Phishing ("pecanje podataka" putem e-pošte)

Što je phishing?

Phishing je proces putem kojega prevaranti dobivaju pristup osjetljivim podacima poput korisničkih imena, lozinki ili podataka s kreditnih kartica, slanjem lažnih elektroničkih ili tekstualnih poruka koje izgledaju kao da su ih poslale legitimne organizacije. Poruke najčešće izgledaju kao da dolaze od banaka, popularnih društvenih mreža ili internetskih stranica za prodaju i kupnju. *Phishing* se uglavnom izvodi putem e-poruka ili tekstualnih poruka u realnom vremenu (*instant messaging*), u kojima se od korisnika često traži da na lažnim internetskim stranicama (koje su gotovo identične stvarnim stranicama) ostave svoje podatke. Čak i dok koristite legitimne stranice banke, ponekad se na njima mogu pojaviti lažni skočni prozori (*pop-ups*). Čim kliknete na takav prozor ili unesete svoje osobne podatke ili podatke za identifikaciju, vaši podaci odlaze nekom drugom pružatelju usluga ili trećoj strani koja nije vaša banka. To znači da od toga trenutka nadalje netko drugi može pristupiti vašim računima. Postoje e-poruke koje sadrže linkove i žele vas navesti da posjetite web stranice na kojima ćete preuzeti štetne ili maliciozne programe (*malware*) uz čiju pomoć prevaranti mogu doći do vaših podataka i vašeg novca.
Iz privitka se može instalirati i tzv. *ransomware,* a ne samo *malware.* Takvi programi šifriraju vaše datoteke, uključujući glazbu i fotografije, a prevaranti od vas traže „otkupninu" kako biste ih dobili natrag.
Zaštitite vaša računala i druge uređaje najnovijim sigurnosnim rješenjima i programima najnovijim sigurnosnim rješenjima, te budite na oprezu prilikom otvaranja privitaka ili poveznica (linkova) u neočekivanim e-porukama ili porukama za koje niste sigurni da su vjerodostojne. Svakako napravite sigurnosne kopije svih važnih datoteka u neumreženim mapama te nikada ne plaćajte otkupninu kriminalcima.

E-poruke od vaše banke

Vaša vam banka povremeno može poslati e-poruku s korisnim savjetima ili informacijama o proizvodima ili uslugama, ali vam:

- nikada neće poslati e-poruku koja sadrži poveznicu (link) koja vas izravno vodi na stranicu koja vas izravno vodi na stranicu Internet bankarstva,
- nikada neće poslati e-poruku u kojoj od vas traži da potvrdite podatke o svom bankovnom računu,
- nikada neće poslati e-poruku (ili vas nazvati) kako bi vas pitala za podatke o kreditnim karticama, PIN-ove, kôdove za prijavu (*one time passworde* - OTPove) i kôdove za autorizaciju transakcija (MACove) koje generira token, kao i lozinke,
- nikada neće poslati e-poruku u kojoj od vas traži da potvrdite nedavno obavljenu transakciju.

Ako ste dobili sumnjivu e-poruku koju je navodno poslala vaša banka, proslijedite je vašoj banci, a zatim čim prije obrišite poruku koju ste dobili.

Kako ga prepoznati?

Nestandardna e-adresa
Krivotvorene e-poruke mogu biti poslane s adresa koje su naizgled slične službenim adresama vaše banke, ali ako ih pažljivije pogledate uočit ćete razliku u odnosu na pravu adresu.

Neformalni pozdravi i osjetljiva pitanja
Lažna e-poruka može ali i ne mora biti naslovljena na vas osobno. Može počinjati vašim osobnim imenom ali i npr. sa „Cijenjeni korisniče" i slično. Obično prevarant od vas traži osobne informacije poput lozinke, podataka o korištenju Internetskoga bankarstva, kontakata ili brojeva kreditnih kartica.

Neodloživi zahtjevi
U lažnim e-porukama često možete naići i na izraze poput ovoga: „Moramo potvrditi informacije o vašem računu". Na taj vas način žele natjerati da im odgovorite smjesta i bez razmišljanja.

Loš pravopis i oblikovanje teksta
E-poruka može sadržavati gramatičke i pravopisne greške. Nadalje, lažna internetska stranica može imati nešto drugačiji izgled te sadržavati pogrešno napisane riječi. E-poruka može biti napisana na lošem hrvatskom odnosno zvučati kao loš automatizirani prijevod (npr. s Google prevoditelja).

E-poruka bez teksta
Ako primite e-poruku bez teksta, samo s privitkom u prilogu, svakako postupite oprezno. Banka vam nikada neće poslati e-poruku bez ikakva sadržaja.

Neobične poveznice (linkovi)
Iako se poveznica (link) može činiti ispravnom, prije klika svakako provjerite pravu destinaciju na koju vas šalje. Prije nego

kliknete, prijeđite mišem preko poveznice (linka) i provjerite kako glasi adresa stranice na koju vas usmjerava. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.

Što poduzeti?

- Ograničite količinu osobnih podataka koji su javno dostupni na internetu, uključujući društvene mreže.
- Oprezno postupajte sa svim e-porukama. Povratne adrese ili adrese pošiljatelja mogu se lažirati. Potpunu e-adresu pošiljatelja možete provjeriti tako što ćete mišem prijeći preko naziva pošiljatelja. Zaglavlje e-poruke i poveznica na internetsku stranicu također se mogu lažirati. Prijeđete li mišem iznad poveznice, možete vidjeti potpuno drugačiju stranicu.
- Ne otvarajte poveznice iz neočekivanih ili sumnjivih e-poruka. Upišite adresu u internetski preglednik. Banka vam nikada u e-poruci neće poslati poveznicu na stranicu na kojoj se logirate u svoj bankovni račun ili na stranicu koja od vas traži sigurnosne ili osobne podatke. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.
- Nikada ne otvarajte privitke iz neočekivanih e-poruka (pogotovo one s nastavcima .exe, .pif ili .vbf)

Prijavi phishing

Dobijete li lažnu e-poruku, ostanite pribrani jer opasnost ne leži u primanju takve poruke. No nemojte otvarati poveznice (linkove) ili privitke iz takve poruke ili otkrivati podatke o internetskom ili mobilnom bankarstvu. Jednostavno ne odgovarajte na nju i izbrišite je. Ako vas neki od skočnih prozora traži vaše sigurnosne podatke, nemojte ih odavati. Prijavite lažnu e-poruku vašoj banci i pomozite u sprječavanju takvih prijevara.