Det månedlige nyhetsbrevet om sikkerhetsbevissthet for deg

Digital arv

Oversikt

Har du noensinne tenkt over hva som skjer med vår digitale tilstedeværelse når vi dør, eller hvis vi blir uføre? Mange har, eller vet at de burde ha et testament og en slags sjekkliste over hva pårørende burde vite dersom man går bort. Men hva med all vår digitale informasjon, og brukerkontoer på nett? Burde vi ha en form for digitalt testament? Burde vi lage en plan for «digital arv»?

Tenk over din tilstedeværelse på nett. Bankkonti, boliglån, bilder av familien, brukere for «smarte» ting, e-post, og sosiale medier. Dette er bare noen av mange eksempler på det som utgjør ditt digitale fotavtrykk. Dersom du går bort kan dine nærmeste ha behov for tilgang på dine brukerkontoer og data. I tillegg burde du tenke over at gamle brukerkontoer over tid kan bli sårbare, og at hackere kan utgjøre en trussel for din familie og dine venner gjennom disse.

Lag en plan

Akkurat som andre ting som omhandler livets slutt, er det en god idé å diskutere dette med familien og nære venner, så de blir innforstått med dine tanker og ønsker. I tillegg til disse samtalene, skaff deg en oversikt over dine digitale eiendeler og brukerkontoer. Dersom du ikke har en plan for hvordan pårørende skal få tilgang til disse etter din død, kan det bli veldig vanskelig for dem å komme inn på noe. For eksempel, dersom du har mange familiebilder lagret i skyen, hadde det vært dumt om familien din mistet all tilgang til dem.

Dersom du har et program for å håndtere passord, en såkalt ***passord manager***, eller ***passordhvelv***, så kan det fungere som en måte å dokumentere brukerkontoer på. I slike programmer lagres innloggingsinformasjon på en sikker måte. De er designet for å gjøre innlogging mye enklere, uten å måtte bekymre seg for å huske kompliserte passord. Dette kan også være et flott verktøy for å kartlegge din digitale tilstedeværelse. Det kan være lurt å ha en plan for hvordan pårørende kan få tilgang til passordene i dette programmet. F.eks. kan du skrive ned hovedpassordet på en lapp, og legge det i en forseglet konvolutt. Konvolutten kan så åpnes etter din død av en advokat eller et familiemedlem som er utpekt på forhånd. På denne måten kan de få tilgang til brukerkontoene dine og nødvendig informasjon som er lagret der.

Noen nettsider har også metoder for å utpeke arvtagere. Facebook lar deg avgjøre hva du vil skal skje med kontoen din etter din død. Du kan velge mellom å få den slettet, eller gjøre den til en minnekonto. På minnekontoer kan de som var Facebook-venner med deg fra før dele minner med hverandre. Du kan også vurdere å snakke med en advokat som har erfaring med digital arv.

Å arve digitale ressurser

Før eller siden havner du kanskje i en situasjon hvor du må gjenopprette eller få tilgang til brukerkontoer på nett, som har tilhørt en nylig avdød venn eller familiemedlem. Vi anbefaler i så fall at du først forhører deg med en advokat og andre pårørende før du går i gang. Det er ikke unormalt at andre pårørende kan bli opprørt dersom du setter i gang uten å ha forhørt deg med dem. Når det er gjort, start med å samle det du kan finne av passord. Har den avdøde skrevet dem ned eller lagret dem på noen måte? Dersom det ikke er tilfelle, har du mulighet til å bruke en datamaskin eller mobil hvor avdøde var logget inn? Om det heller ikke går, kan du bli nødt til å ta kontakt med de som driver de aktuelle nettsidene og tjenestene for hjelp med å få tilgang. Da må du som oftest oppgi både dødsattest eller skifteattest, samt en form for bevis på at du er i nær familie med den avdøde. Som oftest vil du da heller ikke kunne få tilgang til brukerkontoen eller data som er lagret der, du vil kun kunne be om å få den slettet. De fleste sider og tjenester har sin egen måte å håndtere dette på, så det kan bli en tidkrevende prosess.

I dagens digitale verden burde vi ikke bare vurdere de fysiske ressursene når vi planlegger for fremtiden, men også de digitale.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Cheryl Conley *er ekspert på phishing og bevisstgjøring, hun har blant annet vært med på å bygge opp og styre phishingprogrammet til Lockheed Martin. Nå bistår hun SANS sitt sikkerhetsbevissthetsteam, og innehar en SSAP (SANS Security Awareness Professional) sertifisering.*

Ressurser

Passordhvelv: https://www.sans.org/u/Y5Y

Passord gjort enkelt: https://www.sans.org/u/Y63