De maandelijkse Security Awareness nieuwsbrief voor jou!

Digitale erfenis

Overzicht

Heb je ooit nagedacht over de lastige vraag: "Wat gebeurt er met onze digitale aanwezigheid als we sterven of wilsonbekwaam worden? Velen van ons weten dat we een testament en checklists moeten hebben van wat geliefden moeten weten in het geval van ons overlijden. Maar hoe zit het met al onze digitale gegevens en online accounts? Zouden we een soort digitaal testament moeten overwegen? Zouden we een digitaal erfplan moeten creëren?

Denk na over je digitale aanwezigheid. Bank- en pensioenrekeningen, woninghypotheken, familiefoto's en -video's, inloggegevens voor slimme thuistoepassingen, e-mail en sociale media zijn slechts enkele van de vele voorbeelden die onze digitale voetafdruk vormen. In het geval van overlijden of het overlijden van een naast familielid, familie en geliefden kan het nodig zijn om snel toegang te krijgen tot deze rekeningen of gegevens. Bovendien kunnen achtergelaten historische gegevens en online accounts na verloop van tijd kwetsbaar worden voor hackers, waardoor familie en vrienden in gevaar komen.

Een plan maken

Het is een goed idee om jouw wensen te bespreken met je familie of vrienden die je vertrouwt, net als andere details van het einde van het leven. Naast het bespreken hiervan is het belangrijk een inventarisatie te maken en digitale middelen en online accounts te documenteren. Als je vooraf geen toegang tot je accounts regelt in geval van overlijden, kan het bijzonder lastig zijn voor familieleden om toegang te krijgen en ze te sluiten. Zou je bijvoorbeeld willen dat je familie geen toegang meer heeft tot al die jaren aan familiefoto's en - video's die online zijn opgeslagen?

Je online accounts in een wachtwoord manager opslaan is en goede optie. Dit is een programma dat al jouw inloggegevens en wachtwoorden, creditcards en andere gevoelige informatie veilig opslaat. Het is ontworpen om het maken, opslaan en openen van wachtwoorden en veiligheidsvragen veel eenvoudiger te maken. Het is in vele opzichten een zeer krachtige tool om digitale accounts te catalogiseren. Veel wachtwoord managers bieden de mogelijkheid alle, of bepaalde, wachtwoorden te delen met andere vertrouwde familieleden. Als je je daar niet prettig bij voelt, documenteer dan de toegang tot je wachtwoord manager

en verzegel dat in een enveloppe; laat die verzegelde enveloppe openen na je overlijden door een executeur of een vertrouwd familielid. Zo hebben ze toegang tot jouw wachtwoord manager en tot jouw accounts en de informatie die daar is opgeslagen.

Daarnaast bieden sommige sites de mogelijkheid om erfgenamen of vertrouwde contacten te identificeren. Met Facebook kunnen deelnemers bijvoorbeeld vooraf bepalen of ze hun account willen laten verwijderen of herdenken na het overlijden. Met Memorializing wordt een ruimte gecreëerd die alleen zichtbaar is voor bestaande vrienden, waar herinneringen kunnen worden gedeeld. Tot slot kun je overwegen om een advocaat of notaris in de arm te nemen die gespecialiseerd is in digitale erfenis.

Erven van digitale goederen

Het kan zijn dat je je in de situatie bevindt waarin je toegang moet krijgen tot de online accounts van een recent overleden vriend of familielid. Wij raden aan om eerst te overleggen met een advocaat en andere familieleden voordat je actie onderneemt. Andere familieleden kunnen snel van streek raken als ze zien dat je actie onderneemt zonder eerst met hen te overleggen. Begin dan met het identificeren van eventuele wachtwoorden die je kunt vinden. Heeft het familielid ze opgeschreven of ergens opgeborgen? Als dat geen optie is, kun je dan toegang krijgen tot andere computers of mobiele apparaten die ze hebben gebruikt en waar ze nog steeds op zijn ingelogd? Zo niet, dan moet je waarschijnlijk naar elke site gaan om toegang te krijgen tot het account van het overleden lid. Dit houdt vaak in dat je zowel een overlijdensakte moet overleggen als een bewijs dat je direct gerelateerd bent aan het familielid. In sommige gevallen krijg je geen toegang tot het account of de gegevens die in het account zijn opgeslagen, maar verwijder je deze alleen maar. Elke site gaat anders om met deze situaties, wat een tijdrovend proces kan zijn.

In de huidige digitale wereld moeten we niet alleen rekening houden met fysieke goederen, maar ook met digitale goederen.

Gastredacteur

Cheryl Conley *is een expert op het gebied van phishing en bewustwording. Hij heeft onder andere ervaring met het bouwen en beheren van het phishingprogramma bij Lockheed Martin. Ze ondersteunt nu het SANS Security Awareness team en is in het bezit van de SSAP (SANS Security Awareness Professional) certificering.*

Bronnen

Wachtwoord managers: http://www.sans.org/u/Y5Y

Wachtwoorden eenvoudig gemaakt: http://www.sans.org/u/Y63

OUCH! wordt gepubliceerd door SANS Security Awareness en wordt gedistribueerd onder de Creative Commons BY-NC-ND 4.0 licentie. *Het staat u vrij om deze nieuwsbrief te delen of te distribueren zolang u hem niet verkoopt of wijzigt. Redactionele Raad: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley. Vertaald door: Tamara Brandt*