Bitdefender

Itt van az ősz, itt van a home office: azaz vissza az iskolába

Itt van az ősz, itt van. Igen, újra.

Az iskolás korú gyermekek visszatértek az oktatás világába, ami ma már akár digitálisan is megvalósulhat. A szülők, a munkavállalók pedig gyakran élnek az otthoni munkavégzés lehetőségével. A koronavírus járvány miatt egyik napról a másikra jelentősen megnőtt az online szolgáltatások forgalma, azóta az emberek több időt töltenek az interneten, és nagyobb mértékben vannak jelen az online térben.

Ez a gyermekeket is fokozottan érinti, hiszen ők a korábbinál több időt töltenek már a világhálón, egyes esetekben akár felügyelet nélkül is. Az online eszközök lehetővé teszik számukra, hogy fizikai jelenlét nélkül is folytassák tanulmányaikat és kapcsolatban maradjanak társaikkal. Az online tevékenységek ily mértékű bővülésével viszont exponenciálisan nőtt a kibertámadások, csalások veszélye is, amelyek során nemcsak a digitális távoktatásban részesülő gyermekek, hanem az otthonról dolgozó munkavállalók is könnyen áldozattá válhatnak.

Mindezek elkerülése érdekében, a biztributor - a Bitdefender ajánlásai alapján - a biztonságos home office és az iskolakezdés apropóján egy kiadványt készített, melyben számos biztonsági tippel és ötlettel segíti az őszi iskolai szezon megkezdését.

Home office – okosan!

A mai világban egyre több munkáltató dönt úgy, hogy a munkavállalóknak az otthoni munkavégzésre (home office) is lehetőséget biztosít. Ez amennyire jó dolog, annyire veszélyes is tud lenni. Szóval javasolt szem előtt tartani, hogy ha otthonról dolgozik az ember, akkor azt okosan tegye! Ne okosba, okosan!

Az otthoni munkavégzés egy relatív új dolog és még most új szituációkba sodorhatja mind a munkáltatót, mind pedig a munkavállalót. A járvány kitörésekor ez még inkább így volt.

Az ilyen speciális helyzetek és az ilyenkor alkalmazott eljárások során az IT biztonsági szint csökkenhet, ezért kiemelten fontos a szervezetek és a munkavállalók tudatossági szintjének kimaxolása (már amennyire lehet). De ugyanennyire fontos (sőt!), hogy maga a munkavállaló is kiemelt figyelmet fordítson saját otthoni munkavégzése során a bevezetett biztonsági protokollokra.

A szervezeti környezetben megszokott IT biztonsági alapelvek megtartása a home office bevezetése után, otthoni környezetben is szükséges, így a **munkavállalónak javasolt különös figyelmet fordítania az alábbiakra.**

- A munkahelyi eszközöket (laptop, telefon, tablet stb.) kizárólag munkavégzésre használja!
- Nem, rajta online filmet nézni sem jó ötlet, de még a pénzügyeket intézni sem.
- Kölcsönadni a család valamely tagjának, akár csak játék céljából: szintén nem jó ötlet.
- Annál jobb ötlet viszont csak biztonságos weboldalakat felkeresni (a „https” a honlapcím elején pl. jó előjel lehet), és alaposan átgondolni, mielőtt bármire is kattintunk!

- Minden esetben érdemes ellenőrizni az URL címeket is, kimondottan az ismeretlen feladóktól kapott linkeket. A támadók gyakran használnak az eredetihez hasonló domaineket (például y0utube[.]com, faceb00k[.]com, officialpaypal[.]com.) ezért a honlap címek ellenőrzésén nem érdemes időt spórolni. Ezt a taktikát hívják homográf adathalászatnak, amikor lényegében csak egy-egy karakter tér el az eredeti és igazi linktől
- A munkavállaló ne kérjen rendszergazdai hozzáférést az számítógépére, ha mégis olyat kapott, akkor szóljon a rendszergazdának, informatikai biztonsági felelősnek, hogy szerinte az nem oké.
- Javasolt ellenőrizni, hogy az eszközökön van-e vírusírtó, sőt azt is, hogy megfelelően friss-e az adott verzió! Erre a legjobb megoldás egyértelműen a Bitdefender, hiszen az évek óta többszörös független tesztgyőzelem és a folyamatos K+F tevékenységnek köszönhetően kiemelkedik a vírusírtók közül, hiszen a Bitdefender nem csak egy szimpla vírusírtó! Innovatív technológiáinak és a világ egyik legnagyobb merítésű telemátriai adatbázisának köszönhetően – hiba nélkül - képes előre jelezni a készülékekre veszélyt jelentő káros kódokat.
- A munkavállaló e-mailek olvasása során legyen még körültekintőbb és óvatosabb!

Néhány jó tanács a cégeknek.

- Készítsenek üzletmenet-folytonossági tervet, amely figyelembe veszi a kiberbiztonsági kockázatokat és a technológiai követelményeket.
- Álljon rendelkezésre egy olyan intézkedési terv, ami tartalmaz kommunikációs és válságkommunikációs tervet is.
- A cégek gondoskodjanak a biztonságos hálózati hozzáférésekről, valamint az alkalmazottak munkavégzéshez szükséges eszközeiről. Most nem jó a hazai: mármint a munkavállalók ne használjanak privát eszközöket munkára.
- A szervezetek teremtsék meg a biztonságos kommunikáció lehetőségét VPN (Virtual Private Network) csatorna használatával, lehetőség szerint kétfaktoros azonosítással. A Bitdefender VPN ráadásul katonai szintű algoritmusokkal titkosítja a forgalmat, így az olvashatatlanná válik bárki számára, aki megtalálná a módját, hogy hozzáférjen a biztonságos alagúthoz és lehallgassa azt.
- Előre határozzák meg az elérni kívánt szakrendszerek körét, és a tűzfalakon kizárólag ahhoz biztosítsanak hozzáférést.
- A tűzfalszabályokat úgy kell kialakítani, hogy kizárólag a munkavégzéshez szükséges felületek legyenek elérhetőek.
- Oktatás! Minden esetben tartsanak oktatást a munkavállalóknak.
- Használják fel a Biztributor Kft. által biztosított kedvezményes vírusvédelmi (ideértve végpontvédelmet és a VPN szolgálatatásokat is) szoftver beszerzési lehetőségeket!

Vissza az iskolába – online biztonságban!

Az online szokások drámaian megváltoztak az elmúlt években, és nem csak a felnőttek töltenek több időt az interneten. A világjárvány kitörése óta a gyerekek képernyőidő-korlátozása felborult, mivel az iskolai tanórák, korrepetálások, játékok és szórakozás céljából az online platformok felé fordultak. Ez a megnövekedett digitális idő hozzájárult ahhoz, hogy új kiberfenyegetések szülessenek, amelyek tovább növelik az online veszélyek tárházt.

Miközben a gyerekek minden korosztálya felkészült a tanterembe való visszatérésre, vagy éppen az újabb olyan időszakra, amikor esetleg visszatér a digitális távoktatás, a kiberbűnözők mindenféle trükkökkel igyekeznek kihasználni ezt a zsúfolt időszakot, és célkeresztjükben a szülők, a diákok és a tanárok egyaránt benne vannak. Soha sem szabad abba a hamis biztonságérzetbe kergetni saját magunkat, hogy mi biztos, hogy senkinek sem vagyunk érdekesek, mivel gyakorlatilag mindannyian célpontjai lehetünk egy-egy hackernek, aki amellett, hogy személyes és pénzügyi jólétünket károsíthatják, egy veszélyeztetett, megfertőzött eszközzel az iskolai hálózatokhoz is hozzáférhetnek.

Tehát akár otthonról dolgozik valaki, akár irodai munkakörnyezetben van, elengedhetetlen, hogy mindenki megtanítsa arra gyermekét, hogy miképp lehet az online fenyegetések ellen védekezni, és minden esetben szükséges felhívni a gyermekek figyelmét is a helyes kibergyakorlatok fontosságára.

A gyerekek és tanárok akár fizikailag térnek vissza az iskolákba, akár otthonról folytatják a távoktatást, az iskolába való biztonságos visszatérés érdekében elengedhetetlen, hogy mindannyian – sőt a szülők is - felfrissítsék a legjobb online gyakorlatokat. Megéri a ráfordított időt, ezt garantáljuk.

Nézzünk is néhány kulcsfontosságú kiberbiztonsági tippet az idei iskolakezdéshez:

- Az iskolakezdés elején kiemelten legyenek résen az online tanszervásárlásokhoz kötődő csalásokkal és egyéb, iskolai célú adathalász kísérletekkel szemben. Legyen mindig szem előtt, hogy ami túl szép ahhoz, hogy igaz legyen, az általában nem az!
- Csak megbízható weboldalakon vásároljon, és javasolt a VPN használata.
- A szülők vizsgáljanak meg minden olyan iskolával kapcsolatos alkalmazást, amelyet gyermekük telepíteni szeretne a készülékekre. A programok letöltése előtt javasolt átnézni azok értékeléseit, adatvédelmi irányelveit, illetve az appokról szóló szakmai cikkeket.
- Javasolt a gyermekekkel a kiberbiztonsági higiéniáról beszélgetni, kiemelten a megfelelő jelszóválasztásról. A szülők győződjenek meg róla, hogy a gyermek eszközei és iskolai fiókjai erős, egyedi jelszavakkal vannak beállítva. Az egyszerű jelszókezelés megkönnyítése érdekében megfontolandó egy biztonságos jelszókezelő használata.
- A szülők és gyermekek akár együtt is naprakészen tarthatják rendszereiket és böngészőiket: a közös edukáció jó ötlet. Mindezek mellett fontos megtanítani a gyermekeknek, hogy soha semmilyen körülmény között ne adják ki személyes adataikat idegeneknek.

- A gyermekek által használt eszközökön, alkalmazásokon és meglátogatott weboldalakon indokoltak lehetnek a szigorú adatvédelmi beállítások.
- A szülők kellő körültekintéssel válasszák meg azon online játékok körét, melyekkel a gyermekek játszhatnak, hiszen az elmúlt két évben közel 50%-kal nőtt a videójátékokhoz kapcsolódó támadások száma világszerte.
- Javasolt egy biztonsági megoldás használata az eszközökön, amely azt is megakadályozza, hogy bárki akaratlanul is rosszindulatú programokat telepítsen fel rájuk. Egy ilyen szoftver abban is segít, hogy senki se essen áldozatul egy-egy káros linkhez kapcsolódó adathalász kampánynak. A Bitdefender szülői felügyeleti funkciókkal is rendelkezik, amelyek segíthetnek szabályozni a gyermekek online tevékenységét, így könnyebben lehet őket megvédeni az online veszélyektől.
- Az iskolaidőszak több videokonferenciát és webkamera használatot is jelenthet, ezért indokolt lehet meggyőződni arról, hogy biztonsági megoldásai nyújtanak-e webkamera- és mikrofonvédelmet. A Bitdefender beépített kamera- és mikrofonvédelme nagyon komoly védelmi vonalat biztosít a személyes
- Legvégül, de nem utolsó sorban, fontos annak hangsúlyozása, hogy a gyermekek nyíltan kommunikálhatnak a szülőkkel, és jelezzenek minden gyanús tevékenységet, amit az online térben észlelnek. Az áldozattá válás sohasem szégyen.

A fentieken túl a Bitdefender figyeli és blokkolja az adathalász e-mailek mellett a káros weboldalak linkjét, az SMS-ben érkező gyanús üzeneteket, sőt a közösségi média felületét használó támadásokat is. Emellett segíti a biztonságos bankolást, hogy a kártyaadatok se jussanak illetéktelen kezekbe.

A biztributor vezető IT-biztonsági, hálózati és üzemeltetés-támogató disztribútor cég. Az általa képviselt gyártók közé tartozik többek között az APT-támadások elleni védelem szakértője, a **Trellix**, a kiberhírszerzés etalonja, a **Mandiant**, a vezetékes és Wi-Fi hálózatokban jeleskedő **Ruckus**, a sokszoros végpontvédelmi tesztgyőztes **Bitdefender**, valamint a kis- és középvállalati biztonságban stabil pontnak tekintett **GFI**.