Laat geen digitale **puinhoop** achter

Illustratie XF&M

Digitale erfenis
Is er, als je plotseling komt te overlijden, iemand die je wachtwoorden kent? Je bankzaken? Digitale administratie is vaak een blinde vlek. En dat is lastig voor nabestaanden.

Door **Anna Vossers**

Verzekeringen, beleggingsrekeningen, bitcointegoeden, steeds meer geldzaken bewaren mensen alleen digitaal. Groot kunnen de problemen zijn als iemand met zo'n digitale administratie overlijdt en niemand erbij kan.

Mensen denken liever dat ze onsterfelijk zijn, zegt Nora van Oostrom van de Koninklijke Notariële Beroepsorganisatie. „Daarom schuiven ze het regelen van praktische zaken voor zich uit. En telefoon en laptop zijn meestal beveiligd met een wachtwoord, dus daar kan lang niet altijd iemand in."

Stel, je krijgt een fataal ongeluk op reis, en alleen jij wist waar je een reisverzekering had afgesloten. In het ergste geval moeten familieleden verzekeraar na verzekeraar opbellen om erachter te komen wie de repatriëring, die kan oplopen tot enkele duizenden euro's, vergoedt. „Verzekeraars hebben daarvoor niks centraal geregeld", zegt Suzan Bloemscheer van vergelijkingssite Independer.

Bij bankzaken gelden andere problemen. „Er zijn zoveel banken en instanties waar je geld of schulden kunt hebben, dat levert nabestaanden een hoop zoekwerk op", zegt Van Oostrom. „En binnen acht maanden na het overlijden moeten ze wel aangifte hebben gedaan van de nalatenschap bij de Belastingdienst." Sommige tegoeden zijn überhaupt nauwelijks terug te vinden: de anonieme bitcoin, bijvoorbeeld, of tegoeden die fanatieke gamers kunnen hebben in een spel. Je moet dan maar net weten onder welk pseudoniem die staan aangemeld.

Die niet-digitale kluis vergeten we ook

Ook in de niet-digitale administratie zijn er veel dingen die vaak worden vergeten, zegt Marleen Verspoor, specialist in nalatenschappen. Heb je spullen uitgeleend of in bruikleen, heb je een onderhandse lening uitstaan? Leg dat vast en maak duidelijk waar de betreffende papieren te vinden zijn.

Heb je een kluis buitenshuis? Zorg dat de locatie bekend is. Verspoor: „Soms wordt er een kluissleutel gevonden, maar is de plek van de kluis onbekend en wordt deze nooit gevonden."

Minderheid schrijft wachtwoorden op

90%
Uit onderzoek van uitvaartverzekeraar Nuvema blijkt dat 9 op 10 ondervraagden niets heeft geregeld voor zijn digitale nalatenschap. 1 op de 20 heeft zijn wachtwoorden opgeschreven.

33%
Eenderde van de respondenten wil desondanks het liefst zoveel mogelijk van de digitale nalatenschap zelf regelen. De helft wil dat socialemedia-accounts geheel worden verwijderd.

Vijf manieren om te voorkomen dat je een digitale puinhoop achterlaat.

1 Verzamel de belangrijkste gegevens
Maak een e-mail of een bestandje in bijvoorbeeld Google Docs of Dropbox met daarin de belangrijkste gegevens die met een nodig zijn als jou wat overkomt. Waar je een reis- of uitvaartverzekering hebt afgesloten, bijvoorbeeld. Een papieren lijst kan natuurlijk ook. Vertel een familielid of vertrouwenspersoon in alle gevallen waar dat document te vinden is.

2 Zorg voor toegankelijk adresboek
Bedenk of je adresboek toegankelijk is, zodat de juiste mensen kunnen worden uitgenodigd voor de uitvaart. „Zeker bij alleenstaanden of mensen die plotseling overlijden is dat lastig", zegt Marleen Verspoor, die zich met haar bedrijf Via Verspoor heeft gespecialiseerd in nalatenschappen. „Als de familie de computer of telefoon niet kan openen, kan het gebeuren dat belangrijke mensen te laat worden geïnformeerd."

3 Maak een digitaal pakket
Maak voor je executeur of familielid een lijst van andere belangrijke toegangscodes, zoals voor bankrekeningen en betaaldiensten. Denk goed na hoe je zo'n document deelt: je bent kwetsbaar voor identiteitsfraude als je persoonlijke gegevens niet veilig verstuurt. Veiliger en makkelijker is het om wachtwoorden op te slaan in een wachtwoordmanager. Het moederwachtwoord daarvan is de enige toegangscode die je deelt (zie: digitale kluis).

Al wat veiliger dan e-mailen is een digitaal pakketje dat je op slot zet met een veilig wachtwoord. Dat kan met onder meer WinZip. Verstuur het wachtwoord en het document nooit via hetzelfde medium. Sms bijvoorbeeld de code.

Nog veiliger én ingewikkelder is encryptie. De gegevens zijn alleen te ontcijferen met de persoonlijke sleutel van de ontvanger. Je moet dan beiden hetzelfde encryptieprogramma installeren. Gratis en relatief makkelijk te begrijpen opties zijn Peerio en Cloudfogger - of zoek online goede opties in de Internetvrijheid-Toolbox van privacyplatform Bits Of Freedom.

4 Open een digitale kluis
Klinkt dat te ingewikkeld? Er zijn - betaalde - digitale kluizen. Die kun je gebruiken voor bijvoorbeeld het moederwachtwoord van je wachtwoordmanager. Veilige opties zijn Gardid (4 euro per maand) of Erfkluis (15 euro per jaar). Ook de ANWB biedt een kluis voor de opslag van pas(poort)gegevens. Sommige kluizen, zoals Digizeker (10 euro per maand), staan in het testamentenregister. Bij overlijden krijgen aangewezen nabestaanden toegang bij de notaris.

5 Regel je digitale nalatenschap
Aan wie je geld en huis nalaat, leg je vast in een testament. Erfgenamen van je huisraad of sieraden wijs je aan in een handgeschreven codicil. Ook voor je digitale nalatenschap kun je al van alles regelen. Zoals inactiviteitsvoorkeuren instellen bij Gmail en Facebook. Zo bepaal je wat er met je account gebeurt. Death-Switch is een gratis dienst die om de zoveel tijd een bevestiging vraagt of je nog leeft, en bij een uitblijvende reactie een door jou aangewezen persoon een e-mail stuurt met bijvoorbeeld aanwijzingen over je Twitter-account.