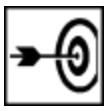
5. Další nebezpečné komunikační jevy

Osobní data ke kapitole

Obsah kapitoly

Text kapitoly

Cíle



Po prostudování této kapitoly budete umět:

- definovat termín phishing a uvést jeho příklady,
- uvést několik pravidel, jak se phishingu bránit,
- definovat a uvést příklady tzv. SMS spoofingu.

Doba potřebná ke studiu

Orientační čas potřebný k prostudování této kapitoly je 3x45 minut.

Průvodce studiem

V dnešní části našeho kurzu se zaměříme na další nebezpečné komunikační jevy, spojené s užíváním internetu a mobilních telefonů. Zaměříme se na oblast zneužití bankovního účtu a zneužití mobilního telefonu (SMS). Přejeme Vám hodně štěstí ve vašem studiu.

Phishing

Phishing je druhem nebezpečných komunikačních praktik, zaměřených na krádež citlivých osobních údajů - např. PIN kódu a čísel platebních karet, hesla a údaje k bankovnímu účtu a další informace, které by mohly být zneužity.

Slovo phishing vzniklo pravděpodobně spojením slov fishing, v rámci kterého došlo k homofonní záměně hlásky f a ph (v rámci tzv. leetspeeku, slangu internetové subkultury). V češtině narazíme na počeštělou variantu rhybaření, rhybolov apod. Existuje také výklad termínu, který tvrdí, že phishing je zkratkou slovo password harvesting fishing (rybolov sklízením hesel). Řada slovníků však považuje tento výklad za chybný.

Phishing je realizován zejména pomocí e-mailového spamu. Uživatelům je doručen důvěryhodně vypadající e-mail (často obsahující loga instituce, odkazy na reálné stránky instituce a informace, převzaté přímo z instituce - banky, pojišťovny, spořitelny), který oznamuje, že je z nějakého důvodu nutné přihlásit se na bankovní účet (pomocí jména a hesla). Uživatel, který uvěří sdělení, klikne na odkaz uvedený v e-mailu. Poté dojde k připojení na falešné internetové stránky, které jsou často věrnou kopií stránek banky uživatele (stejný design, často stejný obsah, stejná loga, pouze drobné odlišnosti zejména v internetové adrese). Pokud se na stránky přihlásí, dojde ke krádeži údajů k účtu.

Phishingové zprávy se často snaží vyvolat v uživateli pocit naléhavosti a nutnosti na e-mail reagovat.

Za phishing můžeme v širším slova smyslu považovat také různé druhy hoaxu, nigerijské dopisy slibující snadné zisky apod.

Příklady formulací útoku v rámci phishingu

Pokud neodpovíte do 48 hodin, váš účet bude zrušen. Pro obnovení účtu klikněte na tento odkaz.

Na váš účet byla připsána platba v cizí měně. Potvrďte prosím převod přihlášením se na svůj účet. Klikněte na tento odkaz.

Testujeme vyšší úroveň zabezpečení. Chcete li využívat vyšší úroveň zabezpečení, přihlaste se na svůj účet kliknutím na

tento odkaz.

Vyplňte dotazník a získejte odměnu 1500-2000 Kč. Detailní informace získáte po přihlášení na svůj účet.

Jak poznat phishing?

1. Na prvním místě je třeba říct, že většina bank s klienty e-maily nekomunikuje. Je tedy nepravděpodobné, že kdyby se něco důležitého stalo, využije pro komunikaci s vámi e-mail.

2. Všímejte si detailů! E-maily jsou často rozesílány hromadně a neobsahují vaše osobní údaje, např. jméno a příjmení! Často jsou phishingové e-maily plné pravopisných chyb - nejsou totiž psané přímo rodilým mluvčím, ale často překládány automatickými softwarovými překladači.

3. Prozkoumejte odkaz, na který máte kliknout. Zjistíte, že odkazuje jinam, než je na něm uvedeno. Všímejte i drobných chyb v odkazu, např. www.microsoft.cz může vypadat jako www.micosoft.cz, www.mircosoft.cz, www.verify-microsoft.cz apod. Tyto odchylky a chyby jso velmi zásadní a důležité.

Zkušenosti ze zahraničí

V anglicky mluvících zemích je tento typ krádeže poměrně běžný. Phishinovému útoku byly vystaveny firmy jako Microsoft, Bank of America, eBay, PayPal, Wester Union, iTunes, UniCreditBank, VISA apod. V České republice je dokumentováno jen málo případů, k nejznámější patří phishingový útok na Českou spořitelnu (březen 2008).

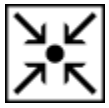
Pro phishing je také vytvořeno množství volně stáhnutelných programů (toolkitů), které umožňují virtuální útok na banku zrealizovat. Detaily naleznete např. na http://www.lupa.cz/clanky/jak-se-dela-phishing/. Řada výrobců software se phishing již účinně brání, phishingové filtry nalezneme např. v prohlížečích Firefox, Internet Explorer, případně rovnou v některých e-mailových klientech.

Mezi zářím 2006 a 2007 se oběťmi phishingu v USA stalo 3,6 milionu lidí. Na jednoho poškozeného připadá ztráta 866 dolarů (1244 v roce 2006). V roce 2007 se phishing postaral o celkové ztráty ve výši 3,2 miliardy dolarů (2,3 miliardy v roce 2006).

V roce 2006 získalo zpět 64% svých peněz 1.5 milionu postižených (1,5 milionu a 54 % v roce 2006).

Měsíčně je rozesláno na 2,2 miliardy phishingových e-mailů, 1 % oslovených na ně reaguje. Útočníci tímto způsobem "vydělají" až 80 milionů dolarů měsíčně.

Příklad z ČR - Útok na Českou spořitelnu (ukázka phishingu)



Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu. S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.

V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

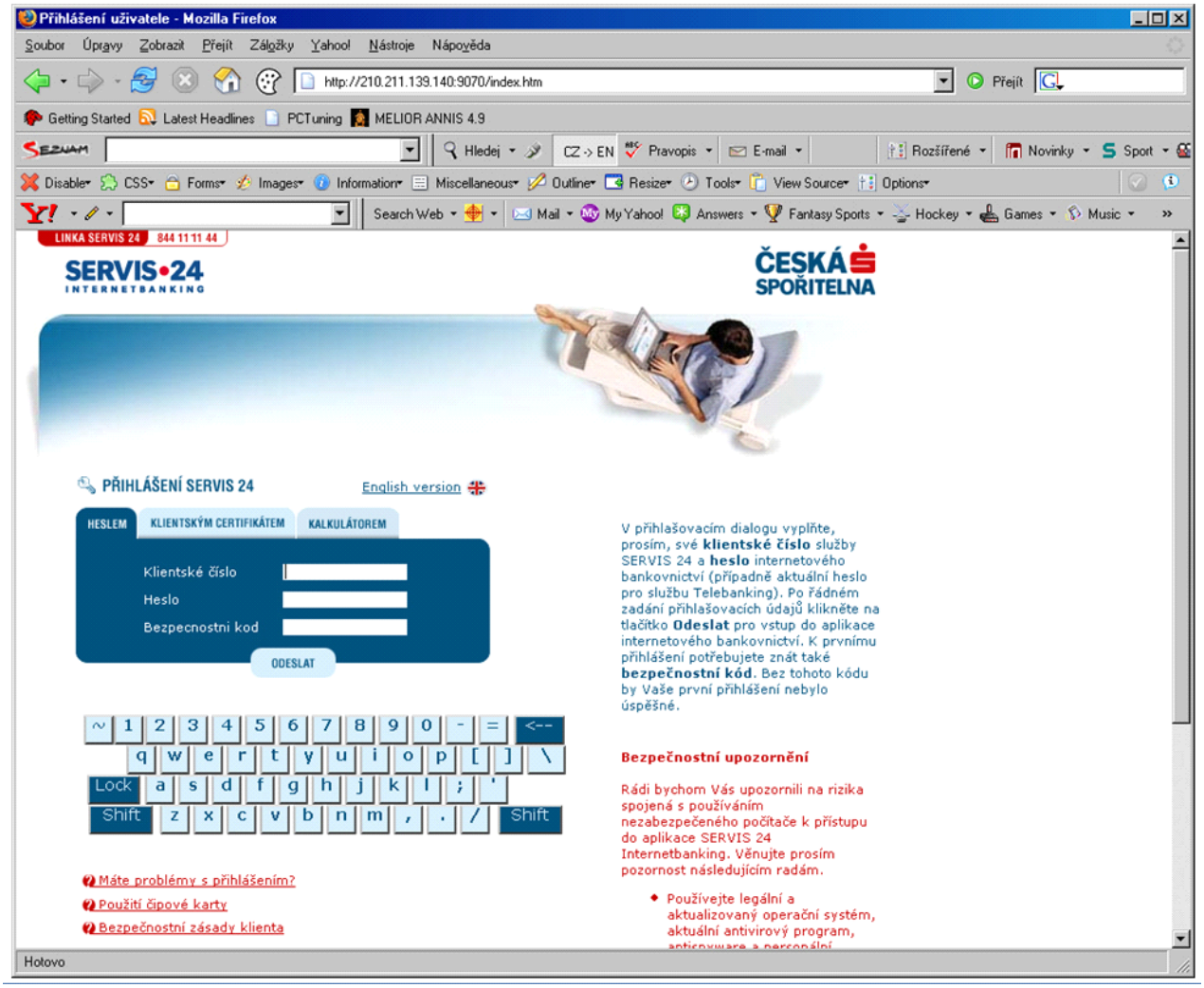
V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti.

Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem

Vzhled falešné stránky, na kterou e-mail odkazoval



Několik pravidel pro obranu před phishingem

1. Nikdy nesdělujte nikomu neznámému či nedůvěryhodnému (kromě zaměstnanců banky přímo v instituci banky) své údaje k bankovnímu účtu! E-mail není důvěryhodným komunikačním prostředkem! Nesdělujte je ani prostřednictvím telefonu (pokud bude banka volat vám).

2. Internet je obrovským zdrojem svobodných informací, ale tato svoboda zároveň dává mnoha podvodným živlům velký prostor pro vyvíjení různých podvodných aktivit (www.hoax.cz). Všechny informace z internetu si vždy ověřujte u důvěryhodných zdrojů.

Zdroje pro studium

První český phishing se stal realitou. IT Help

Rozpoznání podvodů typu phishing a falešných e-mailů

Dočkal, D. Jak se dělá phishing

Archiv portálu Lupa

Internetový portál E-Bezpečí

Průvodce studiem

V následující části textu se zaměříme na další nebezpečný fenomén, který se nazývá SMS Spoofing čili zneužívání SMS zpráv.

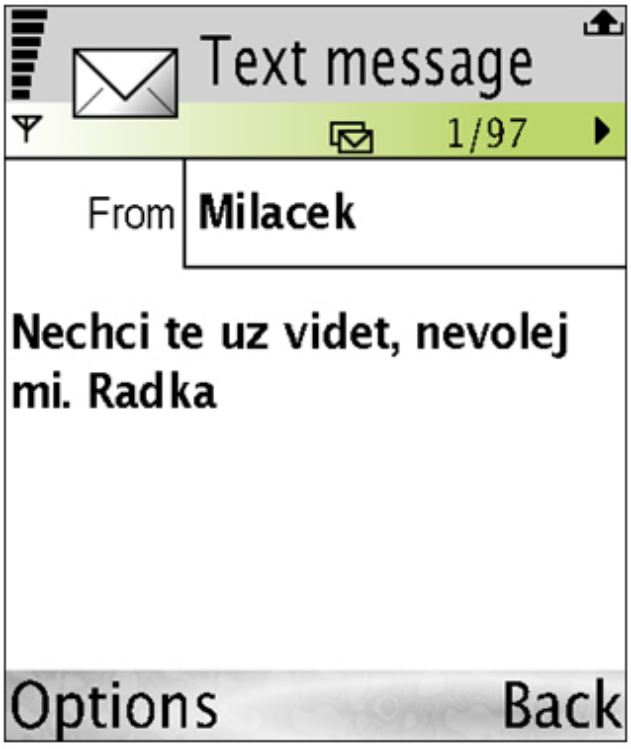
SMS Spoofing

V roce 2004 a 2005 zaznamenal svět případy „falešných SMS“. V praxi to vypadalo tak, že z SMS čísla Vašeho známého přišla neobvyklá SMS – například Váš partner Vám píše, že se s vámi rozchází, Váš šéf píše, že máte vyhazov apod. Většina uživatelů totiž vnímá důvěryhodnost SMS, pokud jsou identifikované číslem osoby, kterou znáte. Každá SMS zpráva v sobě obsahuje několik důležitých údajů – vedle samotného textu zprávy je to čas a datum odeslání, číslo SMS centra, odkud byla zpráva odeslána, a také telefonní číslo odesílatele. Právě díky tomu pozná příjemce zprávy, kdo ji odeslal. Mobilní telefon jen nahradí číslo jménem, pokud je máte uložené v telefonním seznamu.

Službu posílání falešných SMS poskytoval server www.smsspoofing.com. Ten vám umožňoval změnit číslo odesílatele, přestože je SMS odesílána z Internetu. K odeslání anonymní SMS postačí pouze počítač s připojením k internetu nebo mobilní telefon s webovým prohlížečem.

Aby to však nebylo málo, SMSspoofing.com nabízel první dvě odeslané SMS zcela zdarma. Pro odeslání dalších SMS zpráv je nutné zakoupit kredit, což můžete udělat pomocí platební karty, platbou přes systém elektronických plateb PayPal nebo se znovu registrovat na jiné číslo. Problém SMS spoofingu se často označoval za „SMS útoky“, v praxi však jde o nevinnou službu, která je již dnes dostatečně zabezpečena operátory, takže SMS z konkrétních domén nepropouštějí přes své SMS brány. Ostatně vyzkoušet si to můžete přímo online na výše uvedeném odkazu.

Ukázka SMS spoofingu v praxi



Shrnutí

Phishing a SMS spoofing představují nebezpečné techniky, jejichž podstatou je kritické posouzení informací, které nám jsou doručeny prostřednictvím internetu či mobilních telefonů. Jako v reálném životě je třeba vždy si každou informaci prověřit, na internetu můžete využít například www stránky www.hoax.cz.

Osobní data ke kapitole