V aktuálním IT Kompasu jsme pro Vás připravili:

157. číslo

Vybrané aktuality ze světa IT
Tipy – Triky
Soutěž
Vtip pro dobrou náladu

Vybíráme zajímavé aktuality:

Útočníci přizpůsobili šíření spywaru letním dovoleným
Ačkoli spyware v Česku v posledních měsících neútočil v žádné masivní kampani, rizikem zůstává i nadále. Kybernetičtí útočníci své strategie neustále proměňují na základě trendů a chování uživatelů. Více...

Hrozby pro Android: Největším rizikem zůstávají falešné aplikace
Ve více než třetině všech detekovaných případů pro platformu Android v Česku byl v červnu největším rizikem reklamní malware Andreed. Více...

Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na Facebooku .

Jak se nenechat chytit na triky hackerů, kteří číhají na sociálních sítích?

Sociální sítě používá více než polovina světa. Pro 4,62 miliardy lidí jsou sociální sítě součástí každodenního života. Přestože mohou být tyto platformy zábavné a usnadňují sdílení zážitků s přáteli, představují také hrozbu. Sociální sítě jsou totiž také oblíbeným prostředím kyberzločinců. Pokud se chcete chránit před triky hackerů, měli byste znát techniky, které používají, a nedělat triviální chyby. Sdílení osobních informací, odpovědi na nevyžádané e-maily s instrukcemi pro obnovení hesla, klikání na všechny odkazy a nekontrolování URL adres jsou totiž chyby, které mohou vést k získání přístupu k Vašim účtům na sociálních sítích.

Na jaká rizika si musíte dávat pozor a jakých nejčastějších chyb se dopouštíme? Společnost Check Point sestavila varování před čtyřmi největšími chybami, kterých je potřeba se vyvarovat při používání sociálních médií:

1. Nesdílejte osobní údaje: Jedná se o velmi častou a nebezpečnou chybu, která se na sociálních sítích děje každý den. Kyberzločinci se v první řadě snaží ukrást Vaše osobní údaje. Pokud získají cenná data, mohou je využít ve phishingových kampaních a například Vás okrást o peníze. Navíc většina lidí používá stejné přihlašovací údaje pro různé platformy, aplikace a služby, takže krádež jedněch přihlašovacích údajů umožňuje hackerům přístup k Vašim dalším účtům. Je proto nezbytné nesdílet osobní údaje a používat různá hesla, abyste minimalizovali škody, pokud se stanete obětí útoku.
2. Pozor na nevyžádané e-maily s instrukcemi pro změnu hesla: V současné době existuje tolik sociálních platforem, že úniky dat a bezpečnostní incidenty nejsou ničím ojedinělým, čehož mohou hackeři využít. Pokud Vám přijde e-mail s výzvou ke změně hesla, i když jste o to nepožádali, tak řada lidí na odkaz automaticky klikne a heslo resetuje. Ale kyberzločinci tak mohou získat přístup k Vašemu účtu. Pokud chcete heslo resetovat, neklikejte na odkaz ve zprávách a vždy navštivte přímo stránky dané sociální sítě a heslo změňte napřímo. Pokud máte podezření na nějaký únik dat, totéž udělejte u dalších stránek a služeb, kde jste používali stejné heslo.
3. Neklikejte na odkazy bez přemýšlení: Kyberzločinci často přesměrovávají uživatele na škodlivé stránky pomocí podvodných odkazů. Podobné odkazy mohou být ve zdánlivě nevinně vypadajících e-mailech nebo SMS zprávách. Pokud takový odkaz obdržíte, neklikejte na něj a navštivte danou stránku napřímo a zkontrolujte, jestli neobsahuje nějaké nové zprávy.
4. Zkontrolujte si URL adresu: Další trik, který útočníci používají ke krádeži údajů, je napodobování URL adres. Pomocí této techniky mohou hackeři přimět uživatele, aby navštívili webovou stránku, kterou považují za důvěryhodnou, například Facebook. Uživatel je následně vyzván ke změně nebo zadání hesla, čímž se ho útočníci zmocní. Ze zprávy výzkumného týmu Check Point Research vyplývá, že nejčastěji napodobovanou značkou při phishingových podvodech je LinkedIn. Je důležité si vždy zkontrolovat URL adresu, jestli vede na opravdu pravé stránky a jestli stránka používá bezpečnostní certifikát SSL. V adresním řádku by mělo být písmeno „s“ a měli byste tam tedy vidět https://. Díky této technologii jsou veškeré důvěrné informace přenášené mezi dvěma systémy chráněny, takže se kyberzločinci nedostanou k přenášeným údajům a osobním informacím.

Útočník si najde cestu i přes QR kód. Jak skenovat bezpečně?

QR kódy se staly vcelku běžnou součástí našich životů. Najdeme je například v elektronických SMS receptech od lékaře, na složenkách či fakturách, běžné jsou na různých vstupenkách či stolech restaurací a jsou také třeba na sdílených kolech a koloběžkách. Pomocí QR kódu můžete také v telefonu sdílet připojení k Wi-Fi síti, otevřít webové stránky nebo stáhnout a uložit soubor. Většina uživatelů již má v podvědomí neustále omílané poučky o klikání na podezřelé odkazy či spouštění podezřelých souborů, ale jak je to se skenováním QR kódů? Nejsou snad i zde nějaká rizika?

Odpověď je jednoduchá - i QR kód může být nositelem něčeho škodlivého, protože jsou poměrně náchylné na zneužití. A mohou klidně potrápit třeba zrovna Vaši peněženku. QR kód (QR = Quick Response, rychlá reakce) může obsahovat až 4296 alfanumerických znaků, lze do něj tedy schovat v podstatě cokoliv. Běžné QR kódy obsahují znaků méně a lze je velice snadno snímat pomocí chytrého telefonu. Některé telefony pro skenování potřebují speciální aplikaci (čtečku QR kódu), mnohé ale již mají integrovaný fotoaparát softwarově vybaven tak, že umí kód přečíst přímo.

A jak tedy mohou kyberlumpi QR kód zneužít, třeba ke krádeži peněz?

1. Přesměrování na škodlivé webové stránky - podvodníci například umístili falešné QR kódy na parkovací automaty a nasměrovali zákazníky na podvodnou platební bránu.
2. Stažení a spuštění škodlivého souboru - mnoho restaurací používá QR kód ke stažení jídelního lístku nebo ke stažení aplikace, přes kterou pak můžete přímo objednat jídlo a pití. Kyberlump tak může uživatele donutit stáhnout škodlivý PDF soubor nebo nainstalovat podvodnou aplikaci.
3. QR kód spustí v zařízení nějakou akci - například kód na připojení k Wi-Fi síti muže donutit zařízení připojit se ke kompromitované Wi-Fi nebo odeslat SMS či e-mail.
4. Podvodné QR kódy mohou nahradit legální kódy pro placení.
5. Krádež identity či citlivých údajů - některé aplikace (WhatsApp , Telegram...) používají QR kód k "ověření totožnosti uživatele". Pokud se chcete připojit v počítači přes webové rozhraní aplikace, musíte "se ověřit" naskenováním QR kódu zobrazeného na webové stránce aplikace v mobilu. Aplikace WhatsApp se již stala obětí útoku (QRLJacking) -

útočníci se vydávali za provozovatele aplikace a donutili uživatele načíst podvodný QR kód, čímž byli schopni velice jednoduše uživatelské účty kompromitovat. A je také potřeba zmínit, že ve formě QR kódu spousta uživatelů v mobilech nosí velice citlivé osobní údaje - například covidová aplikace Tečka obsahuje pro kyberlumpy hodně zajímavých informací.

Určitě je tedy dobré být při skenování QR kódu ve střehu a snažit se dodržet pár jednoduchých doporučení:

1. Před skenováním QR kódu na veřejném místě se přesvědčte, že s kódem nebylo manipulováno - například že nezakrývá jiný kód.
2. Neskenujte QR kódy v nevyžádaných či podezřelých zprávách, ani náhodně nalezené kódy.
3. Buďte opatrní při platebních transakcích - rozhodně neplaťte pomocí kódu, který nepochází z důvěryhodného či ověřeného zdroje. A i když půjde o důvěryhodný kód, před dokončením transakce se podívejte, zda souhlasí číslo cílového účtu, částka či variabilní symbol.
4. V obecné rovině lze říct, že při práci s QR kódy byste měli být stejně opatrní, jako při práci s e-maily - neznáte odesílatele? Pokud ne, kód neskenujte.
5. Pokud QR kód obsahuje webovou adresu, zkontrolujte, zda je legitimní.
6. Nesdílejte QR kódy obsahující citlivé údaje, například kódy používané pro přístup k aplikacím nebo kódy obsažené v různých dokumentech či zdravotních potvrzeních nebo receptech.
7. Pokud to čtečka QR kódu ve Vašem zařízení umí, zakažte automatické provádění akce při skenování kódu.

Soutěž

Vyhodnocení minulé soutěže:

Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a ze správných odpovědí byl vylosován pan E. P., kterému tímto gratulujeme k výhře softwaru ESET Internet Security pro 1 PC na rok zdarma.

Otázka zněla:

Co znamená pojem "Doomscrolling"?

Správná odpověď měla být:

Termínem doomscrolling nebo také doomsurfing se označuje nadměrné trávení času věnovaného vstřebáváním negativních zpráv. Sledování převážně negativních zpráv může mít v některých případech za následek škodlivé psychické reakce.

Více informací naleznete zde.

Nová otázka:

Co znamená pojem "Racketeering"?

Ze správných odpovědí vylosujeme výherce, který od nás získá AVG PC TuneUp pro 1 PC na rok zdarma.

Odpovědi pište do 20. 8. 2022 na e-mail amenit@amenit.cz.

Správnou odpověď a výherce uveřejníme v příštím čísle. Pokud se chcete co nejdříve dozvědět, zda jste vyhráli, staňte se našimi přáteli na Facebooku. Tam se informace o výherci objeví jako první.

Vtip pro dobrou náladu

"Mami, jestli přijde den,
kdy můj život bude závislý na přístrojích, nech mne jít, odpoj mne…"
"Zlato, určitě to chceš?"
"Co to děláš? Mami! Mami ne! Wifi neeee!"

Vydání IT Kompasu od 1. čísla naleznete zde.