EGYRE TÖBB A KERESKEDELMET ÉRINTŐ HACKERTÁMADÁS. HOGYAN VÉDEKEZHETÜNK ELLENÜK?

A KIBERBŰNÖZŐK NEM KÍMÉLIK OKOSESZKÖZEINKET. MOST HOZTUNK NÉHÁNY TIPPET, HOGYAN VÉDEKEZHETÜNK HATÉKONYAN A KÁRTÉKONY AKCIÓK ELLEN.

Cím: 1054 Budapest, Bank utca 6. II. em. 9.
Telefonszám: +36 1 700 4460
E-mail cím: info@digicode.hu

DIGICODE
VONALKÓDTECHNIKA POS CÍMKE

Bemutatkozás

Rólunk

A DigiCode Kft. vonalkód technikai eszközök és segédprogramok fejlesztője. Székhelye Budapesten található, több mint 2000 darabos termékkínálatával a közép-európai országokat látja el. Mint egy vevő-centrikus cég, állandóan figyeljük vásárlóink igényeit és visszajelzéseit. Ez megteremti az ösztönzést és a lehetőséget, hogy folyamatosan tökéletesítgethessük rendszereinket és termékeinket, hogy a legjobb minőségű fogyasztói szoftvereket biztosíthassuk a piacon.

Céges küldetés

*"Fokozza számítógépes élményeit a munkában, az otthonában, és a szórakozásban."*Küldetésünk teljesítésének módja, hogy vásárlóink számára egyszerű, hatékony, és könnyen használható eszközöket biztosítsunk és szoftvereket tervezzünk, fejlesszünk.

Cégadatok

Adószám: 11885272-2-41
Eu adószám: HU11885272
Bankszámlaszám: 12025000-01167466-00100006
Cégjegyzékszám: 01-09-307420
Székhely: 1054 Budapest, Bank utca 6. II. em. 9.
Swift kód: UBRTHUHBXXX
Iban szám: HU18 1202 5000 0116 7466 0010 0006

Elérhetőségeink

Telefonszám: +36 1 700 4460
Központi e-mail cím: info@digicode.hu
Pénzügy és megrendelés: szamla@digicode.hu
Technikai segítség és szervíz: szerviz@digicode.hu
Iroda: 1054 Budapest, Bank utca 6. II. em. 9.

Szerzői jog

Online hivatkozások

A cég weboldala (https://www.digicode.hu/)
Szerződési feltételek (https://www.digicode.hu/altalanos-szerzodesi-feltetelek)
Jogi nyilatkozat (https://www.digicode.hu/jogi-nyilatkozat)
A dokumentum Online elérhetősége (https://www.digicode.hu/blog/egyre-tobb-a-kereskedelmet-erinto-hackertamadas-hogyan-vedekezhetunk-ellene-bp455)

EGYRE TÖBB A KERESKEDELMET ÉRINTŐ HACKERTÁMADÁS. HOGYAN VÉDEKEZHETÜNK ELLENÜK?

Míg korábban csak számítógépeinket kellett félteni a hackerektől, a mai digitális világban már minden olyan eszköz potenciális támadási célpont lehet, ami össze van kapcsolva az internettel. Nem jelentenek ez alól kivételt a vállalkozások mobileszközei sem.

Sőt, nagyobb fenyegetettségnek is vannak kitéve a kiberbűnözők kártékony tevékenységének, mint a magánemberek saját célokra használt készülékei. Szerencsére azonban a támadások ellen védekezni egyáltalán nem lehetetlen. Ehhez azonban nem csak felkészültségre, de odafigyelésre és a megfelelő eszközökre is szükségünk lesz.

Most mutatunk néhány dolgot, melyekre odafigyelve hatékonyabban védekezhetünk az okoseszközeinket érő, potenciális támadások ellen.

Megbízható eszközök

Mint ahogyan a biztonságos építkezés, úgy az online támadások elleni védekezés is az alapoknál kezdődik. És mint ahogyan jó minőségű építőanyagok nélkül nincs biztonságos építkezés és tartós munka, úgy megbízható munkaeszközök nélkül a hackerek ellen is nehezebb védekezni.

Az olcsó, tömeggyártott kütyük többsége sajnos egyáltalán nem való munkára. Nem csak gyenge hardveres és szoftveres kialakításuk, de gyenge biztonsági megoldásaik miatt sem. Ezek a szinte eldobhatónak nevezhető készülékek ugyanis az esetek többségében nem rendelkeznek olyan, alapvető konfigurációkkal, melyek aZebra, a Honeywell, vagy az egyéb, nagy gyártók eszközeit hatékonyabban teszik ellenállóvá a kibertámadásokkal szemben.

Arról már nem is beszélve, hogy szervizelésük az esetek többségében vagy túlságosan drága, vagy a szükséges alkatrészek hiányában időigényes, esetleg teljes mértékben megoldhatatlan.

Fizetett vírusirtó

Az Android operációs rendszerre rengeteg olyan applikáció elérhető, mely teljes védelmet ígér a digitális vírusok ellen, és látszólag nem kér ezért cserébe semmi. Az igazság azonban az, hogy a mai világban mindennek ára van, így az ingyenes vírusirtó programok vagy nem tudják garantálni a 100%-os védelmet, vagy csak bizonyos kedvezőtlen feltételek mellett képesek erre.

Az ilyen, korlátozott teljesítőképességű szoftverek sajnos rengeteg új kártevőt nem tudnak kiszűrni, vagy túlságosan

lelassíthatják eszközeink működését. Sőt, akár az is előfordulhat, hogy ők maguk is csak látványos köntösbe csomagolt, trójai faló módjára támadó, álcázott vírusok.

Ha szeretnénk azt, hogy eszközeink minden esetben biztonságban legyenek az online bűnözők kártékony tevékenységével szemben, használjunk olyan vírusirtó szoftvert, melynek definícós adatbázisa gyakran frissül, és a legújabb kártevők beazonosítására is képes. Ilyen lehet többek közt a sokak által használt Eset NOD 32, vagy épp a kifejezetten mobileszközökre tervezett Bitdefender.

Használatukkal lényegesen csökkenthetjük az adatlopás vagy a tönkretett eszközök esélyét és elkerülhetjük az egyéb, kellemetlen meglepetéseket.

Nagyobb odafigyelés

Még a legjobb vírusirtó sem garantálja viszont azt, hogy valahol nem csúszik hiba a számításba, és egy kolléga nem kattint véletlenül rá egy e-mailben kapott adathalász linkre, vagy történik hasonló, nem várt baleset. Éppen ezért fontos, hogy eszközeinket mindig a legnagyobb körültekintéssel használjuk.

Mielőtt munkába állítanánk a mobil számítógépeket, érdemes dolgozóinknak előadást tartani az adathalászat veszélyeiről és az online kártevőkkel szembeni, hatékony védekezésről. Fontos továbbá, hogy mindig gondolkodjunk az eszközök szoftveres karbantartásáról, és arról, hogy mind az operációs rendszer, mind a nap, mint nap használt applikációk napra készek legyenek és problémamentesen üzemeljenek.