
# BIDRAG TIL SIKRE TRÅDLØSE MUS OG TASTATURER I DIN WFH-OPSÆTNING

**Det er meget vigtigt at opretholde virksomhedens sikkerhed i dag med stadigt flere cybertrusler. De trådløse mus og tastaturer, som dine medarbejdere bruger hver dag, er en integreret del af det overordnede sikkerhedslandskab.**

## HER FØLGER ET PAR TING, DU SKAL OVERVEJE, NÅR DU VURDERER SIKKERHEDEN I DIN OPSÆTNING AF EKSTERNT UDSTYR.

- ☐ **Find ud af, hvilke enheder der er forbundet til dine slutpunkter.** Hvis din organisation ikke stiller mus og tastaturer til rådighed for medarbejderne eller har en liste over godkendte, acceptable enheder, er det umuligt at vide, hvilket udstyr, dine medarbejdere sidder med.
- ☐ **Sørg for, at der bruges krypterede forbindelser til disse enheder.** Krypterede forbindelser forhindrer hackere i at bruge enheder som wi-fi-"sniffere" og opsnappe tastetryk og museklik på afstand.
- ☐ **Opdater firmwaren på enhederne.** Forældet firmware kan gøre enhederne sårbare over for identificeret udnyttelse.
- ☐ **Sørg for, at *Bluetooth*®-enheder bruger Sikkerhedstilstand 1 - niveau 4.** Denne indstilling vil hjælpe med at sikre forbindelser mellem enheder.
- ☐ **Sørg for, at firmwarens sikkerhedsniveau ikke rulles tilbage i enheder med USB-dongler.** Enheder, der kan rulle sikkerhedsrelaterede firmwareopgraderinger tilbage, kan udsætte dine slutpunkter for angreb.
- ☐ **Sørg for, at dine ansatte er instrueret i faren ved angreb på mus/tastatur.** Sammen med uddannelse i malware- og phishing-sikkerhed skal du sørge for, at dine medarbejdere ved, at mærkelig adfærd med musen/tastaturet kan være et tegn på, at nogen har overtaget uautoriseret kontrol.

**Logitech-løsninger hjælper med at implementere sikkerhedsfunktioner i din virksomheds opsætning i en verden, hvor du kan arbejde overalt. Se nærmere på de nyeste Logi Bolt-enheder til dine medarbejdere i dag.**

logitech | for business