Praktische tips

- ☑ Vergrendel de notebook van de vereniging altijd bij het verlaten van de projectieplek tijdens de pauzes. Voor de Windows PC doe je dit door de **Windows-toets + L** in te toetsen.
  Is er een MacBook aanwezig, toets dan **Ctrl+ cmd+Q**
- ☑ Laat geen ledenlijsten onbeheerd achter op uw bureau, printer of in de zaal.
- ☑ Gebruik nooit de inlog van je mede VNFE-leden en geef ook nooit uw inloggegevens door aan je mede VNFE-leden.
- ☑ Krijgt u de notebook van het VNFE in beheer, gebruik deze dan niet voor privé, doch enkel voor de presentatie-doeleinden van het VNFE.
- ☑ Zorg ervoor dat je mobiel (iPhone, iPad, Androïd) en notebook is beveiligd met een toegangscode. Gebruik minimaal 5 karakters en/of TouchID (vingerafdrukherkenning).
- ☑ Gebruik nooit hetzelfde wachtwoord voor meerdere accounts. Laat datadragers (zoals: notebook, iPad, iPhone, USB-stick) nooit onbeheerd achter op de projectieplek, in uw auto of op uw bureau.
- ☑ Kies nooit voor automatisch opslaan van inloggegevens op je computer.
- ☑ Besef dat openbare netwerken (bijvoorbeeld: Free WiFi bij McDonalds) niet veilig zijn. Het is veiliger om dan de 4G data te gebruiken. Gratis WiFi is gevaarlijk!
- ☑ Let op wat je plaatst of deelt op de sociale media.
- ☑ Bedek je webcam als je hem niet gebruikt. Hiermee wordt ongewenst 'meekijken' voorkomen.
- ☑ Open nooit bijlagen welke verzonden zijn per email door onbekende mensen. Kijk bij de bekende mensen of de tekst in de email wel 'klopt'.
- ☑ Klik nooit op advertenties en zeker niet op spam. Gewoon negeren en zeker niet op klikken!
- ☑ Heeft u een USB-stick gevonden? Meteen weggooien!!!! USB-sticks worden moedwillig achtergelaten met ransomware. Met randsomeware worden je bestanden geblokkeerd. Bewaar daarom je bestanden op een veilige plek digitaal op uw beveiligde PC of NAS-server.
- ☑ Heb je zelf ook een veilig idee, hoe om te gaan met mogelijke datalekken, laat het weten!

d.d.: 22-05-2018