Bezpečnost internetu

Základní výtah projektu S-Guardian

Vypracoval: SWA Lukáš Wolf - 774 354 138

I. Úvod
- Stručný úvod do problematiky bezpečnosti na internetu
- Vysvětlení, proč je důležité být obezřetný při používání internetu a jakým způsobem může být naše soukromí a bezpečnost ohroženo

II. Internetové podvody
- Přehled nejčastějších internetových podvodů (phishing, ransomware, malware, identitní krádeže, apod.)
- Popis, jakým způsobem mohou být uživatelé napadeni a jaká jsou rizika
- Ukázky praktických situací, kdy mohou být uživatelé ohroženi

III. Zabezpečení
- Popis různých možností zabezpečení na internetu (hesla, dvoufaktorová autentizace, zabezpečené připojení, VPN)
- Vysvětlení, proč jsou jednotlivé zabezpečovací prvky důležité a jaké jsou jejich výhody a nevýhody
- Ukázky praktického využití zabezpečení na internetu

IV. Praktická část
- Popis aplikace, která simuluje různé internetové podvody a útoky na uživatele
- Ukázka různých situací a návod, jak se bránit a jak dané útoky odhalit
- Možnosti, jakým způsobem lze zabránit útokům a jak zvýšit bezpečnost na internetu

V. Závěr
- Shrnutí hlavních závěrů a důležitých poznatků
- Upozornění na důležitost bezpečnosti na internetu a výzvu k obezřetnosti
- Informace o certifikátu a školení, které mohou uchazeči získat po absolvování této výuky

I. Úvod

Bezpečnost na internetu je velmi aktuální téma, které se týká všech uživatelů internetu. V dnešní době se většina činností odehrává online, od komunikace s přáteli a rodinou až po platby a nákupy. S tímto rozšířením internetu se však zvyšuje i riziko narušení naší soukromí a bezpečnosti. V dnešní době existuje mnoho nebezpečí, které hrozí uživatelům internetu. Mezi nejčastější patří například krádež identity, phishing, malware a ransomware. Tyto hrozby mohou způsobit finanční ztráty, narušení soukromí, a dokonce i krádež identity.
Proto je důležité být obezřetný při používání internetu a brát ohled na bezpečnostní opatření. Mezi základní bezpečnostní opatření patří například používání silných hesel, neotevírání podezřelých odkazů a souborů, aktualizace softwaru a používání antivirového programu.
V tomto dokumentu se budeme věnovat praktickým zkušenostem s internetovými podvody a způsobům, jak se chránit proti nim.

II. Internetové podvody

Internetové podvody jsou v dnešní době velkým problémem. Čím víc času trávíme online, tím větší je pravděpodobnost, že se staneme obětí internetových podvodů. Zde jsou uvedeny nejčastější typy internetových podvodů:

1. Phishing - podvodné e-maily nebo webové stránky, které se vydávají za legitimní, aby získaly citlivé informace, jako jsou hesla, bankovní údaje nebo osobní informace.
2. Ransomware - škodlivý software, který útočí na počítačové systémy a šifruje soubory, dokud není zaplaceno výkupné.
3. Malware - škodlivý software, který může poškodit nebo zneužít počítačový systém nebo ukrást citlivé informace.
4. Identitní krádeže - krádež citlivých informací, jako jsou jména, adresy, čísla sociálního zabezpečení nebo bankovní údaje, které jsou následně použity k podvodům.
5. Falešné služby a podvody na seznamkách a sociálních sítích: Popis toho, jak mohou být uživatelé oklamáni a jak se chránit před těmito podvody.
6. Falešné platby za zboží: Popis toho, jak mohou být uživatelé podvedeni při nákupu zboží na internetu a jak se chránit před těmito podvody.
7. Rozeznávání komunikace s internetovým protějškem: Vysvětlení, jak mohou být uživatelé podvedeni při komunikaci s někým na internetu a jak rozpoznat, zda je komunikační partner opravdu tím, za koho se vydává.
8. Internetové výkupné a šikana: Popis toho, jak mohou být uživatelé vydíráni a jak se chránit před těmito útoky, včetně ukázky praktických situací.

Rizika, která s sebou tyto podvody nesou, jsou značná. Pokud jsou citlivé informace získány, mohou být použity k finančnímu podvodu, krádeži identity nebo dalšímu zneužití.
Na školení budou představeny příklady konkrétních situací, kdy mohou uživatelé být ohroženi a jakým způsobem se mohou bránit. Tyto příklady zahrnují například falešné e-maily od banky, která žádá o aktualizaci hesla nebo podezřelé webové stránky, které nabízejí neuvěřitelné nabídky nebo ceny.

III. Zabezpečení

Zabezpečení na internetu je velmi důležité pro ochranu našich osobních údajů a soukromí. Existuje několik způsobů, jak lze zabezpečení na internetu realizovat. Některé z nejpoužívanějších jsou:

1. Hesla - Hesla jsou základním prvkem zabezpečení na internetu. Musí být složitá, ale snadno zapamatovatelná, aby uživatelé mohli snadno používat své účty. Hesla by měla být unikátní pro každý účet a pravidelně měněna.
2. Dvoufaktorová autentizace - Dvoufaktorová autentizace je dalším krokem v zabezpečení na internetu. Tento prvek zahrnuje více než jen heslo a vyžaduje druhý ověřovací krok, jako je například ověřovací kód zaslaný na mobilní telefon.
3. Zabezpečené připojení - Zabezpečené připojení je důležité pro ochranu vašich osobních údajů a soukromí při používání internetu. Použití zabezpečeného připojení znamená, že data, která přenášíte mezi vaším počítačem a serverem, jsou šifrována a tedy chráněna proti odposlechu.
4. Virtuální privátní síť (VPN) - VPN vám umožní chránit vaše soukromí a bezpečnost při používání veřejného internetového připojení. VPN vytváří šifrované spojení mezi vaším počítačem a internetovým serverem, což zaručuje, že vaše osobní údaje jsou bezpečné.

Výše uvedené prvky zabezpečení na internetu mají své výhody a nevýhody, a je třeba zvážit, které z nich jsou pro vás nejvhodnější. Důležité je také, aby byly správně implementovány, aby bylo dosaženo maximální ochrany.

Hesla jsou první linií obrany proti neoprávněnému přístupu. Je důležité, aby uživatelé používali silná hesla, která kombinují velká a malá písmena, číslice a speciální znaky. Dvoufaktorová autentizace poskytuje další vrstvu ochrany, kdy kromě hesla uživatel potvrdí svou identitu například pomocí SMS nebo mobilní aplikace. Zabezpečené připojení a VPN (Virtual Private Network) zabezpečují přenos dat mezi uživatelem a internetem a předejdou tak případnému odposlechu.

Je důležité zdůraznit, že ani silné heslo a dvoufaktorová autentizace nejsou stoprocentním řešením, protože například phishingové útoky mohou uživatele přesvědčit, aby své údaje poskytli do rukou útočníků. Je tedy třeba věnovat pozornost i dalším zabezpečovacím opatřením, jako je instalace antivirového softwaru a firewalu a pravidelné aktualizace operačního systému.
Ukázky praktického využití zabezpečení na internetu mohou být například simulace pokusu o hacknutí webové stránky, která není chráněna zabezpečeným připojením, nebo ukázka dvoufaktorové autentizace při přihlašování na bankovní účet.
Je nutné zdůraznit, že žádné zabezpečení není dokonalé a útoky jsou stále sofistikovanější. Proto je důležité nezanedbávat pravidla bezpečnosti a věnovat pozornost jakémukoliv podezřelému chování na internetu.

Dalším způsobem, jak mohou být uživatelé ohroženi, je pomocí techniky zvané "sniffing". Tento postup spočívá v odposlechu komunikace mezi uživatelem a cílovým serverem, kdy útočník zachytává data, která jsou posílána mezi oběma stranami. To může zahrnovat citlivé informace, jako jsou hesla nebo platební údaje. Další nebezpečí hrozí v podobě krádeže kódu skrze SMS, kdy útočník získá kód pro ověření identity uživatele, který je posílán prostřednictvím textové zprávy na mobilní telefon. Tyto útoky jsou stále častější a je důležité být obezřetný a chránit své citlivé údaje.

Kradený software může obsahovat viry, škodlivý kód nebo zranitelnosti, které mohou být zneužity k útoku na uživatele. Pokud uživatel přistoupí k neoprávněnému stažení softwaru z neznámých zdrojů, může to vést ke kompromitaci jeho zařízení a dat.
Rootování telefonu může poskytnout uživateli větší kontrolu nad zařízením, ale zároveň snižuje úroveň zabezpečení a může vést k možnosti útoků. Rootování může také způsobit ztrátu záruky na zařízení a některé aplikace a funkce mohou přestat fungovat správně. Podstatné je si uvědomit, že otevření systému může vést ke zpomalení systému, ztrátě kontroly a ztrátě osobních informací.

IV. Praktická část

V této části se zaměříme na praktickou stránku a na tvorbu aplikace, která simuluje různé internetové podvody a útoky na uživatele. Tato aplikace bude sloužit k výcviku uživatelů a pomůže jim se lépe připravit na možné útoky.
Hlavními funkcemi aplikace budou:

1. Simulace falešných profilů na sociálních sítích, a identifikace rizik spojených s nimi. Uživatelé budou moci vidět, jak falešné profily vypadají, jaké jsou typické prvky, které je odhalují, a jak se bránit proti útokům z těchto profilů.
2. Simulace podvodných eshopů a platebních systémů. Uživatelé se naučí, jak rozpoznat podvodné webové stránky, jaké jsou typické znaky těchto stránek a jak se chránit před podvodníky, kteří chtějí ukrást jejich peníze.
3. Simulace útoků pomocí ransomware, malware, phishingu a dalších technik. Uživatelé se naučí, jak identifikovat rizika a jak se bránit proti těmto útokům.
4. Identifikace falešných SMS a e-mailů a ochrana proti krádeži kódu. Uživatelé se naučí, jak se bránit proti krádeži citlivých údajů, jaká jsou rizika spojená s krádeží kódu skrze SMS nebo e-mail a jak tuto situaci řešit.
5. Identifikace falešných profilů na seznamkách. Uživatelé se naučí, jak identifikovat rizika spojená s používáním seznamovacích aplikací a jak se chránit před podvodníky a falešnými profily.
6. Identifikace falešných plateb za zboží. Uživatelé se naučí, jak identifikovat rizika spojená s platbami na internetu a jak se chránit před podvodníky a falešnými platbami.
7. Identifikace internetového výkupného a šikany. Uživatelé se naučí, jak se chránit před útoky na své osobní údaje a jak řešit situace, kdy jsou vydírání nebo šikanováni na internetu.

Cílem této aplikace bude naučit uživatele, jak se chránit proti různým internetovým podvodům a útokům a jak zvýšit bezpečnost na internetu. Aplikace bude k dispozici pro různé uživatele a jejich skill.

V. Závěr

Shrnutí hlavních závěrů a důležitých poznatků:
Po absolvování této výuky by měli účastníci mít lepší povědomí o bezpečnosti na internetu a být schopni se bránit proti nejrůznějším internetovým podvodům a útokům. Níže shrnujeme několik důležitých poznatků:

- Hesla jsou základem bezpečnosti a je důležité si vybírat dostatečně silná hesla, která jsou unikátní pro každý účet. Je rovněž vhodné je pravidelně měnit a uchovávat je v bezpečí.
- Dvoufaktorová autentizace poskytuje větší bezpečnost a ochranu před útoky, kde zloděj hesla získá přístup k účtu. Používání dvoufaktorové autentizace by mělo být považováno za standardní praxi.
- Zabezpečené připojení a VPN umožňují šifrování komunikace mezi uživatelem a serverem, což ztěžuje útokům odposlech. Používání těchto zabezpečovacích prvků je důležité, zejména při používání veřejných Wi-Fi sítí.
- Identifikace podvodných eshopů a falešných profilů na sociálních sítích je klíčová pro ochranu proti phishingovým útokům. Je důležité si ověřovat důvěryhodnost a kvalitu stránek, aplikací a profilů, se kterými uživatelé interagují.
- Kromě toho, účastníci by se měli naučit rozpoznávat a bránit se dalším nebezpečím jako jsou malware, krádeže dat a další útoky.

Výuka, jak se chránit před nebezpečím na internetu, je důležitá pro každého uživatele, bez ohledu na to, zda používá internet ke komunikaci, práci, zábavě nebo nakupování. Je to proto, že každý má právo na ochranu svých osobních údajů a bezpečnost online prostředí může být velmi křehká, pokud se nedodržují základní pravidla. Certifikát, který účastník obdrží po úspěšném absolvování výuky, slouží jako důkaz toho, že má základní znalosti o bezpečnosti na internetu a že by měl být schopen se chránit před nebezpečnými situacemi a nebezpečnými lidmi online. Zároveň školení pomáhá zvyšovat povědomí o problematice bezpečnosti na internetu a zvyšovat úroveň ochrany online prostředí.

Pokud uživatel úspěšně dokončí školení, obdrží certifikát o absolvování výuky bezpečnosti na internetu, který může přiložit ke svému životopisu a zvýšit tím své šance při hledání práce. Certifikát také může sloužit jako důkaz o získaných znalostech a zkušenostech pro současné zaměstnání. Pokud se uživatel rozhodne pro rekvalifikaci, školení z bezpečnosti na internetu může být užitečným základem pro další vzdělávání, například v oblasti programování, kódování, UX a UI.

SWA Lukáš Wolf
lukaswolf.pc@gmail.com
00420 774 354 138