EKONOMSKA ŠOLA NOVO MESTO

VIŠJA STROKOVNA ŠOLA

VARNA RABA INTERNETA

PROJEKTNA NALOGA

UVOD

Slovenski prevod besede Internet je Medmrežje, kratko tudi Splet. Internet je omrežje med seboj povezanih računalnikov. Povezan mora biti na vsaj en strežnik, ki zagotavlja protokol za komuniciranje med računalniki. Spletno komuniciranje pri vsakdanji rabi ponuja številne prednosti in priložnosti, hkrati pa nas postavlja pred nova vprašanja glede varnosti. Ko beseda nanese na varnost si začnemo postavljati vprašanja ali smo danes na internetu sploh lahko še varni?

V seminarski nalogi bom poskušala predstaviti čim več načinov kako se na internetu obvarovati pred zlorabami in kako moramo svoj računalnik zaščititi, da ne pride do zlorab.

INTERNET

Internet lahko opredelimo kot računalniški dostop do informacij, shranjenih v drugih računalnikih po svetu. V praksi pridemo do takih informacij tako, da v računalniku zaženemo program, ki je namenjen iskanju informacij in ki mu pravimo spletni brskalnik.

Nevarnosti Na Internetu-Spletne Goljufije

Spletno komuniciranje pri vsakdanji rabi ponuja številne prednosti in priložnosti, hkrati pa smo z uporabo interneta vsak dan izpostavljeni nekaterim nevarnostim. Te nevarnosti so:

Krediti Prek Spleta

Bodimo pozorni na sledeče znake prevare:

Najbolj resen znak za alarm je, če nekdo od nas zahteva plačilo preko sistema Western Union! Ta sistem je namenjen hitremu prenosu denarja fizičnim osebam, sledenje nakazilu pa ni možno in je prav zato priljubljeno orodje spletnih goljufov.

Bodimo pozorni na “polomljeno” slovenščino. Tudi v tem primeru, je vsa komunikacija potekala v slovenščini, vendar so bili odgovori očitno prevedeni s strojnim prevajalnikom Google Translate.

Uporaba brezplačnih elektronskih predalov. Vedno preverimo elektronski naslov pošiljatelja. Se elektronski naslov ujema z naslovom uradne institucije? Banka prav gotovo ne bi uporabljala brezplačnega poštnega predala.

Prijateljeva Prošnja Za Pomoč

Preko e-mail naslova nam znanec na hitro opiše, kako so mu na potovanju v tujini ukradli denar in vse dokumente. Sedaj nujno potrebuje denar, da bo lahko plačal hotel in se vrnil domov.

Ukradeno geslo goljufu omogoči, da sporočila pošlje samo osebam, s katerimi se tudi sicer vaš prijatelj dopisuje. Takšno lažno sporočilo bo verjetno polno slovničnih napak, saj bo goljuf uporabil strojni prevajalnik, ali celo v angleščini. Pomembno je, da prijatelju ne pomagate z odgovorom na to sporočilo, ampak ga skušajte kontaktirati kako drugače in preveriti, če dejansko prosi za pomoč.

Ponudba Za Delo Od Doma

Delo od doma oz. delo prek spleta se je izkazalo kot odlična priložnost za goljufe, ki obljubljajo neverjetne zaslužke za skoraj nič truda. Tovrstne ponudbe oglašujejo kar na Facebooku, nanje naletimo na številnih forumih in spletnih oglasnikih.

Phishing Kraja Podatkov

S tem imenom poimenujemo krajo podatkov, ki storilcu omogočijo dostop do spletnih storitev v vašem imenu in v skrajnem primeru tudi krajo vašega denarja.

S phishing prevaro spletni goljuf pridobi osebna uporabniška imena in gesla za dostop do storitev kot so elektronska pošta, Facebook ali PayPal. Če goljuf pridobi geslo za spletno banko, nas lahko oškoduje tudi finančno!

Nigerijska In Loterijska Prevara

Milijonski loterijski zadetki ali neverjetne poslovne ponudbe so v naših e-poštnih nabiralnikih pogoste in mamljive. Žal ne pomenijo bogastva, le opozarjajo na klasično spletno goljufijo – nigerijsko prevaro.

Scenarij je vsakokrat drugačen (zadeli ste na loteriji, odkrili so skrite račune na bankah, vi ste dedič ogromnega premoženja, skratka želijo vam nakazati večjo vsoto denarja), osnovni mehanizem goljufije pa ostaja enak. Z zelo privlačno ponudbo goljufi vzpostavijo komunikacijo z nami (to je lahko prek elektronske pošte, prek spletnih oglasnikov, prek Facebooka itd.), nato nam avtor prevare sporoči, da moramo, zaradi potrebe tega ali onega postopka, najprej poravnati minimalno vsoto. Najprej prosijo za naše podatke (ime, priimek, številko tekočega računa).

Kmalu za tem nas pozovejo, da poravnavamo stroške odprtja novega računa, največkrat preko sistema Western Union. Gre za plačilni mehanizem, ki ne omogoča sledenja transakciji in je ravno zato priljubljeno orodje spletnih goljufov.

Nato sledijo vedno novi izgovori, potrebno je plačati davek, stroške vodenja računa, stroške odvetnika itd. Ko prenehamo s plačevanjem (izmišljenih) stroškov in zahtevamo obljubljeno nagrado, se tudi komunikacija prekine. Tudi če goljufijo prijavimo policiji, so možnosti za povrnitev denarnega oškodovanja praktično nične, saj se goljufi nahajajo v državah, kjer ne moremo računati na uspešen pregon tovrstnih kaznivih dejanj, npr. Nigerija, Gana, Kamerun. Ko denar nakažemo, smo ga pravzaprav nakazali goljufu!

VOHUNSKA PROGRAMSKA OPREMA, ADWARE, TROJANSKI KONJI IN ROOTKITI

Vohunska programska oprema je še ena izmed kategorij škodljive kode. Taki programi se naselijo v računalnik med običajnim brskanjem po internetu, pri čemer za okužbo računalnika izrabijo varnostne pomanjkljivosti spletnega brskalnika.

Adware je kategorija škodljive kode, ki izbira podatke o nas in naših internetnih navadah. Taki predstavniki škodljive kode sporočajo svoje ugotovitve različnim agencijam, ki nas nato zasipajo z oglasi in neželeno elektronsko pošto. Vohunska oprema in adware se od virusov in črvov razlikujeta po tem, da se iz našega računalnika ne moreta širiti naprej v druge računalniške sisteme.

Trojanski konji so vrsta škodljivcev, ki se v računalnik pritihotapijo v preobleki legitimnega programa. Ko uporabniki namesti legitimni program, se hkrati namesti tudi trojanski konj, ki napadalcu omogoči prevzem nadzora nad računalnikom.

Izraz rootkit je med računalničarji prisoten že več kot 10 let. Gre za paket sestavljen iz majhnih in uporabnih programov, ki napadalcu omogočajo ohranjanje dostopa na ravni »root« uporabnika. Definicija takih programov bi se glasila: Rootkit je skupek programov, ki napadalcu omogočajo stalno in prikrito prisotnost v žrtvinem računalniku.

UKREPI PROTI RAČUNALNIŠKIM VIRUSOM IN VDORI

V Računalnik Namestimo Protivirusni Program Oziroma Protivirusni Ščit

S protivirusnim programom lahko kadar koli pregledamo katero koli datoteko v računalniku ali na pomnilniškem nosilcu in preverimo, ali so morda okuženi z virusi. Protivirusni ščit pa opravlja to nalogo samodejno pri vsakem poskusu zapisovanja nove datoteke v računalnik. Protivirusna »zdravila« ponuja veliko proizvajalcev, ki jih lahko poiščemo na internetu, zanje pa se lahko obrnemo tudi na ponudnika internetnih storitev. (Kostrevc, 2006, str. 25)

V Računalnik Namestimo Požarni Zid

Požarni zid je programska ali strojna rešitev, ki upravlja z internetno komunikacijo našega računalnika. Ta zazna poskuse vdorov v računalnik iz interneta in jih tudi prepreči. Takim vdorom so najbolj izpostavljeni računalniki, ki so z internetom stalno povezani, in sicer s povezavo ADSL ali kabelsko.

Požarni zid vsebuje tudi program Windows XP, seveda pa ga moramo vklopiti. (Kostrevc, 2006, str. 26)

ZAKLJUČEK

Z izdelavo projektne naloge sem se zelo veliko naučila. Ugotovila sem katere nevarnosti nam prežijo pri vsakdanji uporabi interneta. Naučila sem se katere vrste spletnih prevar poznamo in kakšno škodo nam le te povzročijo. Zavedam se, da je le teh iz dneva v dan vse več. Naučila sem se tudi, kako se moramo na internetu obnašati in kako moramo naš računalnik že vnaprej zaščititi da do teh prevar sploh ne pride.