Beste collega,

Je ontvangt deze mail omdat je bent geautoriseerd voor Verzuimsignaal, het online verzuimvolgsysteem van de UT.
Vanaf **woensdag 12 december** wordt de toegang tot Verzuimsignaal extra beveiligd. Hierdoor heb je bij het inloggen een tweede authenticatie nodig. Deze tweede authenticatie loopt via een smartphone.

Waarom authenticatie in 2 stappen?

In de Algemene verordening gegevensbescherming (AVG) zijn de eisen die gesteld worden aan de verwerking van bijzondere persoonsgegevens, aangescherpt. Bijzondere persoonsgegevens zijn door hun aard zeer gevoelig en genieten in de AVG extra bescherming. Inloggen met alleen een gebruikersnaam en wachtwoord voldoet niet langer.
De UT heeft meerdere applicaties in gebruik waarmee bijzondere persoonsgegevens worden verwerkt. Op grond van de AVG moet de UT deze applicaties extra beveiligen door authenticatie in twee stappen: Two Factor Authenticatie (2FA).
Verzuimsignaal is de eerste applicatie waarvoor de UT overgaat op een 2FA. In Verzuimsignaal worden gegevens verwerkt over de gezondheid van medewerkers. Daarmee behoort het online verzuimvolgsysteem tot de meest gevoelige applicaties. Andere applicaties volgen op een later moment.

Tweede authenticatie via smartphone

Er zijn diverse 2FA applicaties op de markt voor de smartphone. De UT heeft gekozen voor *NetIQ Advanced Authentication* en G*oogle Authenticator (TOTP)*. Om toegang te krijgen tot extra beveiligde informatiesystemen moet je één van deze apps installeren op je smartphone.
Heb je geen smartphone van de UT en wil je voor de 2FA geen privé smartphone gebruiken? Dan kun je via de LISA selfservice portal een low budget smartphone aanschaffen op kosten van de faculteit/dienst.

Installeren en activeren 2FA applicatie

Log je op of na **woensdag 12 december vanaf 16.00 uur** in op Verzuimsignaal, dan word je automatisch doorgeleid naar de MyID registratieportal. Deze portal stuurt het installatie- en activatieproces van de authenticator op je smartphone. Aan het einde van dit proces ontvang je een recovery key. Deze recovery key heb je nodig om de authenticator bij verlies of vervanging van je smartphone te deactiveren op je oude

toestel en te activeren op je nieuwe toestel. Het is belangrijk om de recovery key op een veilige plaats op te slaan. LISA CyberSafety adviseert hiervoor de passwordmanager LastPass.

Toegang tot verzuimsignaal

Nu 2FA is geactiveerd hoef je alleen nog maar in te loggen op verzuimsignaal en met je smartphone valideer je de verbinding.

Vragen

Heb je vragen over installatie/activatie en gebruik van de 2FA applicatie? Raadpleeg dan de FAQ of neem contact op met de Servicedesk ICT.

Met vriendelijke groet,

Servicedesk ICT
Library, ICT Services & Archive (LISA)