Det månedlige nyhedsbrev om IT-sikkerhed til dig

Fire enkle ting du kan gøre for at forblive sikker

Oversigt

Det kan virke overvældende og forvirrende at bruge teknologierne sikkert, Men uanset hvilken teknologi, du bruger, eller hvordan du bruger det, er her fire enkle trin, som vil hjælpe dig til at forblive sikker.

1. dig selv: først og fremmest skal du være klar over, at teknologi alene ikke kan beskytte dig, du er dit bedste forsvar. IT-kriminelle har lært, at den nemmeste måde at få, hvad de ønsker, er at målrette angreb mod dig, snarere end din computer eller andre enheder. Hvis de vil have din adgangskode, kreditkortoplysninger eller kontrol over din computer, vil de forsøge at narre dig til at give det til dem, ofte ved at skabe en følelse af hastende karakter. For eksempel, kan de ringe til dig og foregiver at være Microsoft teknisk support og hævde, at din computer er inficeret, når i virkeligheden er de bare IT-kriminelle, der vil have dig til at give dem adgang til din computer. Eller måske sender de dig en e-mail med besked om, at din pakke ikke kunne leveres og presse dig til at klikke på et link for at bekræfte din postadresse, når de i virkeligheden blot vil narre dig til at besøge en ondsindet hjemmeside, der vil hacke sig ind i din computer. I sidste ende er det bedste forsvar mod IT-kriminelle dig. Ved at bruge sund fornuft kan du spotte og stoppe mange angreb.

2. passphrases: Moderne computers hastigheder har gjort den gamle, 8-karakter adgangskode forældet og sårbar. Når et websted beder dig om at oprette en adgangskode, skal du i stedet oprette en stærk og unik passphrase. En passphrase, er en type adgangskode, der bruger en række ord, som du let kan huske, såsom "Bee Honey Bourbon Rain". Jo længere din passphrase er, jo stærkere er den. En unik passphrase betyder, at du bruger en unik passphrase for hver enhed eller online konto. På denne måde er alle dine andre konti og enheder er stadig sikre, hvis en passphrase bliver kompromitteret. Kan du ikke huske alle de passphrases? Brug en passwordmanager, som er et specialiseret program, der sikkert gemmer alle dine passphrase i et krypteret format (og også tilbyder masser af andre fantastiske funktioner).

Til sidst skal du benytte totrinsbekræftelse (også kaldet two-factor eller multi-factor authentication). Du bruger din passphrase men også en kode sendt til din smartphone eller en kode, der er genereret i en app.

Totrinsbekræftelse er nok det vigtigste skridt, du kan tage for at beskytte dine online konti, og det er meget nemmere, end du måske tror.

3. opdatering: Sørg for, at alle dine computere, mobile enheder, programmer og apps kører den nyeste version af softwaren. IT-kriminelle søger konstant efter nye sårbarheder i den software dine enheder bruger. Når de opdager sårbarheder, benytter de særlige programmer til at udnytte dem og hacke sig ind i de enheder, du bruger. Samtidig arbejder de virksomheder, der skabte softwaren til disse enheder hårdt på at lukke sårbarhederne ved at frigive opdateringer. Ved at sikre, at dine computere og mobile enheder installerer disse opdateringer hurtigt, gør du det meget sværere for nogen at hacke dig. For at holde dig opdateret skal du blot aktivere automatisk opdatering, når det er muligt. Denne regel gælder for næsten enhver teknologi, der er forbundet til et netværk, herunder Internet-tilsluttede tv's, babyalarmer, overvågningskameraer, hjemmeroutere, spillekonsoller eller endda din bil.

4. backups og gendannelse: nogle gange, uanset hvor omhyggelig du er, kan du blive hacket. Hvis det er tilfældet, er backup ofte den eneste måde at gendanne alle dine personlige oplysninger. Sørg for at foretage regelmæssige sikkerhedskopieringer af vigtige oplysninger, og tjek, at du kan gendanne dine data fra dem. De fleste operativsystemer og mobile-enheder understøtter automatisk sikkerhedskopiering, enten til eksterne drev eller til skyen.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

*SANS certificeret instruktør **Steve Anson** giver vejledning til IT-sikkerhedsteams og regeringer rundt om i verden for at forbedre deres sikkerhed. Steve er forfatteren til den kommende bog "Applied Incident Response" og giver gratis informationer og tips til folk der arbejder med IT-sikkerhed på www.AppliedIncidentResponse.com.*

Hvis du vil vide mere

Social Engineering:	https://www.sans.org/u/W3G
Personlige svindel:	https://www.sans.org/u/W3Q
Gør passwords enkle:	https://www.sans.org/u/W3V
Fik sikkerhedskopier:	https://www.sans.org/u/W40