BIDRA TIL Å SIKRE TRÅDLØSE MUS OG TASTATURER I HJEMMEKONTORGRUPPEN HVORDAN SIKRE TRÅDLØSEENHETER SOM MUS OG TASTATUR PÅ HJEMMEKONTOR

Med dagens stadig ekspanderende nettrusler er det viktig å styrke bedriftssikkerheten. De trådløse musene og tastaturene de ansatte bruker hver dag, er en integrert del av det samlede sikkerhetslandskapet.

HER ER NOEN TING SOM BØR VURDERES VED EVALUERING AV SIKKERHETEN TIL DE ANSATTES TRÅDLØSE ENHETER.

- ☐ **Få en oversikt over trådløseenheter og endepunktene.** Hvis organisasjonen ikke leverer musene og tastaturene til de ansatte eller har en liste over godkjente, tilfredsstillende enheter, er det umulig å si hva som befinner seg der ute.
- ☐ **Sørg for at disse enhetene har krypterte tilkoblinger.** Krypterte tilkoblinger kan bidra til å hindre hackere i å bruke enheter som «wifi-sniffere» og dermed snappe opp tastetrykk og museklikk fra avstand.
- ☐ **Oppdater firmware og sikkerhetsoppdateringene på enhetene.** Utdatert firmware og oppdateringer kan gjøre enheter sårbare for identifiserte utnyttelser.
- ☐ **Sørg for at *Bluetooth*®-enheter anvender sikkerhetsmodus 1, nivå 4.** Denne innstillingen bidrar til sikre tilkoblinger mellom enheter. Unngå at enheter med USB-maskinvarelåser svekker sikkerhetsrelaterte firmware og oppdateringer, da dette kan eksponere endepunktene for angrep.
- ☐ **Unngå at enheter med USB-maskinvarelåser svekker sikkerhetsfastvaren.** Enheter som kan svekke sikkerhetsrelaterte fastvareoppdateringer, kan eksponere endepunktene for angrep.
- ☐ **Lær opp de ansatte om mus-/tastaturangrep.** I tillegg til opplæring om skadelig programvare og phishing-sikkerhet, må det påses at de ansatte vet at merkelig mus-/tastaturatferd kan tyde på at noen har tatt uautorisert kontroll.

Logitech-løsninger hjelpermed å implementere sikkerhetsfunksjoner for arbeidsstyrken i en verden hvor folk jobber hvor som helst. Utforsk de seneste Logi Bolt-enhetene for de ansatte i dag.

logitech | for business