HITRI VODNIK

abc varnosti na spletu

VARNI NA INTERNETU

Od mene je odvisno vse.

www.varninainternetu.si

EN KLIK, TISOČ POSLEDIC

Vse se zgodi na spletu. Eksotične počitnice, dobra kupčija, kultni film, vroče novice, prijateljstvo. Dogaja se ves čas, vsako sekundo. Z njim je vse laže, hitreje, bolj učinkovito, bliže, velikokrat tudi ceneje.

Toda vsi na spletu ne igrajo po pravilih, zato je pomembno, da se zaščitite pred spletnimi prevarami.

NE NASEDAJTE PRAVLJICAM

Izogibajte se nakupu storitev ali izdelkov, ki jih neznani ali ponudniki dvomljivega slovesa ponujajo po neverjetnih cenah.

VEDITE, S KOM IMATE OPRAVKA

Pred namestitvijo programske opreme, nakupom izdelka ali posredovanjem osebnih podatkov se vedno skrbno pozanimajte, komu nameravate zaupati svoje podatke oziroma denar.

NE IZPOSTAVLJAJTE SE

Nikoli ne uporabljajte javnih računalnikov (knjižnice, cyber cafe) za dostop do družabnih omrežij, spletnega bančništva ali drugih spletnih mest, kjer se morate izkazati z uporabniškim imenom in geslom.

PODROBNOSTI ZADRŽITE ZASE

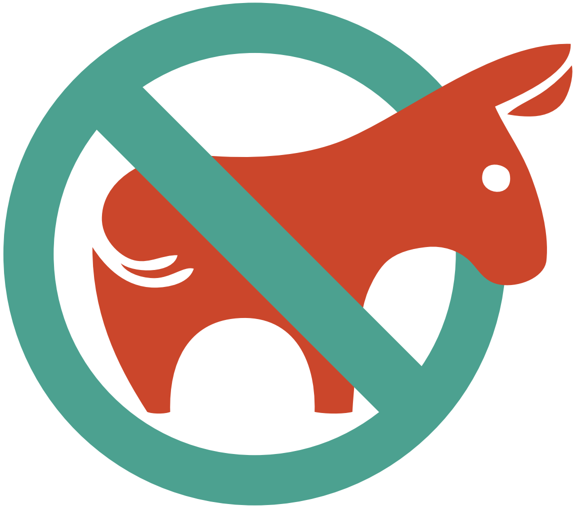
Osebnih in bančnih podatkov ne pošiljajte prek spleta, preden natančno ne preverite identitete tistega, ki vas prosi za te podatke.

ZAŠČITITE RAČUNALNIK

Namestite požarni zid in protivirusni program, vse potrebne popravke svojega operacijskega sistema in najnovejšo različico spletnega brskalnika.

PAZITE NA GESLA

Izberite geslo, ki ga ni lahko uganiti (daljše od 8 znakov, vsebuje naj male in velike črke, številke in ločila), in ne uporabljajte enakega gesla za vse uporabniške račune. Nikomur ne zaupajte svojega gesla in ga ne shranjujte v bližini svojega računalnika.



NAJPOGOSTEJŠE SPLETNE PREVARE

NIGERIJSKA IN LOTERIJSKA PREVARA

Milijonski loterijski zadetki ali neverjetne poslovne ponudbe v naših e-poštnih nabiralnikih so pogosti in mamljivi. 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, ste dedič ogromnega premoženja, skratka želijo vam nakazati večjo vsoto denarja), osnovni mehanizem goljufije pa ostaja enak: z zelo privlačno ponudbo vzpostavijo komunikacijo z nami, 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). V naslednjem koraku nam sporočijo, da so za potrebe transakcije odprli nov račun – v dokaz pošljejo tudi nekakšno potrdilo o novem računu, odprtem na naše ime. Kmalu po tem pozovejo k nakazilu denarja za povračilo stroškov, temu pa sledi cela vrsta drugih izgovorov (carina, plačilo odvetnika …) za ponovno nakazilo denarja.

Ko denar nakažemo, smo ga pravzaprav nakazali goljufu!

Pozornost zahtevajo velike obljube, nerazumljiva govorica in nenavadne dežele.

Prosimo, Odgovori

Mr.Frank Morgan (frank.morgan101@verizon.net) 15.9.2011 10:40

Za: janez_novak@guest.arnes.si;

Dober dan,

Jaz sem Frank Morgan, jaz delam v računovodskem oddelku hiše finance tukaj v Evropi. Videl sem vaš stik med moje zasebno iskanje na informacijski center, želim verjeti, da vas bo zelo iskren, predano in lahko pomaga pri tem poslu.
Temelji na tem, da sem se obrnete vas stati kot naslednji-of-sorodstvu pozno stranko Finance House, tako da bo skupna vsota $ 16.5million (šestnajst milijonov petsto tisoč ameriških dolarjev), se sprosti in plačanih za vas, kot upravičenec in naslednji-of-kin do umrlega.
Vsi dokumenti, in dokaz, da boste dobili sredstva so bila skrbno izdelane kot sem zavarovani iz različnih uradov, ki skrbijo za nemoten prenos sklada za vas.
Če je ta predlog vam ustreza, odgovorite mi z naslednjimi podatki.
-FULL IMENA
-TELEPHONE/FAX NUMBER-
-NASLOV-
-AGE-
-SEX-
-poklica-
Čakam na vaš hiter odziv, vse najboljše in Bog vas blagoslovi.
S spoštovanjem,
Frank Morgan
+447031901697
mrfrankmorgan444@hotmail.com

PHISHING

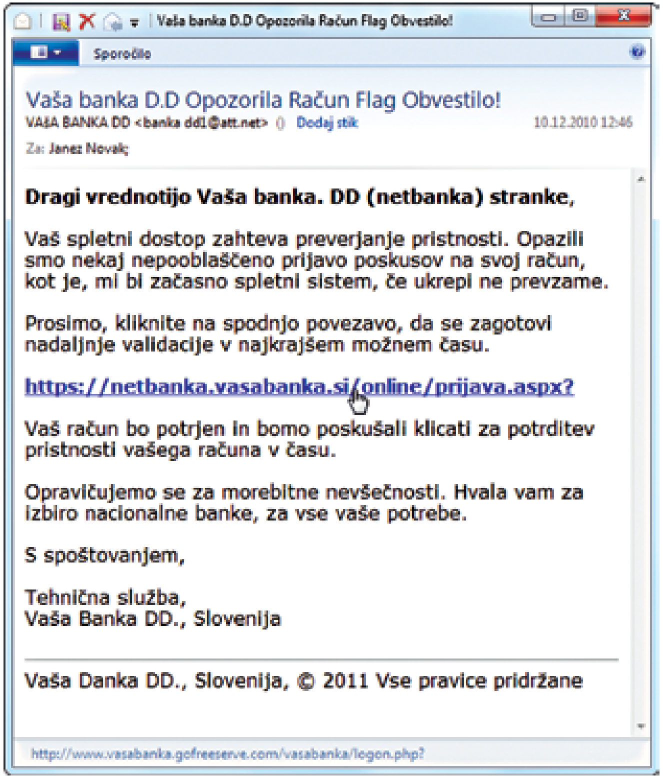
S phishingom spletni goljuf pridobi osebna uporabniška imena in gesla za dostop do storitev, kot so elektronska pošta, Facebook ali PayPal. Če goljuf pridobi geslo za spletno banko, nas oškoduje tudi finančno.

Tipična prevara s phishingom se začne z elektronskim sporočilom, ki naj bi ga poslala naša banka ali ponudnik neke spletne storitve. Obvestijo nas, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in ponovno vnesti svoje podatke. V sporočilu je tudi povezava, na katero naj bi kliknili, ki pa nas vodi na lažno spletno stran, zelo podobno, morda skoraj identično strani legitimnega ponudnika.

Če na tej lažni, phishing strani vpišemo geslo za dostop in druge osebne podatke (npr. podatke o kreditni kartici), smo jih pravzaprav posredovali goljufu.

!

Banka nas nikoli ne bi pozvala k pošiljanju osebnih podatkov prek elektronskih sporočil.



Vaša banka D.D Opozorila Račun Flag Obvestilo!

VAŠA BANKA DD <banka dd1@att.net> 10.12.2010 12:46

Za: Janez Novak;

Dragi vrednotijo Vaša banka. DD (netbanka) stranke,

Vaš spletni dostop zahteva preverjanje pristnosti. Opazili smo nekaj nepooblaščeno prijavo poskusov na svoj račun, kot je, mi bi začasno spletni sistem, če ukrepi ne prevzame.

Prosimo, kliknite na spodnjo povezavo, da se zagotovi nadaljnje validacije v najkrajšem možnem času.

https://netbanka.vasabanka.si/online/prijava.aspx?

Vaš račun bo potrjen in bomo poskušali klicati za potrditev pristnosti vašega računa v času.

Opravičujemo se za morebitne nevšečnosti. Hvala vam za izbiro nacionalne banke, za vse vaše potrebe.

S spoštovanjem,

Tehnična služba,
Vaša Banka DD., Slovenija

Vaša Danka DD., Slovenija, © 2011 Vse pravice pridržane

http://www.vasabanka.gofreeserve.com/vasabanka/logon.php?

GOLJUFIJE PRI SPLETNI PRODAJI IN NAKUPIH

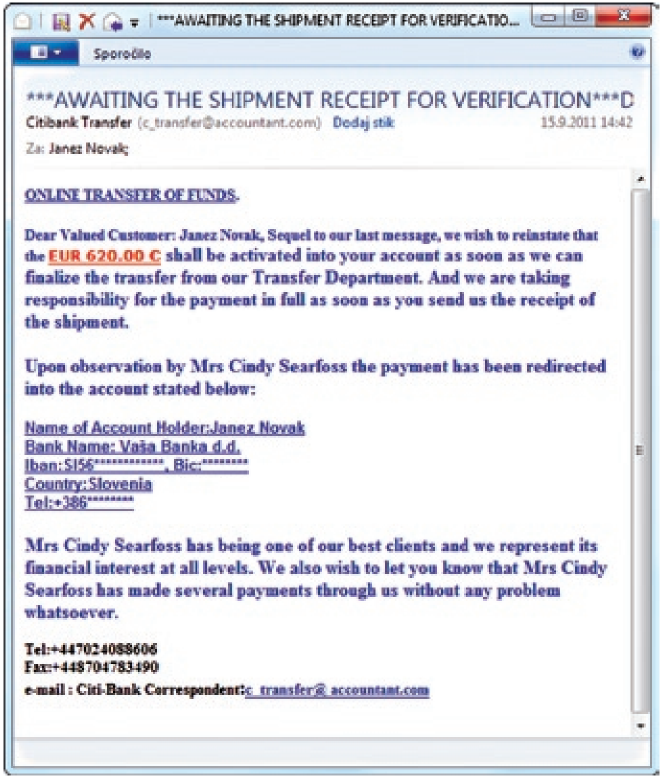
Meja med dobro kupčijo in opeharjeno denarnico je na spletu tanka. Za goljufe so še posebej privlačne spletne strani z malimi oglasi, kot so denimo bolha.net, nepremicnine.net, avto.net in njim podobne.

Goljufija se po navadi začne tako, da se goljuf oglasi na naš mali oglas. Predstavi se kot mogoči kupec in navede, da je rezident evropske države, a da kupuje fotoaparat za sorodnika v Nigeriji. Ker so sporočila včasih zasilno prevedena v slovenščino s spletnim prevajalnikom Google Translate, je jezik v njih zelo okoren in težko razumljiv.

Pri plačilu naj bi posredoval PayPal ali kakšen drug zaupanja vreden sistem plačevanja prek spleta. Pozove nas, da mu pošljemo paket z izdelkom in njegovo sledilno številko, čemur naj bi sledilo plačilo na naš osebni račun. Goljuf tudi pošlje lažna sporočila posrednika ali banke in zahteva dodatna plačila za izvedbo transakcije.

Prevara pa deluje tudi v nasprotni smeri. Goljuf objavi mali oglas, v katerem prodaja določeni izdelek (največkrat avtomobil) po izredno ugodni ceni. S prav tako lažnimi sporočili logističnega podjetja nas želi prepričati, da bo izdelek odpremljen, le da moramo najprej nakazati del kupnine, običajno nekaj tisoč evrov.

Vedno preverite dejansko identiteto pošiljatelja sporočila oziroma institucij, na katere se sklicuje (denimo PayPal).



AWAITING THE SHIPMENT RECEIPT FOR VERIFICATIOND
Citibank Transfer (c_transfer@accountant.com) 15.9.2011 14:42
Za: Janez Novak;

ONLINE TRANSFER OF FUNDS.

Dear Valued Customer: Janez Novak, Sequel to our last message, we wish to reinstate that the EUR 620.00 € shall be activated into your account as soon as we can finalize the transfer from our Transfer Department. And we are taking responsibility for the payment in full as soon as you send us the receipt of the shipment.

Upon observation by Mrs Cindy Searfoss the payment has been redirected into the account stated below:

Name of Account Holder:Janez Novak
Bank Name: Vaša Banka d.d.
Iban:SI56************, Bic:********
Country:Slovenia
Tel:+386********

Mrs Cindy Searfoss has being one of our best clients and we represent its financial interest at all levels. We also wish to let you know that Mrs Cindy Searfoss has made several payments through us without any problem whatsoever.

Tel:+447024088606
Fax:+448704783490
e-mail : Citi-Bank Correspondent:c_transfer@ accountant.com

KRAJA IDENTITETE

Neznana oseba pridobi naše osebne podatke in se začne predstavljati v našem imenu. Posledično lahko zavede naše sodelavce ali prijatelje, okrni naš ugled ter si pridobi dostop do naših informacij, denarja ali slik.

Kako lahko neznanec prevzame našo spletno identiteto? Najlažje takrat, kadar smo sami nepazljivi in ko po nesreči ali celo namerno razkrijemo geslo za e-pošto ali Facebook. Naslednji način je phishing oziroma kraja podatkov, ko nas elektronsko sporočilo pripravi do tega, da razkrijemo svoje uporabniške podatke.

Lahko se tudi zgodi, da je naš računalnik okužen; takrat nam lahko podatke »ukrade« podtaknjeni program. Med goljufi pa so priljubljena mesta za krajo osebnih podatkov tudi cyber cafeji oziroma računalniki, ki jih uporabljamo na potovanjih, da bi plačali račune ali pa pogledali elektronsko pošto, novice na Facebooku ali, denimo, naložili fotografije na splet.

! Z geslom ravnajte
kot z zobno ščetko – ne posojajte ga
in ga redno menjajte!

Kako so mi ukradli identiteto

Minuli teden so z mojega zasebnega spletnega naslova na vse konce sveta potovala sporočila, češ da sem v stiski v tujini in da nujno potrebujem denarno pomoč. Sporočil seveda nisem pošiljala sama. Gre za še en primer kraje identitete na spletu, o čemer veliko slišimo, a mislimo, da se dogaja samo drugim. Nekaj izkušenj s krajami v resničnem svetu že imam: ukradli so mi avto, dvakrat sem ostala brez denarnice in dokumentov, vlomili so mi v stanovanje. Kraja v virtualnem svetu pa se mi nikoli ni zdela resna grožnja, saj sem skrajno konservativna uporabnica spleta.

Pa vendar mi je nekdo ukradel geslo za e-naslov na hotmailu. Posledice: nepovratno sem ostala brez vseh shranjenih sporočil v nabiralniku, veliko znancev je bilo zaskrbljenih, le malo pa je manjkalo, da neka prejemnica "mojega" pisma ni nakazala denarja v London in me rešila iz domnevnih škripcev.

Ilinka Todorovski

Finance, 30.8.2010

PREVARE NA DRUŽABNIH OMREŽJIH

Družabna omrežja nam omogočajo razvijanje stikov s širokim krogom ljudi. Bolj so priljubljena, bolj se razvijajo tudi goljufije, ki to »povezovanje« in »druženje« izkoriščajo za širjenje prevar.

Najbolj neposreden primer prevare v družabnih omrežjih je prošnja za pomoč. V njej se goljuf predstavi z identiteto, ki jo je ukradel našemu prijatelju oziroma znancu, in nas prosi za denarno pomoč. Tako sporočilo bo verjetno polno slovničnih napak ali celo v angleščini.

Številčnost uporabnikov družabnih omrežij in njihovo medsebojno zaupanje omogočata tudi hitrejše širjenje zlonamernih programov. Škodljivo kodo lahko nevede razširjajo tudi naši prijatelji, s pošiljanjem nenavadnih povezav – največkrat gre za povezave, ki naj bi vodile do zelo zanimivega video posnetka. Po navadi gre za ponarejene Youtubove strani, ki od nas zahtevajo posodobitev predvajalnika Adobe Flash. Če na taki strani »izberemo« posodobitev predvajalnika, smo pravzaprav začeli nameščati zlonamerni program, ki bo okužil računalnik.

! Prijatelju ne pomagamo, preden osebno ne preverimo, ali dejansko prosi za pomoč.