi slednji niso vsi enako varni. Predstavili bomo, kako varno uporabljati aplikacije, kako varno komunicirati ter kakšne preventivne ukrepe mora poznati vsak uporabnik katerekoli elektronske naprave, da zmanjša možnost vdora ali okužbe z zlonamerno programsko opremo.

Ključne besede:

varnost, komunikacije, aplikacije, kibernetski napad, šifrirani protokoli

Abstract:

Security of Communications and Applications

Security of communications and applications in the modern digital society, both in business and private field, is increasingly important. Given the current unpredictable situation in the area of the European Union and in the world, the level of risk of a cyber-attack is increasing every day. In the paper, the security of electronic communications and those applications that are most often used in the business world - e-mail, protocols for remote access when working from home and other communication protocols - will be presented.

The authors will also discuss applications from the private sector, such as WhatsApp, Viber, Messenger, Zoom and similar. All communication channels use encrypted protocols, but also the latter are not all equally safe. They will present how to use applications safely, how to communicate safely and what preventive measures every user of any electronic device should know in order to reduce the possibility of a cyber-attack such as hacking or malware infection.

Key words:

security, communications, applications, cyber attack, encrypted protocols

1. Komunikacija in aplikacije

»*Komuniciranje je sporazumevanje, občevanje, sistem izmenjevanja simbolov ali informacij med informacijskim virom in sprejemnikom. Strokovni izraz 'komuniciranje' se uporablja tako v družboslovju kot humanistiki in tehničnih znanosti, na primer v računalništvu, elektrotehniki ipd. Beseda komuniciranje izhaja iz latinske besede communicare, kar pomeni posvetovati se, razpravljati o nečem, vprašati za nasvet. Komuniciranje je prenos sprejetih simbolov med ljudmi. Ko komunicirajo, ljudje med seboj prenašajo sporočila s pomočjo različnih simbolov (besed, kretenj, govorice telesa, slik …)*« (Wikipedija, 2022).

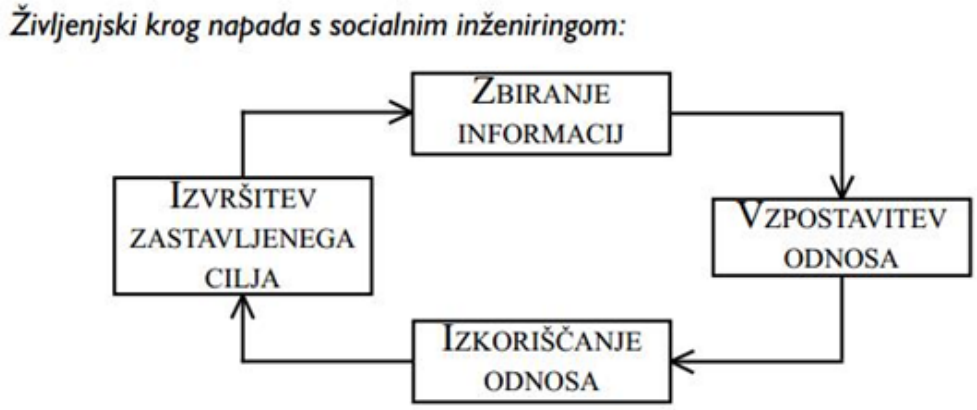
Spletna aplikacija je za uporabnika vsaka aplikacija, ki za dostop potrebuje uporabo spletnega brskalnika – klasične spletne strani, spletni dostop do elektronske pošte, spletni dostop do spletne banke, spletni vmesnik za SharePoint itd. Za skrbnika oz. razvijalca pa aplikacija predstavlja skupek datotek oz. skript (php, java, css itd.), ki se nahajajo na določeni direktorijski strukturi in se definirajo kot »spletna stran« za posamezno spletno aplikacijo (Smart Com, 2019).

Vedno bolj pogosto uporabljamo pametne naprave (mobiteli, tablični računalniki, itd.) za najrazličnejše zadeve in seveda razne aplikacije za prebiranje elektronske pošte, družbeno mreženje, branje novic na portalih, za klepet, brezplačno pošiljanje sporočil, igrice itd. Nekatere aplikacije so prednaložene že ob nakupu posamezne naprave, ostale pa si uporabniki lahko brezplačno ali plačljivo naložimo v aplikacijskih trgovinah, kot so npr. Google Play, App Store ipd., ali pa si jih naložimo z določenega spletnega mesta.

Računalniške komunikacije so se s hitrim razvojem internetnih povezav zelo spremenile. Orodja za komunikacijo so se v preteklosti razvijala predvsem za namizne računalnike, z množično uporabo brezžičnega interneta pa se je večina razvoja preusmerila na mobilne naprave. Tako poznamo dandanes istoimenske aplikacije tako za namizne računalnike kot tudi za mobilne naprave, kar omogoča vzpostavitev učinkovitih povezljivih okolij s številnimi funkcionalnostmi (npr. prenos datotek, oddaljeni nadzor, prenos slik itd.). K temu so veliko pripomogli računalniški oblaki, ki jih uporabljajo aplikacije, kot so DropBox, GoogleDrive, GoogleFoto itd. Najpogosteje uporabljena komunikacija je elektronska pošta, v poslovnem svetu, kjer obstaja velika nevarnost zlonamernih vdorov predvsem v obliki socialnega inženiringa, pa programska oprema Office 365. Najpogosteje se v poslovnem svetu pojavi zlonamerni vdor v obliki posredovane elektronske pošte z lažno in škodljivo povezavo ali škodljivo priponko.

Socialni inženiring je ena najbolj podcenjenih, hkrati pa najnevarnejših metod zlorabe človeškega zaupanja. To pomeni, da je človek pri kibernetskih napadih med najšibkejšimi členi varnostnega sistema. Napadalec, ki uporablja metode socialnega inženiringa, se poslužuje majhnih laži, prevar in zvijač. Napadenega izkorišča z različnimi čustvenimi in psihičnimi stanji. Velikokrat tudi izkorišča nezadovoljstvo v službi oz. »prijateljstvo na delovnem mestu« ali vlogo »prijazne« stranke oziroma poslovnega partnerja. Socialni inženir uporabi vse metode »idealne«, prijazne in zaupanja vredne osebe, ki jo žrtev napada z veseljem spusti v svojo bližino (Potokar in Androić, 2015).

Socialni inženiring je tehnika napada, s katero se manipulira človeka z namenom pridobivanja osebnih ali poslovnih informacij ali podatkov. Napad s socialnim inženiringom lahko opišemo s naslednjimi štirimi stopnjami, ki so razvidne na sliki 1: zbiranje informacij, vzpostavitev odnosa, izkoriščanje odnosa in izvršitev zastavljenega cilja. Pri vseh korakih je ključen človeški vir, saj se večina napadov na informacijske sisteme s pomočjo socialnega inženiringa zgodi ravno zaradi človeških napak (Androić in Špehonja, 2015).



Slika 1: Življenjski krog napada s socialnim inženiringom (Informacijski pooblaščenec, 2009)

Napad preko elektronske pošte se lahko, kot smo že omenili, izvede s pomočjo lažnih povezav, sporočili z zahtevami za vpis podatkov, okuženih priponk itd. Zaskrbljujoča za neukega uporabnika je možnost pošiljanja elektronske pošte v primeru, ko SMTP-strežniki niso pravilno konfigurirani. Tako lahko npr. pošlje napadalec kot direktor podjetja elektronsko sporočilo za izplačilo računovodji tega podjetja, ki izplačilo izvede, saj ne podvomi v pristnost sporočila ali pošiljatelja, ki je njemu viden kot njegov direktor (Androić in Špehonja, 2015).

Uporabniki v poslovnem in zasebnem življenju radi hitro posežemo po različnih aplikacijah in jih z veseljem pričnemo uporabljati, ob premajhnem zavedanju, kakšne dostope in do katerih podatkov dovolimo pri tem posameznim aplikacijam. Le-te nam na pričetku uporabe resda prihranijo čas, a sčasoma pričnemo zapravljati vedno več časa zanje. Glede na hiter tehnološki razvoj in življenjski tempo uporabniki enostavno ne bomo več mogli pravočasno slediti vsem spremembam in nevarnostim, kar pa bo vedno večja nevarnost, ki jo bodo s pridom izkoristili zlonamerni napadalci.

Hitro se nam lahko tudi zgodi, da z namestitvijo nepreverjene aplikacije okužimo napravo. Priklop takšne naprave v katero koli omrežje pomeni tveganje tudi za ostale naprave, saj obstaja zlonamerna koda, ki se je sposobna sama širiti v omrežju. Ko nameščamo aplikacije, moramo imeti v mislih, da aplikacije za svoje delovanje želijo imeti več dovoljenj in podatkov, kot jih dejansko potrebujejo. Največkrat gre za vse informacije, kar vključuje fotografije, telefonske številke, dostop do datotek, dovoljenje za snemanje zvoka brez dodatnega obvestila, aktiviranje morebitne plačljive storitve in druga dovoljenja.

V času epidemije koronavirusa je uporaba različnih aplikacij za komuniciranje zelo porastla, saj so bili zaposleni na delu od doma, šolarji na izobraževanju na daljavo, ljudje so bili tudi v karantenah in izolacijah. Glede na stroge državne ukrepe, kot so gibanje samo v okviru občine stalnega bivališča, zaprtje posameznih dejavnosti in podobno, smo ljudje prešli na različne komunikacijske kanale, da smo se lahko medsebojno sporazumevali. Na primer, šolarji so uporabljali aplikacijo Zoom, večina podjetij aplikaciji Microsoft Teams in Office 365, posamezniki pa aplikacije, kot so Viber, WhatsUp, Signal itd.

Varna aplikacija za klepet bi morala imeti naslednje funkcije:

- šifriranje sporočil na vseh stopnjah komunikacije,
- šifriranje od konca do konca, tako da zaposleni v podjetju, ki upravlja storitev sporočanja, ne morejo brati komunikacij,
- sposobnost preverjanja, s kom komunicirate,
- varnost zgodovine komunikacije v primeru kraje ključev za šifriranje,
- kodo aplikacije lahko ocenjujejo zunanji in neodvisni inšpektorji,
- zasnova in izvedba kriptografije je dokumentirana,
- koda je bila preverjena v zadnjem letu.

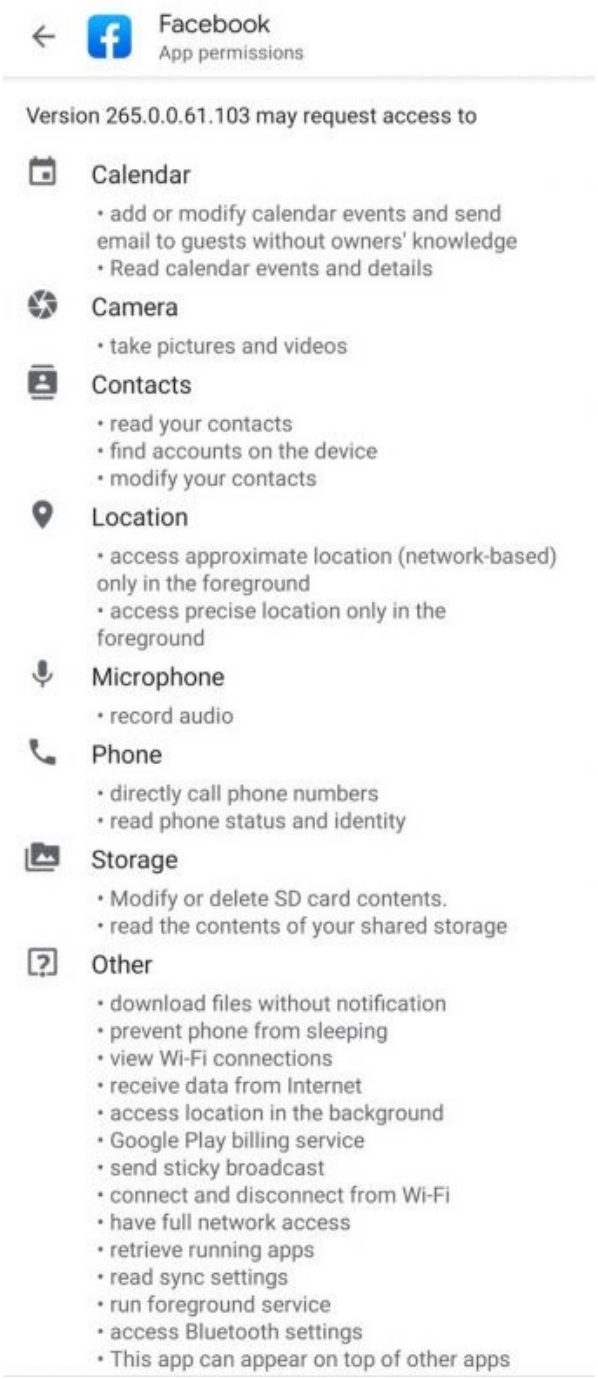
Aplikacija za komuniciranje Signal izpolnjuje vse pogoje za varno sporočanje in je vzgled dobre prakse, saj je preprosta za uporabo. Lahko se uporablja kot privzet odjemalec za sporočila sms, ki seveda niso šifrirana. Lahko se uporablja tudi za šifrirano komuniciranje. Prav tako za besedilna, slikovna, glasovna in video sporočila ter tudi telefonske klice. Dostop do aplikacije lahko zaklenemo tudi z geslom (passphrase). Vmesnik je preprost, varno lahko komuniciramo le s stiki, ki imajo tudi nameščen Signal. Omogoča skupinska sporočila in sporočila, ki po preteku nastavljenega časa nepovratno izginejo.

Pri uporabi Microsoft Teams ne smemo omenjati nekoga, ki ni del ekipe, spreminjati ekipe iz zasebne v javno, preimenovati kanalov in pošiljati v več kanalov. Previdni moramo biti pri deljenju datotek v klepetu in dodajanju novih oseb v klepet. Uporabniki pogosto delijo datoteke in potem zapustijo klepet. Uporabniki tudi delijo datoteke v klepet in jih potem izbrišejo. Uporabnikom se pojavijo težave, ki jih ne znajo sami rešiti.

2. Primeri nevarnosti

2.1 Dovoljenja in pravice

Pri uporabi mobilnih aplikacij velikokrat povsem pozabimo na zasebnost in osebne podatke. Hitimo z nameščanjem raznovrstnih aplikacij samo zato, ker »jih imajo vsi«, in želimo biti v nenehnem virtualnem stiku z okolico. Ko namestimo aplikacijo za komuniciranje, se moramo strinjati z vsemi pogoji in aplikaciji velikokrat podati vsa dovoljenja, saj v nasprotnem primeru ne deluje. Ker je uporabniški cilj priti čim prej do uporabe aplikacije, največkrat potrdimo vsa dovoljenja in že naslednji trenutek pozabimo, da smo vse svoje shranjene podatke delili s proizvajalcem programske opreme. Na sliki 2 podajamo primer dovoljenj, ki jih za svoje delovanje potrebuje Facebook aplikacija.



Slika 2: Primer dovoljenj, ki jih za svoje delovanje potrebuje Facebook aplikacija (Crambler, 2020)

2.2 Zlonamerne aplikacije

Pri nameščanju aplikacij moramo biti izjemno pozorni, da jih namestimo iz uradnega vira. Nameščanje in prenos aplikacij s poljubnih spletnih strani, forumov, portalov za izmenjavo datotek ipd. je lahko izredno nevarno. Napadalci izdelajo aplikacijo, ki je zlonamerna programska oprema in v veliko primerih ne bi prestala filtrov App stora ali Google Playa. Zato tovrstne aplikacije odlagajo na razne spletne strani, forume in mesta za deljenje datotek ter tako čakajo, da se uporabnik ujame v past in namesti aplikacijo na svoj telefon. Pri tem največkrat poda aplikaciji vsa dovoljenja, kar pomeni, da ima zlonamerni razvijalec mobilne aplikacije načeloma dostop do vseh podatkov na mobilni napravi. Aplikacije, ki se pojavijo na App storu ter Goole Playu, so vsaj delno preverjene, čeprav se je velikokrat izkazalo, da lahko tudi tovrstne aplikacije kradejo podatke iz naprave in se obnašajo kot zlonamerna programska oprema.

Poleg tega pa moramo biti izredno previdni, da v Google Play-u ali App Storu izberemo pravo aplikacijo za namestitev. Ko iščemo določeno aplikacijo, se nam velikokrat pojavijo različice aplikacije, ki imajo podobno ime in zelo podobno grafično ikono. Pri tem pa ne gre za iskano aplikacijo, ampak za lažne aplikacije drugega proizvajalca. Velikokrat si lahko pri izbiri prave aplikacije pomagamo s številom namestitev, ki je prikazana pri vsaki aplikaciji posebej. Originalna aplikacija ima praviloma najvišje število prenosov ter namestitev. Če namestimo lažno aplikacijo in to ugotovimo ob prvem zagonu, jo nemudoma izbrišimo ter ponovimo iskanje.

2.3 Neželena vsebina

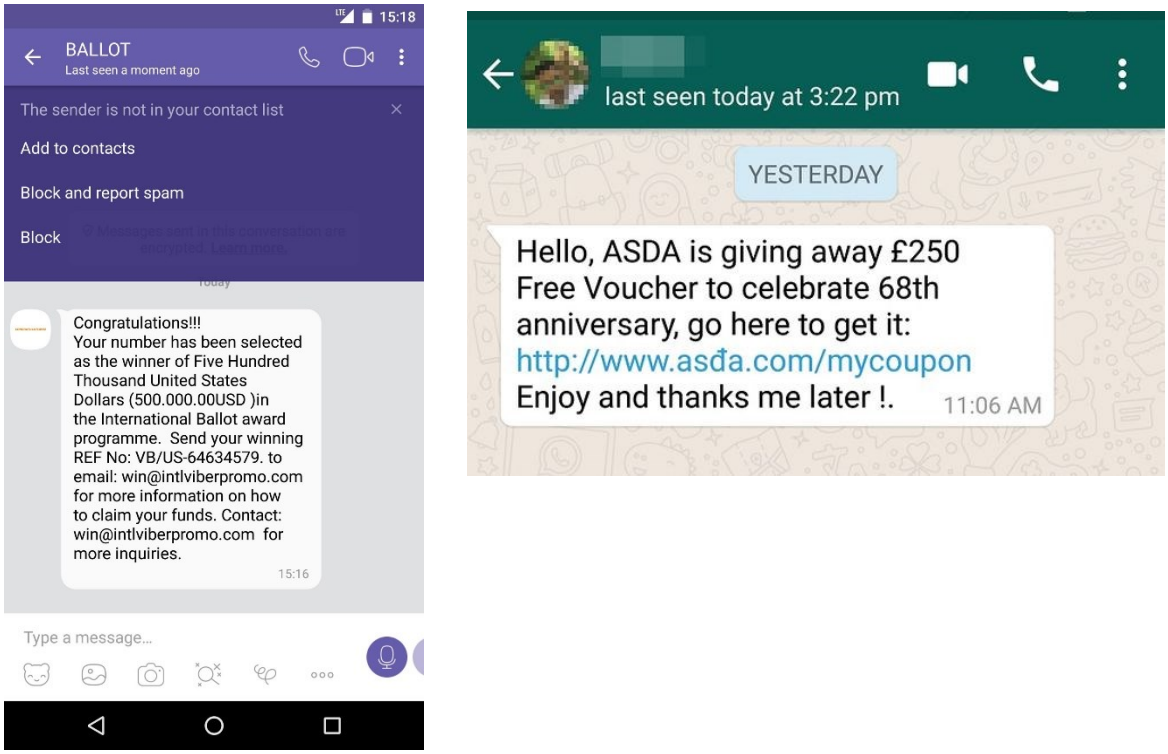
Veliko mobilnih aplikacij za komuniciranje zahteva ob registraciji uporabnikovo telefonsko številko. To pa omogoča vsakomur, ki ima našo telefonsko številko, da preko aplikacije komunicira z nami.

Kot že omenjeno, uporabniki na spletu velikokrat pozabijo na svojo zasebnost ter osebne podatke. Posledično vpisujejo vse osebne podatke, vključno z elektronskim naslovom in telefonsko številko, na najrazličnejša spletna mesta. Če pride na spletnem mestu do vdora in odtujitve podatkov, pridobijo napadalci bazo vseh osebnih podatkov, ki jih uporabniki vpišejo. To je le en izmed primerov, kako lahko naša telefonska številka pride v roke napadalcev. Po tem se začnejo napadi s tehnikami socialnega inženiringa po vseh možnih kanalih ter aplikacijah – po elektronski pošti, sporočilih sms, preko Google koledarja ali najrazličnejših aplikacij za komuniciranje, kot so Signal, Viber, WhatsUp in druge. Napadalci nam največkrat pošiljajo naslednje tipe prevar:

- Nigerijska prevara – gre za sporočilo, kjer zatrjujejo, da ste zadeli veliko količino denarja ali želijo na vaš bančni račun nakazati večjo vsoto denarja. Pred tem pa od vas zahtevajo plačilo najrazličnejših stroškov.
- Zlonamerna povezava – gre za sporočilo, ki vsebuje povezavo na spletno mesto. Povezave lahko vodijo na najrazličnejša mesta, od direktnega prenosa zlonamerne programske opreme, spletnih strani, namenjenim kraji podatkov (phishing), do zlonamernih strani, kjer zatrjujejo, da ste zadeli nagrado in od vas želijo pridobiti številko bančne kartice.

V primeru prejema neželenega sporočila na katerikoli kanal nanj ne odgovarjamo in ne klikamo na povezave. Sporočilo izbrišemo in se z njim ne ukvarjamo. V primeru klika na povezavo pa se moramo prepričati, da se ni zgodil avtomatski prenos kakršne koli datoteke na našo elektronsko napravo. Takšno datoteko izbrišemo in je ne odpiramo. Če pa nas povezava odpelje na spletno stran, na kateri od nas zahtevajo kakršne koli podatke, brskalnik zapremo in podatkov ne vpisujemo.

Primer takšnih sporočil so prikazane na spodnji sliki 3.



Slika 3: Primer nezaželenih sporočil (Crambler, 2020)

2.4 Ranljive aplikacije

Redno posodabljanje aplikacij, operacijskega sistema in nameščanje varnostnih popravkov mora postati higienski minimum, če želimo biti na spletu nekoliko varnejši. Popravki nas ne ščitijo pred napadi iz sklopa socialnega inženiringa, lahko pa nas ubranijo nekaterih tehničnih napadov na elektronsko napravo. Ranljivosti se v programski opremi ter v IT-svetu odkrivajo vsakodnevno, proizvajalci programske opreme pa te ranljivosti krpajo s popravki.

Nameščanje popravkov velja za vse aplikacije, ki jih imamo nameščene, ne glede na to, ali jih uporabljamo ali ne. Če aplikacij ne posodabljamo, na njih pa odkrijejo varnostne ranljivosti, postane naša naprava ranljiva in le vprašanje časa je, kdaj bodo to odkrili zlonamerni napadalci. Obseg škode in vrsta napada je odvisna od vsake ranljivosti posebej. Zato velja že omenjeno priporočilo, da poleg nameščanja popravkov redno odstranjujemo aplikacije, ki jih ne uporabljamo več. Poleg tega priporočamo, da se na vsako elektronsko napravo namesti protivirusna programska oprema znanega proizvajalca, pri čemer svetujemo plačljive različice.

2.5 Zasebnost

Pri uporabi aplikacij ne smemo pozabiti na našo zasebnost in na to, katere informacije delimo s svetom. Zato priporočamo, da po namestitvi vsake aplikacije preverite tako varnostne nastavitve kot nastavitve zasebnosti. Nastavite, kdo vse lahko vidi vaše osebne podatke, vključno s telefonsko številko, kdo vam lahko piše in vas kliče, kdo vas lahko splošno išče v iskalniku aplikacije, po kolikšnem času naj se sporočila izbrišejo, ali aplikacija izdeluje avtomatske varnostne kopije pogovorov itd.

Predvsem pa velja zlato priporočilo, ki smo ga že zdavnaj pozabili – po komunikacijskih kanalih naj bi se pogovarjali le tiste stvari, ki bi lahko postale v vsakem trenutku javne in ne bi imele nikakršnega vpliva in posledic. Ker to v današnjem času skoraj ni mogoče, pa poskrbimo za svojo zasebnost v čim večji meri.

3. Varnostna priporočila

Na podlagi raziskovanja in izkušenj iz prakse podajamo naslednja priporočila za končnega uporabnika za varno uporabo komunikacij in aplikacij:

- Na pametne naprave in računalnike namestite protivirusni sistem.
- Izberite močna gesla ter vklop dvofaktorske avtentikacije.
- Nalagajte le aplikacije iz uradnih spletnih trgovin.
- Pred nastavitvijo aplikacije preverite, kakšni so pogoji uporabe ter kakšna dovoljenja aplikacija potrebuje.
- Redno odstranjujte aplikacije, ki jih ne potrebujete več.
- Nameščajte posodobitve operacijskega sistema in aplikacij.
- Oddajanje svoje geolokacije imejte vklopljeno zgolj, ko je to potrebno.
- Redno varnostno kopirajte podatke.
- Šifriranje datotek oz. priponk elektronskega sporočila za zaščito vsebine ter pošiljanje gesla prejemniku po drugem kanalu npr. sms na mobilni telefon.
- Zaščita verodostojnosti pošiljatelja z digitalnim podpisom.

4. Viri in literatura

Androić, S., Špehonja, B. (2015). Posledice premalo skrbnega ravnanja z elektronskim in papirnim gradivom. V N. Gostenčnik (Ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 14. Zbornik mednarodne konference v Radencih 15.–17. april 2015* (str. 35–51). Maribor: Pokrajinski arhiv.

Clambler (2020). *The Scary Truth About the Facebook Messenger App and Your Privacy.* Pridobljeno 20. 4. 2022 s spletne strani: https://crambler.com/truth-about-facebook-messenger-app-privacy/.

Informacijski pooblaščenec (2009). *Socialni inženiring in kako se pred njim ubraniti?* Pridobljeno 19. 4. 2022 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.

Potokar, M., Androić, S. (2015). Socialni inženiring – človek kot del varnostnega sistema. V N. Gostenčnik (Ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 14. Zbornik mednarodne konference v Radencih 15.–17. april 2015* (str. 53–65). Maribor: Pokrajinski arhiv.

Smart Com (2019). *10 zapovedi za varne spletne aplikacije.* Pridobljeno 20. 4. 2022 s spletne strani: https://www.smart-com.si/varnost-spletnih-aplikacij-bela-knjiga/.

Wikipedija. Pridobljeno 19. 4. 2022 s spletne strani: https://sl.wikipedia.org/wiki/Komuniciranje.

SUMMARY

SECURITY OF COMMUNICATIONS AND APPLICATIONS

Boštjan ŠPEHONJA
Information Security Specialis, director, Go-lix d.o.o. Šempeter pri Gorici, Slovenia
bostjan.spehonja@golix.si

Sanja GERDAK
Head of Work Management Sector, Maribor Water Supply Company, Maribor, Slovenia
sanja.gerdak@mb-vodovod.si

The security of communications and applications is increasingly important in the modern digital society, both in the business and private spheres. Given the current unpredictable situation in the European Union and in the world, the level of risk of a cyber-attack is increasing every day. The article presents the security of electronic communications and those applications that are most often used in the business world. These are e-mail, protocols for remote access when working from home, and other communication protocols. The authors also discuss applications from the private sector, such as WhatsApp, Viber, Messenger, Zoom and similar. All communication channels have in common that they use encrypted protocols, but even the latter are not equally secure. The authors present how to use applications safely, how to communicate safely and what preventive measures every user of any electronic device must know to reduce the possibility of being hacked or infected with malicious software. A secure chat app should have the following features:

- Encryption of messages on all levels of communication.
- End-to-end encryption so that communications cannot be read by employees of the company operating the messaging service.
- Ability to verify who you are communicating with.
- Security of communication history in case of theft of encryption keys.
- Application code can be evaluated by external and independent inspectors.
- The design and implementation of cryptography is documented.
- The code has been verified/assessed within the last year.

Based on research and experience from practice, the authors provide the following recommendations for the end user for the safe use of communications and applications:

- Installing an anti-virus system on smart devices and computers.
- Strong passwords and activation of two-factor authentication.
- Download applications only from official online stores.
- Before setting up the application, check the terms of usage and what permissions the application needs.
- Regularly uninstall apps you no longer need
- Installing operating system and application updates.
- Broadcast your geolocation only when needed.
- Back up your data regularly.
- File encryption or e-mail attachment to protect the content and send the password to the recipient via another channel, e.g. SMS to mobile phone.
- Protection of the authenticity of the sender with a digital signature.