

TUI IT beveiligingsadvies voor klanten

1. Denk na voordat je klikt

Als je berichten op afstand controleert, kun je gemakkelijk fouten maken. Wees op je hoede voor phishing e-mails, sms'jes of voicemailen. Fraudeurs proberen je vaak op te jagen om iets te doen. Neem even de tijd om adem te halen en na te denken voordat je reageert. Geef nooit je boekingsgegevens aan iemand die je niet kent of vertrouwt.

2. Gebruik een veilig netwerk

Vermijd het bekijken van gevoelige informatie als je openbare Wi-Fi gebruikt. Het is beter om te wachten tot je een privé Wi-Fi-netwerk kunt gebruiken of gebruik een Virtual Private Network (VPN) om je verbinding veilig te houden.

3. Veiligheid van sociale media

Wees voorzichtig met het plaatsen van berichten over waar je bent of je reisplannen. Deel niet te veel informatie die fraudeurs kunnen gebruiken om zich voor te doen als jou of om toegang te krijgen tot je accounts. Maak je Social Media-account privé zodat alleen vertrouwde vrienden en familie je berichten kunnen zien.

4. Sterke wachtwoorden en PIN-codes

Veilige wachtwoorden en pincodes houden je persoonlijke gegevens en accounts veilig voor fraudeurs. Maak sterke wachtwoorden en PIN-codes met een mix van letters, cijfers en symbolen. Gebruik geen gemakkelijk te raden wachtwoorden of PIN-codes zoals uw naam of geboortedatum. Kies PIN-codes die niet voor de hand liggen, zoals "1234" of "0000". Het best gebruikt je voor elk account een ander wachtwoord en wijzig je deze wachtwoorden regelmatig.

5. Multifactor Authenticatie (MFA) inschakelen

Door een extra beveiligingslaag toe te voegen aan je accounts kun je onbevoegde toegang voorkomen, zelfs als iemand je wachtwoord kent. Met MFA kun je je identiteit bevestigen met een extra beveiliging, zoals een code die via sms wordt verzonden of via gezichts- of vingerafdrukherkenning.