

Čo potrebujete vedieť o Phishingu

Phishing je forma kybernetického útoku formou e-mailov, telefónnych hovorov alebo správ. Spravidla tieto útoky vykonáva aktér vydávajúci sa za niekoho iného, čo mu umožňuje ľahšie získať citlivé údaje, ako sú platobné údaje a heslá k osobným účtom.

Poznajme riziká

STRATA OSOBNÝCH ÚDAJOV

Ak sa mladý človek stal obeťou úspešného pokusu o phishing, hackeri môžu získať prístup k jeho osobným údajom za účelom vydierania. Niektorí hackeri môžu požiadať o výkupné, aby majitelia získali súbory späť, zatiaľ čo iní ich jednoducho môžu zničiť alebo dokonca zverejniť na darkwebe.

CIELENÝ PHISHING

Ak hacker dokáže oklamať dieťa pri prvom phishingovom útoku, je pravdepodobné, že sa k nim znova vráti. Môžu začať požadovať „neškodné“ informácie a potom prejsť na citlivé informácie, ako sú heslá a vstupné kódy. Mnoho útokov tohto typu sa začína tým, že útočník ponúkne pomoc obeti s bežným problémom, aby si k nemu vybudovala dostatočnú dôveru a vzťah a následne prešla k citlivým údajom.

SKRYTÉ PRÍSTUPY

Ak sa útočníkovi podarí úspešne vykonať phishing, v podstate si nachádza „cestu dovnútra“ alebo zadné vrátka do online priestoru obete. Aj keď si samotná osoba nemusí všimnúť žiadne zmeny vo svojom online priestore, hacker môže jej činnosť monitorovať a ovládať bez jej vedomia.

Užitočné rady pre zvýšenie bezpečnosti

ZÁLOHUJTE SVOJE DÁTA

Zálohujte Vaše súbory na externý disk alebo USB pred akýmkoľvek možným poškodením alebo zničením. Ak pravidelne robíte zálohy, možno budete musieť zálohovať iba súbory, ktoré boli nedávno pridané / aktualizované od poslednej zálohy.

ODPÁJAJTE ZARIADENIA

Ak sa domnievate, že dieťa bolo cieľom pokusu o phishing, najskôr zariadenie odpojte od siete vypnutím nastavení Wi-Fi alebo odpojením sieťového kábla. Prípadne vyhľadajte smerovač a odpojte ho. Toto zabráni malwaru v prístupe k akýmkoľvek internetovým službám.

SKENOVANIE SYSTÉMU

Odporúčame vykonávať pravidelné a komplexné kontroly softvéru. Tým skontrolujete všetky potenciálne škodlivé programy nainštalované vo Vašom počítači. Kontroly sú najúčinnnejšie, keď je antivírus aktualizovaný, aby vedel udržať krok s novými typmi malwarov.

KONTROLA WEBSTRÁNOK

Ak si nie ste istí dôveryhodnosťou správy, ktorú ste obdržali, neklikajte na žiadne odkazy ani nepostupujte podľa pokynov. Adresu uvedenú pri správe môžete jednoducho skontrolovať prostredníctvom webového prehliadača a uistiť sa, či ide teda o podvod alebo phishing.



Dávajte pozor na...

PODOZRLIVÉ URL ADRESY

Odkazy a prílohy v správach vás môžu presmerovať na úplne inú webovú stránku ako ste očakávali. Keď umiestnite kurzor myši na hypertextový odkaz, zobrazí sa skutočná webová stránka. Niektoré odkazy môžu byť však v skrátenej forme, takže skutočná adresa webovej stránky je skrytá za všeobecným odkazom, napríklad goo.gl/7fh28. Odporúčame nikdy nekliknúť na skrátené adresy URL.

NALIEHAVOSŤ SPRÁVY

Hackeri často pracujú pri phishingu s emóciou strachu, a teda prostredníctvom formuliek, ako napr. „kliknite kým nebude neskoro“ alebo „ide o život“ vytvárajú domnienku naliehavosti a neodkladnej povinnosti na tú správu reagovať. Odporúčame teda vždy pri takýchto správach spozornieť a nekonať hneď podľa požadovaných pokynov.

PRÍLIŠ DOBRÉ NA TO, ABY TO BOLA PRAVDA...

Ak dostanete e-mail s oznámením, že ste dostali „nový telefón“ alebo „pobyt v zahraničí“, pravdepodobne ide o e-mail s neoprávneným získavaním údajov.

Viac nájdete na

WWW.STALOSATO.SK
#STOPONLINEGROOMINGU
#ZALEZINATEBE
#DEJESATO
#POMOCEXISTUJE

Tento poster pre Vás vytvorili
psychológovia z IPčko.sk.
Inšpirované: nationalonlinesafety.com



STALOSATO.SK

