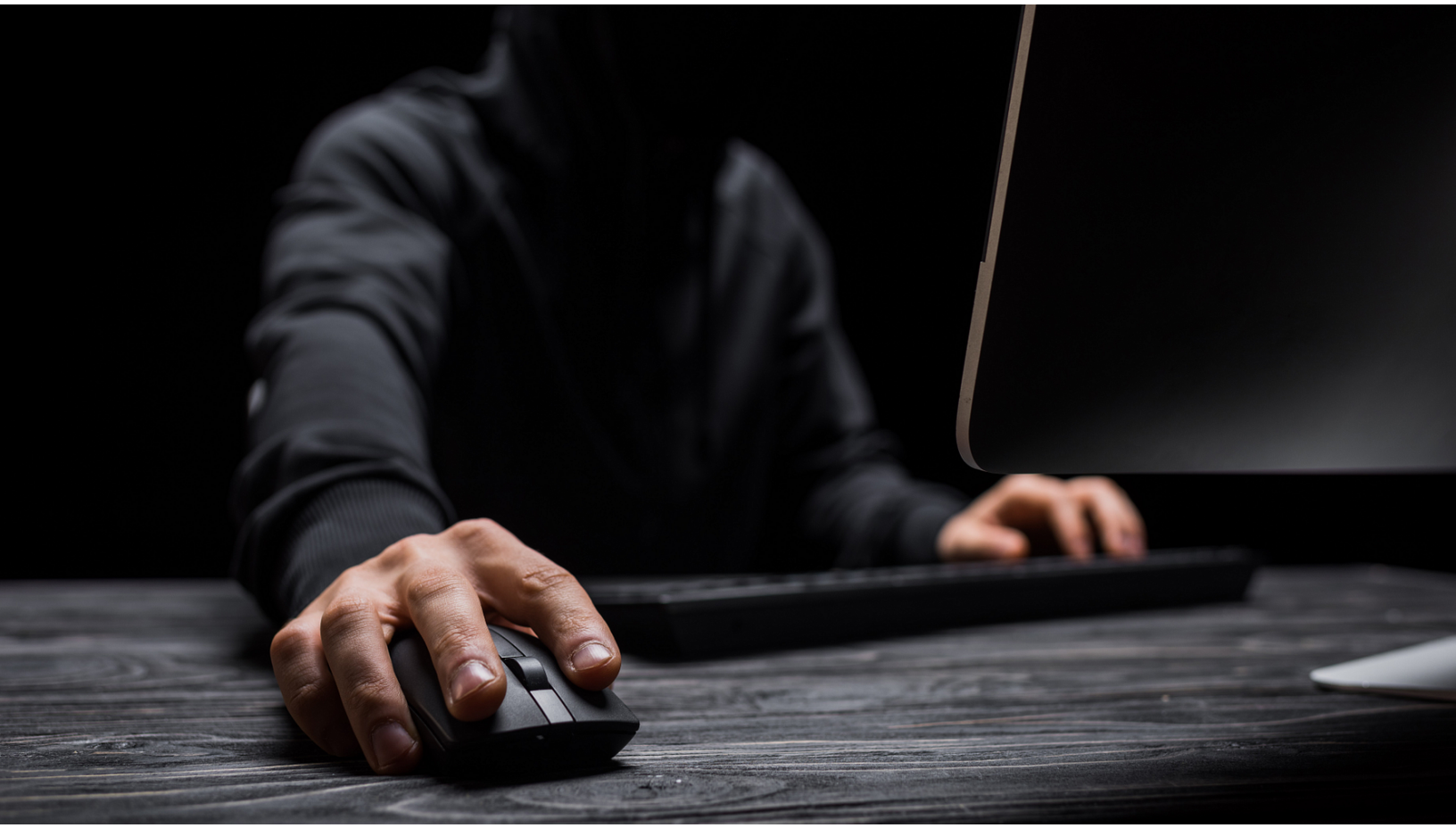

2024-01-04 07:00 CET

”Smarte” enheder er en åben invitation til hackere og svindlere

Ny data fra Telenor viser, at hjemmet er en overset legeplads for hackere og digitale svindlere, der kan udføre ondsindede angreb gennem alt fra din robotstøvsuger til din automatiske belysning – uden at du bemærker det.

Da Telenors sikkerhedsfilter SikkerSurf, der automatisk blokerer hjemmesider med svindel og virus, i efteråret blev lagt på alle selskabets internetabonnementer, fik det antallet af blokeringer til at stige markant.

Data fra Telenor viser, at der bliver foretaget 800 % flere SikkerSurf-

blokeringer pr. abonnement på internet sammenlignet med mobil. Ifølge Per Olsen, sikkerhedschef hos Telenor, understreger det, hvor overset hjemmet er som potentiel indgang for hackere og svindlere, og hvor massivt behovet er for bedre digital sikkerhed i hjemmet.

”Rigtig mange danskere tænker ikke over, hvor mange enheder i hjemmet, der er koblet på internettet. Og hvis først hackerne har fået adgang til én enhed, fx et ældre smart-tv, der ikke er blevet sikkerhedsopdateret længe, eller en bærbar computer, hvor din teenager har downloadet en fil af tvivlsom oprindelse, kan hackerne lynhurtigt rykke videre og angribe andre enheder, der er koblet på hjemmets wi-fi,” siger Per Olsen.

Center for Cybersikkerhed vurderer også, at truslen fra cyberangreb mod ”smarte” enheder er meget høj. Hackerne betragter generelt disse enheder som attraktive mål, fordi de generelt er dårligere beskyttede end almindelige computere og dermed nemmere at kompromittere.

Ét svagt led er alt, der skal til

Hackerne og de digitale svindlere kan udnytte selv det mindste svage punkt til at få adgang til hele dit netværk. Hackerne kan fx kigge med på dit overvågningskamera eller udnytte en brandalarm til at stjæle personlige oplysninger fra dit internet. De kan også bruge adgangen til dit internet og dine ”smarte” enheder til at angribe din arbejdsplads eller deltage i koordinerede angreb mod virksomheder og myndigheder.

”De største risici for forbrugerne er datalæk og ransomware-angreb, men konsekvenserne kan være meget mere vidtrækkende end det. Og desværre kan det ske helt uden, at forbrugerne bemærker det. Netop fordi brugerne ikke er klar over de potentielle sikkerhedsrisici ved de smarte enheder, ved de ofte heller ikke, hvordan de skal beskytte sig selv,” siger Per Olsen.

Per Olsen og Telenor har disse tre råd til dig, der gerne vil have bedre styr på den digitale sikkerhed i hjemmet:

1. Opdater din "smart"-enhed for at undgå sikkerhedshuller og forhindre digitale svindlere i at få adgang til dit internet og andre enheder.
2. Beskyt dit internet mod digitale svindlere ved at sikre din router

på samme måde, som du sikrer dine enheder.

3. Vælg et stærkt kodeord til din "smart"-enhed for at beskytte dine personlige oplysninger og forhindre uautoriseret adgang. Et stærkt kodeord bør være langt og komplekst med en kombination af store og små bogstaver, tal og specialtegn uden personlige oplysninger.

Telenor hjælper danskerne med at skabe gode forbindelser via mobil og internet. Vores mål er at skabe sammenhæng i vores kunders digitale liv og i det danske samfund. Derfor investerer vi hvert år massivt i innovation og i udvikling af den danske teleinfrastruktur.

Telenor er Danmarks næststørste teleselskab og en del af Telenor-koncernen, som opererer i hele Norden og i Asien, og på verdensplan hjælper vi 186 millioner kunder med at kommunikere. I Danmark er vi ca. 1000 medarbejdere, har 38 butikker fordelt over hele Danmark og gør hver dag vores yderste for at gøre det nemt for vores kunder at kommunikere og sikre deres forbindelse på både mobil og internet. I Danmark er CBB Mobil også en del af Telenor-familien. Du kan læse mere om os på www.telenor.dk.

Kontaktpersoner

Cecilie Bruun Iversen
Pressekontakt
Pressechef
info@telenor.dk
25 600 800