



BIDRAR TILL ATT SÄKRA TRÅDLÖSA MÖSS OCH TANGENTBORD I DIN INSTALLATION FÖR ARBETE HEMIFRÅN

Att bibehålla företagssäkerhet är extremt viktigt i dagens värld som är full av nya hot på internet. De trådlösa möss och tangentbord din personal använder dagligen är en väsentlig del av säkerheten i stort.

HÄR ÄR NÅGRA SAKER ATT TÄNKA PÅ NÄR DU UTVÄRDERAR SÄKERHETEN FÖR GRUPPENS TRÅDLÖSA TILLBEHÖR.

- Känn till vilka enheter som är anslutna till slutpunkterna.** Om organisationen inte tillhandahåller möss och tangentbord till personalen eller har en lista över godkända, acceptabla enheter så kan vad som helst användas.
- Säkerställ att dessa enheter har krypterade anslutningar.** Krypterade anslutningar förhindrar hackare från att använda enheter som "Wi-Fi-sniffare" och att fjärrstoppa tangentkopplingar och musklick.
- Uppdatera enheternas inbyggda programvaror.** Inbyggda programvaror som är inaktuella kan göra enheter sårbara för identifierade exploateringar.
- Säkerställ att Bluetooth®-enheter använder säkerhetsläge 1, nivå 4.** Inställningen hjälper till att säkra anslutningar bland enheter.
- Förhindra enheter med USB-donglar från att återställa den inbyggda säkerhetsprogramvaran.** Enheter som återställer uppgraderingar av inbyggda, säkerhetsrelaterade programvaror kan exponera slutpunkter för angrepp.
- Utbilda personalen inom angrepp mot möss/tangentbord.** I hop med utbildning om skadliga programvaror och säkerhet gällande nätfiske kan du säkerställa att personalen känner till att udda mus-/tangentbordsbeteende kan vara ett tecken på att någon obehörig har tagit kontroll.