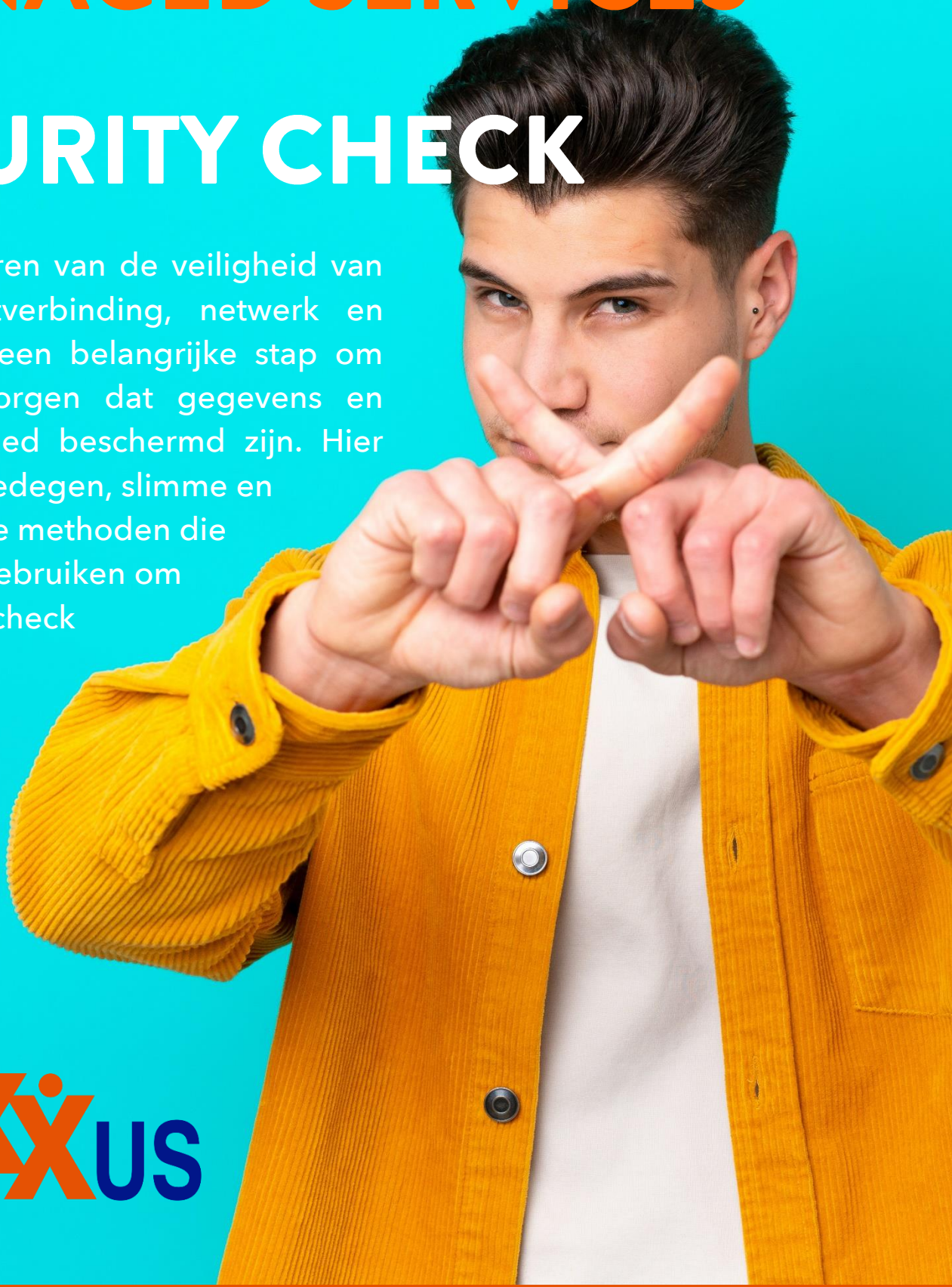
MAXXUS
MANAGED SERVICES

SECURITY CHECK

Het controleren van de veiligheid van een internetverbinding, netwerk en werkplek is een belangrijke stap om ervoor te zorgen dat gegevens en systemen goed beschermd zijn. Hier zijn enkele gedegen, slimme en redelijk snelle methoden die we kunnen gebruiken om een security check uit te voeren



MAXXUS
ICT & TELECOM

"ONLINE" MODERNE WERKPLEK | MICROSOFT 365 FOR BUSINESS & TEAMS | TELEFONIE INFRASTRUCTUUR | KPN EEN EXCELLENCE PARTNER | VODAFONE SOLUTION PARTNER

BEDRIJFSBOUWSTEEN

SECURITY

Er zijn verschillende redenen waarom Security één van de belangrijkste aandachtspunten zou moeten zijn binnen organisaties. Eén van de belangrijkste redenen is dat er vaak waardevolle informatie wordt opgeslagen, zoals persoonlijke gegevens van klanten en financiële gegevens, die kwetsbaar zijn voor cyberaanvallen. Onderstaand onze 10 security check stappen:

1. Gebruik sterke wachtwoorden: Zorg ervoor dat je sterke, unieke wachtwoorden gebruikt voor al je accounts. Gebruik een wachtwoordmanager om wachtwoorden te genereren en op te slaan.

2. Regelmatige software-updates: Zorg ervoor dat al je software, inclusief besturingssysteem, antivirusprogramma's en andere toepassingen, up-to-date zijn met de nieuwste beveiligingspatches. Schakel automatische updates in waar mogelijk.

3. Firewall inschakelen: Zorg ervoor dat je firewall is ingeschakeld op zowel je router als je computer. Dit helpt ongeautoriseerde toegang tot je netwerk te voorkomen.

4. Versleutel je draadloze netwerk: Stel een sterk wachtwoord in voor je draadloze netwerk en gebruik indien mogelijk de WPA2- of WPA3-versleuteling. Hiermee voorkom je dat ongeautoriseerde gebruikers toegang krijgen tot je netwerk.

5. Gebruik een VPN: Overweeg het gebruik van een Virtueel Private Netwerk (VPN) wanneer je verbinding maakt met openbare Wi-Fi-netwerken. Een VPN versleutelt je internetverkeer en beschermt je tegen mogelijke aanvallen.

6. Phishing-e-mails vermijden: Wees voorzichtig met verdachte e-mails, vooral die waarin om persoonlijke informatie wordt gevraagd. Open geen bijlagen of klik niet op links in e-mails van onbekende afzenders.

7. Gebruik tweestapsverificatie: Schakel tweestapsverificatie in voor al je accounts waar mogelijk. Dit voegt een extra beveiligingslaag toe door een verificatiecode te vereisen naast je wachtwoord.

8. Beveiligingsscans uitvoeren: Voer regelmatig beveiligingsscans uit op je netwerk en apparaten met behulp van betrouwbare antivirus- en anti-malwareprogramma's.

9. Beveiligde back-ups: Maak regelmatig back-ups van je belangrijke gegevens en bewaar ze op een externe schijf of in de cloud. Dit helpt bij het herstellen van gegevens in geval van een beveiligingsincident.

10. Bewustwording van sociale technieken: Wees alert op sociale technieken, zoals phishing, waarbij aanvallers proberen gevoelige informatie te verkrijgen door zich voor te doen als betrouwbare entiteiten. Wees voorzichtig met het delen van persoonlijke of gevoelige informatie.

Het is ook raadzaam om regelmatig contact te hebben met uw IT Partner of Managed Service Provider om een uitgebreide beoordeling van de beveiliging van je netwerk en systemen uit te voeren. Meer weten over onze Security Check?
070 307 66 00 of www.maxxus.nl