Kizárva: Mi történik a digitális életeddel a halál után

Kizárva egy virtuális ajtón, a lehető legrosszabb pillanatban?

Amikor Carlos váratlanul elhunyt, családját elárasztotta a gyász és a zavarodottság. Felesége tudta, hogy be kell fizetnie a számlákat, be kell nyújtania a biztosítási igényeket, és értesítenie kell a családtagokat. Carlos azonban mindent egyedül, online intézett.

Az e-mail fiókját olyan jelszó védte, amelyet senki sem ismert. A telefonja feloldásához PIN-kódra volt szükség. Bankszámlái, befektetési és közüzemi fiókjai mind olyan bejelentkezési adatokat igényeltek, amelyeket korábban kizárólag ő használt. A bankoktól és biztosítóktól érkező fontos üzenetek az e-mail-fiókjában rekedtek. Az automatikus fizetések meghiúsultak. Az előfizetések továbbra is terhelték a számláját. Közösségi média fiókjai továbbra is születésnapi emlékeztetőket küldtek, felidézve fájdalmas hiányát. Családja hónapokat töltött azzal, hogy kapcsolatba lépjen a különböző szolgáltatókkal, halotti anyakönyvi kivonatokat juttasson el számukra, és eligazodjon a zavaros ügyfélszolgálati folyamatok között. Gyakran azt a választ kapták: „Nem tudunk segíteni a fiókhoz való hozzáférés nélkül.” Carlos számos dolgot felelősségteljesen megtervezett az életében — ám digitális létére ez nem terjedt ki.

Miért fontos a digitális örökség?

Napjainkban életünk jelentős része az online térben zajlik. A pénzügyi számlák, nyugdíjalapok, online fizetési szolgáltatások, sőt még a hűségpontok is gyakran kizárólag digitális formában léteznek. Fényképeink, dokumentumaink és személyes emlékeink gyakran nem kerülnek nyomtatásra vagy offline tárolásra. Az okoseszközök vezérlik otthonunkban a világítást, a zárakat és a közüzemi szolgáltatásokat. Amikor valaki digitális öröklési terv nélkül hal meg, a családok valós károkat szenvedhetnek el:

- **Pénzügyi fennakadások**, amikor nem tudnak hozzáférni a pénzeszközökhöz vagy kezelni a folyamatban lévő kötelezettségeket.
- **Érzelmi megterhelés** a rendezetlen online fiókok vagy a személyazonossággal való visszaélés kockázata miatt.
- **Biztonsági kockázatok**, ha a fiókok aktívak maradnak és ezáltal illetéktelen személyek kezébe kerülnek.
- **Elveszett vagyonelemek**, beleértve a digitális pénztárcákat, a kizárólag online létező befektetéseket vagy fontos dokumentumokat.

A digitális öröklés nem a magánélet feladásáról szól. Arról szól, hogy biztosítsuk a folytonosságot, a védelmet és a gondoskodást azok számára, akik itt maradtak.

1. Készítsünk leltárt digitális életünkről

A digitális öröklési terv elkészítésének első lépése annak átlátása, mivel rendelkezünk. A legtöbben meglepődnének azon, hogy az életük milyen nagy része zajlik online. Kezdjük azzal, hogy átgondoljuk mik a legfontosabb fiókjaink: például a banki és befektetési számláink, a felhő- és fotótároló szolgáltatásokhoz kapcsolódó fiókjaink, az egészségügyi adatainkat nyilvántartó felhasználóink, a közösségi média-, valamint az okosotthon-rendszereket irányító profiljaink. Az e-mail különös figyelmet érdemel, mivel gyakran ezt használjuk számos más fiók jelszavának visszaállítására. Nincs szükség teljeskörű listára. Összpontosítsunk azokra a felhasználókra, amelyek problémát okoznának, ha senki se férne hozzájuk. Ez a jegyzék szolgáljon alapul minden további lépéshez.

2. Használjunk jelszószéfet!

A halálesetet követően a családok egyik legnagyobb adminisztratív kihívása az, hogy nem ismerik az elhunyt jelszavait. Ezt a problémát egy jelszószéf biztonságos és megbízható módon orvosolja. Az összes felhasználónevet és jelszót titkosított digitális tárolóban őrzi, amelyet egyetlen erős mesterjelszó véd. Számos jelszókezelő rendelkezik vészhelyzeti vagy örökösi hozzáférési funkcióval is, amely lehetővé teszi, hogy kijelöljünk egy megbízható személyt, aki hozzáférést kap, ha velünk történne valami. A legtöbb ember számára a jelszókezelő a digitális örökség kezelésének leghatékonyabb eszköze. Ha a jelszókezelő valamiért nem opció, akkor a fontos fiókok és jelszavak adatait tartsuk egy biztonságos jegyzetfüzetben, amelyet zárt iratszekrényben vagy más biztonságos helyen őrzünk.

3. Jelöljünk ki egy megbízható digitális kapcsolattartót

Határozzuk meg, kire bízzuk digitális életünk kezelését arra az esetre, ha mi magunk erre már nem lennénk képesek. Ez lehet házastárs, élettárs, nagykorú gyermek, közeli családtag vagy végrendeleti végrehajtó. Alaposan gondoljuk át ezt a döntést! Ez a személy érzékeny pénzügyi, személyes és érzelmi információkhoz férhet hozzá. Ugyanilyen fontos, hogy tájékoztassuk őt a döntésünkről, és ismertessük vele a szerepét. Tájékoztassuk arról, hol található a jelszószéfünk mesterjelszava, valamint arról is, mit várunk tőle: például számlák rendezését, fiókok megszüntetését, vagy fényképek és emlékek megőrzését.

4. Kapcsoljuk be a beépített örökösi és inaktív fiók-funkciókat!

Számos online szolgáltatás kínál kifejezetten digitális öröklésre tervezett, beépített megoldásokat. Ezek a funkciók lehetővé teszik, hogy kijelöljünk valakit a fiók kezelésére, meghatározott inaktivitási időszak után hozzáférést biztosítsunk számára, vagy halálunk esetén kérjük a fiók törlését. Ezen lehetőségek kihasználása csökkenti a családra nehezedő terheket, és mérsékli a hosszas ügyfélszolgálati egyeztetések vagy jogi ügyintézés szükségességét. Az ilyen funkciók aktiválása - ahol erre lehetőség van - további védelmi réteget jelentenek, és segítenek biztosítani, hogy kívánságaink érvényesüljenek. Ha életünkben meghatározó változások történnek, mindenképpen frissítsük ezeket az adatokat.

Egy utolsó gondolat

A digitális öröklési terv elkészítése megóvja családunkat a felesleges stressztől, megelőzi a pénzügyi fennakadásokat, és biztosítja, hogy online életünk a kívánságainknak megfelelően kerüljön rendezésre. Nem szükséges mindent azonnal megoldanunk, ám a témáról való beszélgetés elindítása és néhány egyszerű lépés megtétele később sok kellemetlenségtől és frusztrációtól kímélheti meg szeretteinket.

Vendégszerkesztő

Cynthia Taylor több mint egy évtizedes IT-tapasztalattal rendelkezik, közel harminc tanúsítványt szerzett, és kiberbiztonsági MsC diplomával bír. Jelenleg alkalmazásbiztonsági területen dolgozik. Cynthia elkötelezett amellett, hogy növelje a kiberbiztonság hozzáférhetőségét az egyetemes és a biztonságos tervezés közötti szakadék áthidalásával.

Források

A jelszókezelők ereje: https://www.sans.org/newsletters/ouch/power-password-managers/
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 Jelmondatok Ereje: https://www.sans.org/newsletters/ouch/power-passphrase/

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

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