Tiltak etter en lekkasje …

1. Bytt passordene dine

Begynn med tjenesten som ble rammet av lekkasje, og tingene du bruker mest. Tenk på nettbank, e-post, nettbutikker og sosiale medier.

2. Skru på 2FA («tofaktorautentisering»)

Dette gjør det vanskeligere for folk å få tilgang til kontoen din, ved at det må to koder eller «faktorer» til for å logge inn på den. Selv om noen skulle ha passordet ditt, har de ikke den andre «faktoren» – ofte en kode sendt til telefonen din. På nettsiden Authy kan du søke etter plattformer med 2FA og bli guidet gjennom oppsettet.

3. Varsle banken din, og frys om nødvendig kredittkortet ditt

Avhengig av lekkasjens art kan det være greit å kontakte banken og kredittvurderingsbyrået du bruker (eller en annen institusjon som vurderer kredittverdighet i landet du bor i). Dette hindrer folk i å søke om nye kredittkort i ditt navn og hindrer dermed at problemet sprer seg. Lokale forbrukerorganisasjoner og offentlige forbrukerorganisasjoner kan også hjelpe til. Banken din vil snakke med deg for å finne ut om du behøver nye kontonumre og kort.

4. Fortell dine nærmeste hva som har skjedd

Dette er dine nære venner og slektninger. Da vil de være på vakt for uvanlige oppringninger eller e-poster fra mulige svindlere.

Nå kan du se på hva du kan gjøre for å begrense skaden når lekkasjen rammer.

5. Sjekk hva du kan finne ut på nettet

Det kan være greit å sjekke om din personlige informasjon ligger ute. Hva slags informasjon kan du finne uten å måtte grave noe særlig? Begynn med søkemotoren du vanligvis bruker, og bruk søkeord som i seg selv ikke forteller så mye, f.eks. navnet ditt og de siste fire sifrene i telefonnummeret ditt, men ikke hele telefonnummeret. Med Firefox Monitor kan du søke og se om informasjonen din har blitt lekket, og du kan registrere deg for å motta siste lekkasjenytt.

6. Be nettsider direkte om å slette dataene dine

Tenk deg at du har et jobbintervju i nær fremtid og ikke er helt fornøyd med hva søkeresultatene viser om deg. Du kan ta direkte kontakt med nettsider for å få dataene dine slettet, i henhold til rettighetene dine etter EUs personvernforordning (GDPR) Mange nettsider retter seg ivrig etter de nye personvernreglene i GDPR, så om du ber dem om å slette informasjon, vil de ofte gjøre det raskt for å spare seg for bryderi og utgifter. Generelt er det slik at dersom et produkt eller en tjeneste tilbys i EU, må databehandlingen følge GDPR, uavhengig av om du eller selskapet fysisk befinner dere der.

Du kan også bruke tjenester som får dataene slettet for deg. Nettsider som Reputation Defender, Privacy Duck og Abines Delete Me tar kontakt med nettsider for å få slettet informasjonen din. Dette tar de betalt for, men de har også mer informasjon om hvordan du kan gjøre det selv.

Tiltak du kan gjøre når som helst …

1. Sjekk hvilke av dataene dine som er tilgjengelige på nettet

(Begynn med viktige tjenester som e-post, banktjenester, butikker og chat.)

Spør deg selv:

1. Hvor har jeg kontoer med personlige data?
2. Hvordan kan dette bli et problem ved en lekkasje?
3. Hvorfor er den der? (Trenger den være der?)
   Hva slags sikkerhetstiltak har de? Finn nettsidens personvernerklæring eller bruksvilkår og se etter begreper som «kryptering» pluss «langtidslagring» («at rest») eller «datakommunikasjon» («in transit»), som betyr at dataene dine er sikkert lagret.
4. Hvilke regler har de for tilgangskontroll, og hvor lenge lagrer de dataene? Sier bruksvilkårene noe om hvorvidt alle ansatte har tilgang til informasjonen din? Hvilke rutiner har de for dataarkivering? Om en nettside ikke oppgir hvor lenge de beholder informasjonen din, er svaret antakeligvis for alltid.

2. Jevnlig ryddesjau

Om tjenester ikke har dataene dine, kan de heller ikke lekkes eller stjeles. Om de bare har informasjon fra de siste tre måneder, er dette alt som kan komme på avveier. Derfor bør du jevnlig rydde opp i dataene dine på nett. Spør deg selv: «Hvorfor beholder jeg dette?» Slett det du ikke trenger, og last ned det du faktisk trenger, slik at du kan fjerne dataene fra nettsiden eller appen.

3. Sjekk igjen

Kan jeg styrke sikkerheten min med bedre passord og 2FA?

4. Be selskaper om å ta bedre vare på dataene dine

Noen vil si det alltid vil skje lekkasjer, slik det alltid vil finnes kriminalitet. Men selskaper kan også gjøre mer for å beskytte dataene dine. Kontakter du dem, kan de bli oppmerksomme på at de må lytte og handle. For eksempel kan du tvitre til dem og skrive noe slikt som «Vi ønsker å vite hvor lenge dere beholder dataene våre. Det bør ikke være for alltid».

TACTICAL TECH DATA DETOX #datadetox datadetoxkit.org