NASES
NATIONAL AGENCY FOR NETWORK AND ELECTRONIC SERVICES

PHISHING

Čo je to phishing?

Phishing je podvodná činnosť kyberzločincov, pri ktorej sa snažia získať citlivé a dôverné informácie ako sú prihlasovacie údaje do rôznych účtov (email, internet banking...), čísla bankových účtov a platobných kariet vrátane PIN kódu, rodného čísla a pod.

Ako phishing funguje?

Najčastejšou formou je phishingový email, ktorý pôsobí ako správa od dôveryhodných spoločností. Takýto email nabáda používateľa si napr. zmeniť heslo do svojho účtu. V emaili je odkaz na phishingovú stránku, ktorá môže vyzerať na nerozoznanie od legitímnej stránky spoločnosti.

Po vložení údajov do formulára na phishingovej web stránke ich môže útočník ihneď zneužiť vo svoj prospech a pristúpiť k účtom obete, spôsobiť finančnú ujmu, ako aj získať ďalšie informácie, a tým ešte zväčšiť spôsobenú škodu. V prípade, ak používate rovnaké heslo vo viacerých účtoch, útočník môže zneužiť všetky účty.

PHISHING

Vzor phishingového emailu

Komu: Ján Zamestnanec <jan.zamestnanec@uzol.gov.sk>
Od: NASES <nases@security.com>
Predmet: Upozornenie – URGENTNE

Vážený pán/pani,

z bezpečnostných dôvodov je potrebné urgentne overiť prístupové údaje do vašej emailovej schránky. Na nižšie uvedenom odkaze, ktorý je zabezpečený šifrovaním, zadajte vaše prihlasovacie meno a heslo.

Bezpečný odkaz

Ďakujeme

NASES

Vzor legitímneho emailu

Komu: Ján Zamestnanec <jan.zamestnanec@uzol.gov.sk>
Od: NASES <info@nases.gov.sk>
Predmet: Upozornenie – zmena hesla

Vážený p. Ján Zamestnanec,
dovoľujeme si Vás požiadať o zmenu prihlasovacích údajov do Vašej emailovej schránky, návod nájdete na intranete v dokumente – Zmena prihlasovacích údajov.

Ďakujeme

Ivana Zamestnaná
Analytik
Sekcia bezpečnosti
direct +421 (0)2 3278 0780
gsm +421 (0) 917 000 000
ivana.zamestnana@nases.gov.sk
NASES
Národná agentúra pre sieťové a elektronické služby
BC Omnipolis
Trnavská cesta 100/II
821 01 Bratislava
nases.gov.sk

Ako konať v prípade, že som bol obeťou phishingového emailu a poskytol som citlivé údaje?

1. Kontaktujte zodpovednú osobu vo svojej organizácii.
2. Zmeňte si prihlasovacie údaje (ak používate rovnaké heslo na viaceré účty zmeňte si všetky, ktoré mohli byť dotknuté únikom informácií).
3. Berte to ako ponaučenie a vyvarujte sa rovnakej chybe v budúcnosti.

NASES
NATIONAL AGENCY FOR NETWORK AND ELECTRONIC SERVICES

Ako sa chrániť?

GOV CERT SK NASES
COMPUTER EMERGENCY RESPONSE TEAM
NATIONAL AGENCY FOR NETWORK AND ELECTRONIC SERVICES

1. Neverte zobrazenému menu odosielateľa

Obľúbeným trikom medzi kyberzločincami je falšovať zobrazované meno emailu. Ak kyberzločinec chce zosobniť nejakú značku alebo organizáciu napr. email môže vyzerať nasledovne:

Komu: Vaše meno <meno.priezvisko@uzol.gov.sk>

Od: NASES <nases@security.com>

Predmet: Upozornenie - neoprávnený prístup

Nakoľko doména "security.com" nepatrí do Govnetu, je takýto email veľmi podozrivý.

Akonáhle je takýto email doručený do Vašej schránky, email sa tvári legitímne - niektoré mobilné zariadenia zobrazujú len zobrazované meno (Display name) a preto treba byť obozretný.

Odporúčanie: Vždy, ak email vyzerá podozrivo, preverte odosielateľa v hlavičke emailu. Ak máte podozrenie, že ide o phishingový email - nahláste ho zodpovednej osobe.

2. Opatrne s prílohami

Prílohy v rôznych formátoch môžu obsahovať škodlivý softvér ako vírus, trójsky kôň, červy, spyware a pod., ktorý môže poškodiť Váš počítač a informácie v ňom.

Odporúčanie: Neotvárajte žiadne prílohy v emailoch, ktoré neočakávate a nie sú z dôveryhodného zdroja.

3. Nespoliehajte sa len na legitímne pôsobiacu emailovú adresu odosielateľa

Podvodníci nefalšujú len zobrazované meno odosielateľa, ale taktiež dokážu falšovať značku/ organizáciu aj v odosielateľovej emailovej adrese, zahŕňajúc doménu. V takom prípade sa nestačí spoľahnúť len na preverenie emailovej adresy odosielateľa.

Nezabudnite, že ak emailová adresa odosielateľa vyzerá legitímne, neznamená to, že email je legitímny.

Odporúčanie: Skontrolujte emailovú adresu odosielateľa a ak máte podozrenie, ako aj ďalšie znaky ktoré Vám pomôžu identifikovať email. V prípade, ak máte podozrenie, že ide o phishingový email - nahláste ho zodpovednej osobe.

4. Preverte, ale neklikajte

Kyberzločinci radi vkladajú do phishingových emailov odkazy, ktoré vyzerajú legitímne a obsahujúce škodlivý softvér. Vo phishingových emailoch môžu byť uvedené aj legitímne odkazy, medzi ktoré podvodníci skryjú podvodný odkaz.

Odporúčanie: Neklikajte na odkaz! Ak sa chcete presvedčiť, kam smeruje odkaz v tele emailu, môžete prejsť na odkaz myšou (neklikať) a zobrazí sa adresa. Skontrolujte všetky adresy, na ktoré odkazuje text v tele emailu. V prípade, že adresa pôsobí podozrivo, nahláste to zodpovednej osobe.

NASES
NATIONAL AGENCY FOR NETWORK AND ELECTRONIC SERVICES

PHISHING

GOV CERT SK NASES
COMPUTER EMERGENCY RESPONSE TEAM
NATIONAL AGENCY FOR NETWORK AND ELECTRONIC SERVICES

5. Skontrolujte pravopis a gramatiku

Keďže spoločnosti a organizácie dbajú na serióznosť svojich oficiálnych emailových správ, vo všeobecnosti neobsahujú gramatické a pravopisné chyby. V prípade, že sa v emaili objavia pravopisné chyby alebo gramaticky nesprávne výrazy, **môže** sa jednať o phishingový email.

Odporúčanie: Čítajte emailové správy s opatrnosťou a v prípade, ak máte podozrenie, že sa jedná o phishing - nahláste to zodpovednej osobe.

6. Skontrolujte oslovenie

Spoločnosti často oslovujú zákazníkov konkrétne - menom a priezviskom. V prípade, že v oslovení je len Vážený zákazník a pod., **môže** sa jednať o phishingový email.

Odporúčanie: Skontrolujte oslovenie v emaile - môže to byť jeden z viacerých znakov, že sa jedná o phishingový email.

7. Skontrolujte kontaktné informácie

V legitímnych emailoch od serióznych organizácií sú takmer vždy uvádzané kontaktné informácie v tele emailovej správy. V prípade, že tam kontaktné informácie chýbajú, môže ísť o podvodný email.

Odporúčanie: Skontrolujte kontaktné informácie, či sú uvedené v tele emailovej správy a či sú legitímne a skontrolujte ich v porovnaní s oficiálnymi kontaktnými informáciami uvedenými napr. na oficiálnej web stránke organizácie.

8. Pozor na požadované informácie

Väčšina serióznych spoločností nevyžaduje od svojich zákazníkov osobné údaje prostredníctvom emailu, hlavne nie banky. Ak spoločnosť prostredníctvom emailu a odkazy v ňom uvedené, vyžadujú osobné údaje alebo dôverné informácie, zastavte sa, overte si v inštitúcii, ktorá od vás informácie požaduje, či je ich žiadosť oficiálna a oprávnená.

Odporúčanie: Nezadávajte osobné údaje a dôverné informácie v prípade, že ich od vás žiada osoba/organizácia cez email a odkazy v ňom uvedené. Preverte si, či je žiadosť oficiálna a oprávnená na oficiálnych kontaktoch inštitúcie, nie cez informácie uvedené v podozrivom emaili (tie môžu byť taktiež podvrhnuté podvodníkmi).

9. Urgencia – časová tieseň

Kyberzločinci často používajú vo phishingových emailoch termíny, či už v predmete alebo v tele emailu, ktoré majú navodiť časovú tieseň (napr. URGENT, Vaše konto bude čoskoro zablokované) a prinútiť užívateľa, aby konal nerozvážne a bez dostatočnej obozretnosti.

Odporúčanie: Vždy konajte s rozvahou a nenechajte sa rozhodiť časovým nátlakom. Ak ste zaregistrovali časový alebo iný nátlak na Vás, aby ste konali, **môže** ísť o phishingový email. Ak máte podozrenie – nahláste to zodpovednej osobe.

10. Zlaté pravidlo – Neverte tomu čo vidíte a preverujte!

Informácie sú získané z voľne dostupných zdrojov a praxe