

OUCH!

Az Ön Havi Biztonsági Tudatosságról Szóló hírlevele

Az okostelefon: aranybánya a kiberbűnözőknek

Egy zsebméretű katasztrófa

Emma az egy hetes nyaralását élvezte egy gyönyörű, napsütötte szigeten. Egyik délután, miután több órát töltött a strandon, megállt egy kis kávézóban ebédelni, mielőtt visszaindult volna a szállásához. A tengeri kilátás annyira lekötötte, és már annyira vágyott vissza a szabadba, hogy távozáskor véletlenül az asztalon hagyta az okostelefonját. Csak órákkal később vette észre, hogy eltűnt a telefonja.

Emma eleinte nem aggódott különösebben. Visszasétált a kávézóhoz, hogy megkeresse, de már nyoma sem volt. Bárki találta is meg a telefont, lehetősége nyílt hozzáférni Emma személyes e-mail-fiókjához, közösségimédia-fiókjaihoz, banki alkalmazásaihoz, sőt még ahhoz a hitelesítő alkalmazáshoz is, amelyet a személyazonossága igazolására használt, amikor fontos weboldalakra jelentkezett be.

Ráadásul, mivel éppen utazott, Emma a telefonjára támaszkodott a térképek, a szállodai foglalások és a repülőjáratokkal kapcsolatos információk eléréséhez, valamint a családjával való kapcsolattartáshoz. Többé nem fért hozzá a beszállókártyáihoz, nem tudta megerősíteni az utazási terveit, és a készülékére küldött biztonsági kódokat sem tudta fogadni.

Szerencsére Emma még az utazása előtt képernyőzárat állított be, és a távoli helymeghatározást is bekapcsolta. A szállodai szobájába visszatérve a laptopjáról bejelentkezett a fiókjába, és látta, hogy a készülék már nincs a kávézóban. Amikor világossá vált számára, hogy nem fogja visszakapni, távolról zárolta azt, és az adatai védelme érdekében törölte teljes tartalmát. Szerencsére gyorsan helyre tudta állítani az adatait is, mivel biztonsági másolatot készített róluk.

Öt lépés mobileszközünk biztonságának megőrzéséhez

1. Állítsunk be erős képernyőzárat

Az első védelmi vonalunk annak megakadályozása, hogy illetéktelenek hozzáférjenek a készülékünkhöz. Használjunk PIN-kódot, jelkódot, ujjlenyomatot vagy arcfelismerést telefonunk vagy táblagépünk zárolásához. Ha készülékünk elveszik vagy ellopják, egy erős képernyőzár megakadályozhatja, hogy valaki azonnal hozzáférjen alkalmazásainkhoz, fiókjainkhoz és személyes adatainkhoz. Gondoljunk a képernyőzárúra úgy, mintha digitális otthonunk bejárati ajtaja volna. Állítsuk be készülékünket úgy, hogy tétlenség esetén a számunkra még kényelmes lehető legrövidebb idő elteltével automatikusan zárolja magát. Tegyük szokásunkká, hogy amikor letesszük a telefonunkat, le is zárjuk.

2. Kapcsoljuk be a készülék helymeghatározását és a távoli adattörlést

Mi történik, ha készülékünk elveszik vagy ellopják? A legtöbb modern mobileszköz beépített szolgáltatásokat kínál, amelyek segítségével megkereshetjük készülékünket a térképen, megcsörgethetjük, távolról zárolhatjuk,

vagy törölhetjük róla az összes adatot, ha nincs lehetőség a visszaszerzésére.

Az Apple-felhasználók bekapcsolhatják a „Find My” funkciót. Az Android-felhasználók pedig a „Find My Device” funkciót. Ezek a szolgáltatások ingyenesek, és gyakran már eleve rendelkezésre állnak a készülékünkön. Ha szánunk néhány percet annak ellenőrzésére, hogy ezek a funkciók be vannak-e kapcsolva, később rengeteg stressztől kímélhetjük meg magunkat. Ha készülékünk eltűnik, gyorsan megkereshetjük, vagy távolról törölhetjük róla az adatainkat, mielőtt valaki más hozzáférne azokhoz.

3. Kapcsoljuk be az automatikus frissítéseket

A kiberbűnözők folyamatosan keresik a mobileszközök operációs rendszereinek és alkalmazásainak sebezhetőségeit. Amikor felfedezik ezeket a sebezhetőségeket, a szoftvergyártó vállalatok frissítéseket adnak ki, hogy javítsák őket. A probléma az, hogy sokan napokkal, hetekkel vagy akár hónapokkal is elhalasztják a frissítések telepítését. A legegyszerűbb megoldás, ha bekapcsoljuk az automatikus frissítéseket, beleértve a mobilalkalmazásaink automatikus frissítését is. Ez biztosítja, hogy készülékünk azonnal megkapja a biztonsági javításokat, amint azok elérhetővé válnak, gyakran anélkül, hogy bármit is tennünk kellene.

4. Csak megbízható forrásokból telepítsünk alkalmazásokat

A mobileszközök biztonságát leggyakrabban a rosszindulatú alkalmazások veszélyeztetik. Kizárólag hivatalos alkalmazásáruházakból töltsünk le mobilalkalmazásokat, például az Apple App Store-ból vagy a Google Play-ről. Még ebben az esetben is ellenőrizzük telepítés előtt az értékeléseket, a hozzászólásokat és az alkalmazás által kért engedélyeket. Legyünk különösen óvatosak azokkal az alkalmazásokkal, amelyek olyan adatokhoz vagy funkciókhoz kérnek hozzáférést, amelyekre nincs szükségük. Például egy zseblámpa-alkalmazásnak nem kellene hozzáférést kérnie a névjegyeinkhez, a mikrofonunkhoz vagy a helyadatainkhoz. Ha egy alkalmazás gyanúsnak tűnik, vagy indokolatlanul sok engedélyt kér, válasszunk helyette másikat.

5. Kapcsoljuk be az automatikus biztonsági mentéseket

Egy készülék elvesztése igencsak stresszes lehet. Ha telefonunk eltűnik, megsérül vagy tönkremegy, egy friss biztonsági mentésnek köszönhetően percek alatt mindent visszaállíthatunk egy új készüléken, beleértve a korábban telepített alkalmazásokat, és még azok beállításait is. Győződjünk meg arról, hogy az automatikus biztonsági mentések be vannak kapcsolva.

Vendég szerkesztő

Dr. Khushi Gupta a University of North Georgia kiberbiztonsági tanszékének adjunktusa. Kiberbűnügyi kriminalisztikából szerzett Ph.D.-fokozatot, több mint 30 publikáció szerzője, munkája során pedig a bűnüldözés területén szerzett kriminalisztikai tapasztalataira is épít. Mentorként tevékenykedik a WiCyS, a Women4Cyber és a BBWIC programjaiban.



Források

A letöltések veszélye: hogyan járn túl a rosszindulatú mobilalkalmazások eszén: <https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps>

SMS-támadások: Egy smishing történet: <https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga>

A Misztikum Feloldása: Hogyan lopják el a jelszavakat a kiberbűnözők? <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords>

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)

OUCH! A SANS Security Awareness által közzétett és a Creative Commons BY-NC-ND 4.0 licence alatt terjesztett kiadvány. Ezt a hírlevelet szabadon megoszthatja vagy terjesztheti egészen addig, amíg nem adja el vagy nem módosítja. Szerkesztőbizottság: Phil Hoffman, Leslie Ridout, Princess Young.

Többet találhat az Ouch!-ból A következő linken: <https://www.sans.org/newsletters/ouch>