

TILGJENGELIGGJØRING AV DIGITALE VERKTØY I HELSE- OG OMSORGSSEKTOREN

Tema 1.4. Sikker og enkel bruk av mobile enheter

Finansiert av Den europeiske union. Synspunktene og meningene som kommer til uttrykk, er imidlertid kun forfatterens egne og gjenspeiler ikke nødvendigvis synspunktene til EU eller European Education and Culture Executive Agency (EACEA). Verken EU eller EACEA kan holdes ansvarlig for dem.

Innholdsfortegnelse

1. Introduksjon til kurset
2. Enkel bruk av mobile enheter
3. Sikker bruk av mobile enheter

1. Introduksjon til kurset

1.1 Oversikt over kurset

1.2 Målgruppe

1.3 Mål for opplæringen

1.4 Format og indikatorer

1. Introduksjon til kurset



1.1. Oversikt over kurset

Hva handler kurset om?

Kurset tar sikte på å øke helsepersonells ferdigheter og kunnskaper om sikker og effektiv bruk av mobile enheter i arbeidshverdagen. Kurset tilbyr tiltak, verktøy og tips som er enkle å implementere. For å sikre at den tilegnede kunnskapen brukes mest mulig effektivt i praksis, er det viktig å bygge videre på erfaringer og eksisterende ressurser i målgruppen.

Nytteverdi

SociALL-prosjektets transnasjonale rapport viste at praksis rundt bruk av mobile enheter er et sentralt tema på tvers av landegrensene. De fleste helsearbeidere bruker mobile enheter til personlig bruk og har kjennskap til funksjonalitet, operativsystem, applikasjoner osv. Dette kurset gir dem muligheten til å utføre arbeidsoppgaver raskere og enklere, føle seg tryggere på bruken av mobile enheter og dermed bli mer produktive.

1. Introduksjon til kurset



1.2. Målgruppe

Hvem er kurset for?

Målgruppen omfatter alle fagpersoner som jobber i helse- og omsorgssektoren, inkludert sosialarbeidere, rådgivere, helsepersonell, ledere og støttepersonell. Alle disse personene bruker mobile enheter daglig, i det minste til privat bruk, men som regel også i jobbsammenheng.

Passer det for meg?

Det forventes at du er vant til å bruke mobile enheter i det private, og at du har praktisk erfaring med grunnleggende funksjoner og tjenester. For å tilrettelegge for digital læring og egenutvikling, vil du bli veiledet gjennom fysiske workshops. Det vil også bli tilbudt nettbaserte workshops, nettbasert veiledning og ekstra undervisningsmaterieil.

1. Introduksjon til kurset



1.3. Mål for opplæringen

Læringsutbytte

- Forstå **betydningen** bruk av mobile enheter kan ha i helse- og omsorgssektoren
- **Bruke tips og triks som er** spesifikke for **bruk** av mobile enheter på jobb i felt.
- Lære og implementere **grunnleggende tiltak** for å øke din **digitale sikkerhet**.

Hva vil dette endre?

Etter endt opplæring vil deltakerne kunne :

- **Effektivisere arbeidsoppgaver** ved målrettet **bruk av mobile enheter i** felten
- **Øke omfanget av oppgaver og kommunikasjon** via mobile enheter.
- **Få økt tillit** til egen evne til å løse komplekse problemer og samarbeide via mobile enheter.
- **Forbedre den digitale sikkerheten** på mobile enheter.

1. Introduksjon til kurset



1.4. Format og indikatorer

Undervisningsmetode

For å tilrettelegge for digital læring og egenutvikling, er det nødvendig å veilede og aktivere deltakerne gjennom fysiske workshops. For fordypning tilbys nettbaserte workshops, nettbasert veiledning og andre former for læringsmateriell.

Organisering av undervisning

- **To fysiske workshops** à 3-4 emner
- Maks. **10** deltakere/workshop
- Det anbefales å **delta på begge workshopene** for å sikre **kontinuitet** og **maksimal læring**.

2. Workshop Enkel bruk av mobile enheter

2.1. Introduksjon og generell informasjon

2.2 Praktisk anvendelse og nyttige tips og triks

2. Enkel bruk av mobile enheter

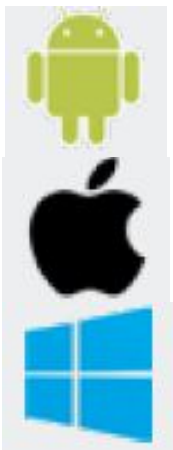
2.1. Innledning og generell informasjon

Produsenter av enheter og operativsystemer

Operativsystem

Operativsystemet er den grunnleggende programvaren som brukes til å styre en datamaskin, en smarttelefon eller et nettbrett.

De vanligste operativsystemene er



Android - Google, Samsung, LG, HTC, Huawei osv.

iOS - Apple, iPhone, iPad

Windows - Nokia, Microsoft

2. Enkel bruk av mobile enheter



2.1. Innledning og generell informasjon

Begrepsforklaring

Android

Android er Googles operativsystem.

Apper

"Apper" er programmer for mobile enheter som gjør hverdagen enklere eller leverer underholdning. Det finnes både gratis og betalte apper.

App-butikk

App-butikker. De viktigste app-butikkene: App Store (Apple), Play Store (Android), Phone Store (Windows).

Sikkerhetskopiering

Kopier for å sikre data.

Bluetooth

Bluetooth er en teknologi for trådløs overføring mellom enheter over korte avstander via radio.

2. Enkel bruk av mobile enheter



2.1. Introduksjon og generell informasjon

Begrepsforklaring

Skytjenester

Skytjenester er tjenester som gjøres tilgjengelig via Internett, f.eks. lagringsplass, datakraft eller brukerprogramvare.

GPS

GPS står for Global Positioning System, som brukes til navigasjon eller posisjonsbestemmelse ved hjelp av satellittsignaler.

IMEI-nummer

15-sifret internasjonalt serienummer på smarttelefonen (IMEI-nummer: International Mobile Station Equipment Identity).

iOS

iOS er Apples operativsystem.

Nettbank

Behandling av banktransaksjoner over Internett kalles nettbank eller mobilbank.

2. Enkel bruk av mobile enheter



2.1. Introduksjon og generell informasjon

Begrepsforklaring

Phishing

Forsøk på å svindle til seg person- og kontoinformasjon eller penger via e-post eller nettsteder.

PIN-KODE

Personlig identifikasjonsnummer.

Skjermlås

Skjermlåsen hindrer tilgang til mobilenheten og slås automatisk på etter en viss tid hvis enheten ikke har vært i bruk. Det finnes ulike alternativer for opplåsing: PIN-kode, mønsteropplåsing, fingeravtrykksskanner, ansiktsgjenkjenning.

SIM-kort

Chipkort i ulike formater som settes inn i smarttelefonen eller nettbrettet. Dette muliggjør tydelig identifikasjon, på samme måte som et medlemskort.

2. Enkel bruk av mobile enheter

2.1. Introduksjon og generell informasjon

Begrepsforklaring

Smarttelefon

En smarttelefon er en mobiltelefon med basisfunksjonene ringe, sende og motta meldinger. I tillegg tilbyr smarttelefonen andre funksjoner ved hjelp av apper, for eksempel tilgang til e-post, internett, bilder osv.

Nettbrett

Et nettbrett er en mobil enhet som ligner på en smarttelefon, men med en større skjerm. En annen vesentlig forskjell er at det ikke alltid brukes SIM-kort, men at man er avhengig av WiFi for å bruke Internett.

Oppdateringer

En oppdatering er en ny versjon av et installert program/app.

WLAN/WiFi

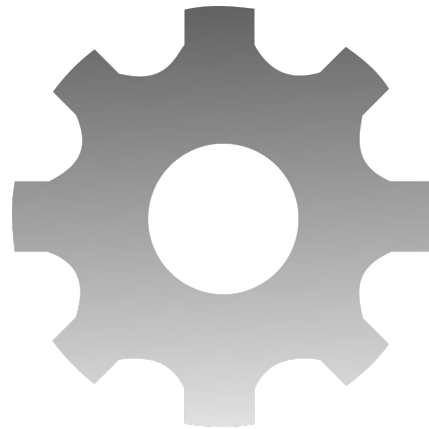
WLAN står for "Wireless Local Area Network", også kalt WiFi. Et lokalt trådløst nettverk som gir tilgang til Internett.

2. Enkel bruk av mobile enheter

2.1. Innledning og generell informasjon

Appen Innstillinger

Appen med tannhjulssymbolet tilbyr mange innstillinger for din mobile enhet.



- ✓ Konfigurere enheten bedre (f.eks. skjerminnstillinger, lyd, enklere betjening)
- ✓ Tilkoblingsinnstillinger (bruk Wi-Fi, Bluetooth, hotspot...)

2. Enkel bruk av mobile enheter

2.1. Innledning og generell informasjon

Varslingscenter og rask tilgang



2. Enkel bruk av mobile enheter

2.1. Innledning og generell informasjon

Varslingscenter og rask tilgang

På høyre side:

- Tid
- Batterinivå
- Aktuelle tilkoblinger (mobilmottak, WLAN, Bluetooth...)

Ikoner vises til venstre når operativsystemet eller enkelte apper har varsler til deg.

For eksempel:

- Google Play Store: App-oppdateringer er tilgjengelige eller har blitt installert
- WhatsApp / e-post: Du har nye meldinger
- Telefon: Ubesvart anrop
- Android-system: Oppdatering av operativsystemet er tilgjengelig
- ...

2. Enkel bruk av mobile enheter

2.1. Introduksjon og generell informasjon

Få tilgang til varslingscenteret



For å få tilgang til varslingscenteret må skjermen være ulåst. Sveip deretter nedover fra toppen, fra utsiden av berøringsskjermen. Det kan hende du må sveipe en gang til for å få full tilgang til varslingscenteret.

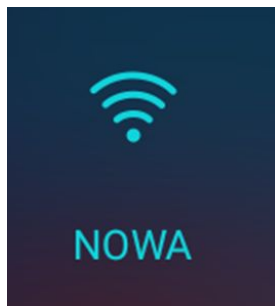
2. Enkel bruk av mobile enheter

2.1. Innledning og generell informasjon

Ikonene i varslingscenteret

Avhengig av produsenten av enheten og operativsystemets versjon, vises ulike symboler for funksjoner som kan slås av og på. Hvis en funksjon er aktivert, endrer symbolet enten farge eller lysstyrke.

Her er noen eksempler:



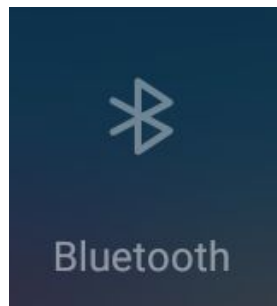
WLAN

I dette tilfellet er Wi-Fi-tilkoblingstypen aktiv, og enheten er koblet til Wi-Fi-nettverket "NOWA". WLAN står for "wireless local area network". lokal (Internett-)tilkobling". Slik Internetttilgang er ofte tilgjengelig i butikker, barer og hoteller, og du trenger gjerne et passord for å få tilgang til den.

2. Enkel bruk av mobile enheter

2.1. Innledning og generell informasjon

Ikonene i varslingscenteret



Bluetooth

På dette bildet er Bluetooth deaktivert.

Bluetooth er også en type radioforbindelse, men mellom to "Bluetooth-aktiverte" enheter (for eksempel en hodetelefon med en smarttelefon).



Automatisk (skjerm)rotasjon

Hvis denne funksjonen er aktivert, roterer skjermen fra stående til liggende når du holder enheten horisontalt, og omvendt.

Hvis dette er irriterende, kan du låse visningen ved å deaktivere den.

2. Enkel bruk av mobile enheter

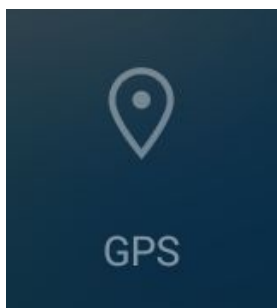
2.1. Introduksjon og generell informasjon

Ikonene i varslingscenteret



Mobile data

Hvis et SIM-kort fra en mobiloperatør er satt inn i enheten, vises dette ikonet. I land utenfor EU eller hvis du allerede har brukt opp datakreditten din, er det sannsynligvis bedre å deaktivere denne funksjonen. Du vil da fortsette å motta samtaler og SMS, men ikke lenger motta e-post og meldinger fra messenger-apper som WhatsApp.



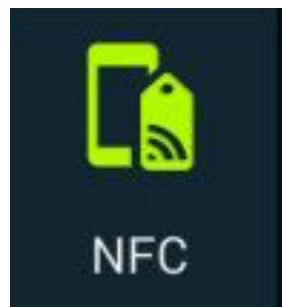
GPS (globalt posisjoneringssystem)

Hvis denne funksjonen er aktivert, kan enheten bruke satellitter til å finne posisjonen. Dette kan være nyttig hvis du navigerer i et ukjent område ved hjelp av en kartapp. Selv uten GPS blir enhetens posisjon alltid registrert, for eksempel ved at den befinner seg i nærheten av ulike radiomaster fra leverandøren din.

2. Enkel bruk av mobile enheter

2.1. Introduksjon og generell informasjon

Ikonene i varslingscenteret



NFC (nærfeltskommunikasjon)

Denne typen tilkobling er en relativt ny teknologi som du allerede kjenner fra minibanker i hverdagen: For mindre beløp kan minibankkortet ganske enkelt plasseres på leseren for å betale.

En ny smarttelefon eller et nytt nettbrett har nå også en chip som, koblet til en egnet mottakerenhet, kan utveksle informasjon bare ved å berøre den.



Flymodus

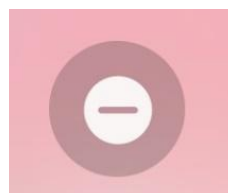
Når du aktiverer denne modusen, kobles mobil- og datatilkoblingene fra. Det betyr at du verken mottar anrop eller nye meldinger, og at du ikke kan surfe på Internett. Det er fortsatt mulig å bruke enhetens "offline"-funksjoner (notater, lytte til musikk, bruke mange apper og spill).

Under flyreiser blir du bedt om å gjøre dette av sikkerhetsmessige årsaker.

2. Enkel bruk av mobile enheter

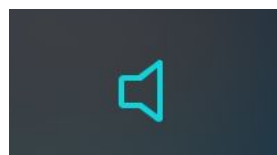
2.1. Innledning og generell informasjon

Ikonene i varslingscenteret



Ikke forstyr

Hvis du aktiverer denne funksjonen, blir anrop og meldinger (SMS, WhatsApp, ...) dempet. Anropene viderekobles direkte til telefonsvareren og vises som ubesvarte anrop. I innstillingene kan du definere unntak (hvem som slipper gjennom).



Ringelyd

Trykk på dette ikonet for å dempe ringetonen, et nytt trykk deaktiverer også vibreringen. Ideelt for konsert- eller kinobesøk, men også for en uforstyrret natts søvn! Med et langt trykk kommer du direkte til alle voluminnstillingene. Du kan for eksempel slå av lyden på videoer og musikk mens innkommende anrop fortsetter å lage lyd.

2. Enkel bruk av mobile enheter

2.1. Introduksjon og generell informasjon

Ikonene i varslingscenteret



Lommelykt

Dette symbolet slår på blitsfunksjonen i telefonens kamera inntil du trykker på det igjen. Med en smarttelefon har du alltid en lommelykt med deg for å finne et nøkkelhull i mørket eller for å lyse opp en sti bedre.



Innstillinger

Selv om du kan finne enhetens Innstillinger-app et annet sted, er det likevel praktisk med rask tilgang fra varslingscenteret.

2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Bruk taleinndata (tale-til-tekst) og stemmeassistent

Mikrofonikonet ligger på tastaturet eller andre steder i apper og lar deg diktere tekst i stedet for å skrive den inn.



2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Installere en app

Google-konto (Android) eller Apple-ID

- Lås opp enheten og åpne skrivebordet
- Trykk på Play Store (Android) eller App Store (Apple).
- Når butikken åpnes, blir aktuelle og nye apper først anbefalt i ulike kategorier.
- Hvis du vil søke etter en bestemt app, trykker du på søkeikonet (Android: søkefeltet øverst, Apple: søk nederst).
- Skriv inn appens navn eller et søkeord

2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Installere en app

- Hvis du har skrevet inn et generelt søkeord (f.eks.: memory game), får du opp en liste med resultater, og du kan bestemme deg for hvilken du vil ha basert på stjerangeringer og beskrivelser av appene.
- Når du har bestemt deg for en app, trykker du på "Installer" (Android) eller "Last ned" og skriver inn Apple ID-passordet ditt (Apple).
- Deretter installeres appen. Når installasjonen er fullført, kan appen åpnes.
- Når du starter en app for første gang, kan du bli bedt om å gi visse tillatelser. Ta deg tid til å lese gjennom dette for å forstå hvilken informasjon appen vil bruke fra nettbrettet eller hvilke enhetssensorer den ønsker tilgang til.

2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Widgets

Det engelske begrepet "widget" er dannet av "window" for vindu og "gadget" for tilbehørsenhet. Dette er grafiske vinduer på smarttelefonens startskjerm som inneholder en lenke til en app.

I motsetning til app-ikonene tilbyr en widget alltid "mer" informasjon. Værwidgeten viser for eksempel den aktuelle vær-situasjonen og temperaturen på det angitte stedet.

For å legge til en ny widget sveiper du innover med to fingre på den ulåste skjermen, som om du skulle gjøre et bilde mindre.

Det vises nå en knapp nederst som viser alle tilgjengelige widgeter på enheten

Avhengig av hvilken enhet du har, er det bare å trykke på ønsket widget eller dra den til ønsket sted på skjermen.



2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Widgets

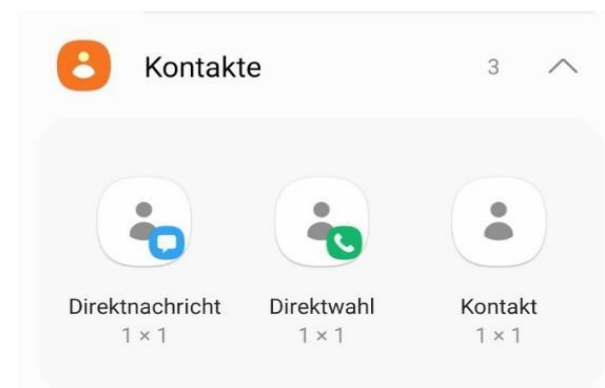
Praktiske widgets, i tillegg til været, søkefeltet og kalenderen, fins det også kontakt-widgets:

Du kan bruke den til å lagre personer fra adresseboken din direkte på startskjermen, enten som hurtigvalg (ved å trykke på den, starter samtalen med en gang), som en direkte melding (SMS til personen starter) eller som en snarvei til kontakten i Kontakter-appen (adresseboken).

Noen widgets er tilgjengelige når du kjøper enheten.

Du kan installere flere via Playstore.

For å gjøre dette er det bare å installere den tilhørende appen.



2. Enkel bruk av mobile enheter

2.2. Praktisk anvendelse, nyttige tips og triks

Ruteplanlegging og navigasjon med smarttelefonen via kartapp (for bil og kollektivtransport)

Batteri



- ✓ Sjekk forbruket (avinstaller "strømslukende" apper)
- ✓ Aktiver strømsparingsmodus om nødvendig, bruk strømbank

Administrere varsler



- ✓ Fjern apptillatelser om nødvendig

3. Workshop Sikker bruk av mobile enheter

3.1 Nettleserinnstillinger

3.2 Type informasjonskapsler

3.3 Virus og trojanske hester

3.4 Tips for å gjøre de mobile enhetene dine trygge

3.5 Nyttige lenker

3. Sikker bruk av mobile enheter



Mobile enheter er lojale følgesvenner i mange situasjoner.

Vi lagrer kontoer, kontakter, data, avtaler, tlagrer opplevelser som bilder og lyd, kommuniserer via ulike apper og utfører banktransaksjoner på nettet.

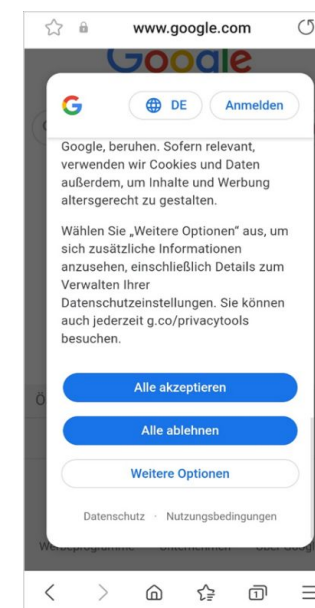
Mye sensitiv informasjon lagres på enhetene våre, og disse må beskyttes.

3. Sikker bruk av mobile enheter

3.1. Innstillinger for nettleser

I mange apper kan du gjøre innstillinger for en lang rekke funksjoner. I en nettleser kan du for eksempel endre startsidene, aktivere eller deaktivere informasjonskapsler og slette lagrede passord. Du finner sannsynligvis innstillingene for nettleserappen i menyen som er skjult bak symbolet med tre streker eller tre prikker.

I sin opprinnelige form er en informasjonskapsel en tekstfil på datamaskinen. Den inneholder vanligvis data om besøkte nettsteder som nettleserprogramvaren lagrer når du surfer på Internett. Siden noe lagres på enheten din, vil du bli informert om det via irriterende popup-vinduer.

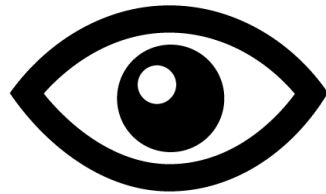


✓ Hvis det finnes et alternativ for å avvise alle informasjonskapsler, kan du velge at alle viktige funksjoner på nettstedet fortsatt skal være aktive.

3. Sikker bruk av mobile enheter

3.2. Typer informasjonskapsler

Informasjonskapsler



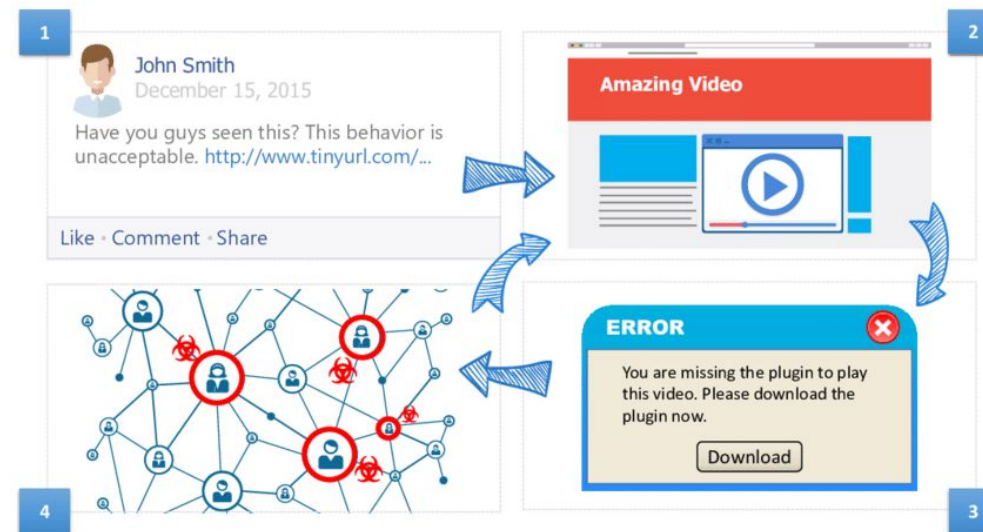
- Det finnes funksjonelle informasjonskapsler som for eksempel brukes for å hindre at du må logge deg inn når du besøker et kryptert nettsted på nytt. Slike informasjonskapsler hjelper også nettsteder med å huske informasjon om besøket ditt, for eksempel foretrukket språk og andre innstillinger. Dette hjelper deg med å finne frem på nettstedet raskere og bruke det mer effektivt neste gang du besøker det.
- Andre informasjonskapsler brukes til å føre statistikk over besøket på nettstedet samt til markedsførings- og PR-formål. Disse har ingen betydning for deg personlig.
- I tillegg finnes det sporingscookies som ikke er begrenset til et bestemt nettsted, men som sporer surfeatferden din for å samle inn informasjon om deg og for bedre å kunne vurdere deg som forbruker. For å beskytte personvernet ditt kan du melde deg av der det er mulig.

3. Sikker bruk av mobile enheter

3.3 Virus og trojanske hester

Nettsteder / Google / Sosiale medier

- For å beskytte deg mot skadelig programvare bør du ikke besøke nettsteder som prøver å selge deg tvilsomme apper med mange popup-vinduer, eller lokke deg til å delta i konkurranser. Målet er ofte å installere skadevare eller spionere på personopplysningene dine.
- Vær forsiktig på sosiale nettverk som Facebook og WhatsApp. Ikke trykk for raskt på lenker eller applikasjoner som lover deg interessante videoer eller bilder, gode tilbud eller kuponger.



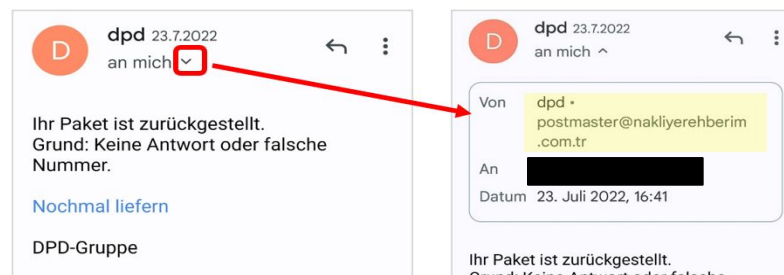
3. Sikker bruk av mobile enheter

3.3 Virus og trojanske hester

E-post

Det er viktig å ikke åpne filvedlegg i e-poster eller chat-meldinger fra personer eller selskaper du ikke kjenner. Kriminelle bruker ofte falske e-poster (f.eks. falske fakturaer) for å få tak i penger eller kontoinformasjon - **phishing**.

✓ Sjekk alltid avsenderens e-postadresse før du trykker på knapper eller lenker i e-postmeldingen.



Merk falske e-poster som søppelpost og slett dem **umiddelbart**.

3. Sikker bruk av mobile enheter



3.3 Virus og trojanske hester

E-post

Du kan bruke en ekstra e-postadresse i stedet for hovedadressen din til abonnementer, bestillinger osv. på Internett. For å gjøre dette kan du opprette en gratis e-postadresse hos leverandører som Gmail eller gmx, der det ikke er så irriterende hvis innboksen din oversvømmes av tvilsomme e-poster.

Hver gang du oppgir e-postadressen din på nettet, øker du risikoen for å motta uønskede og dermed falske e-poster.

3. Sikker bruk av mobile enheter



3.3 Virus og trojanske hester

Oppdatering av operativsystem og apper

- Generelt bør du bare installere apper fra Playstore, ellers kan det ikke utelukkes at de inneholder skjult skadelig programvare.
- Kriminelle utnytter sikkerhetshull i operativsystemer og apper til å utføre målrettede angrep mot ofrene sine. Det hjelper dem at mange internettbrukere ikke holder programvaren oppdatert. Dette til tross for at det allerede finnes oppdateringer som fikser sikkerhetshullene.

3. Sikker bruk av mobile enheter

3.3 Virus og trojanske hestekreps

Oppdatering av operativsystem og apper

Noen apper er rene dataspioner - vær skeptisk hvis for eksempel en enkel lommelykt-app vil ha tilgang til din nåværende posisjon, telefonboken osv. Denne informasjonen bør ikke være relevant for bruk av lommelykt!



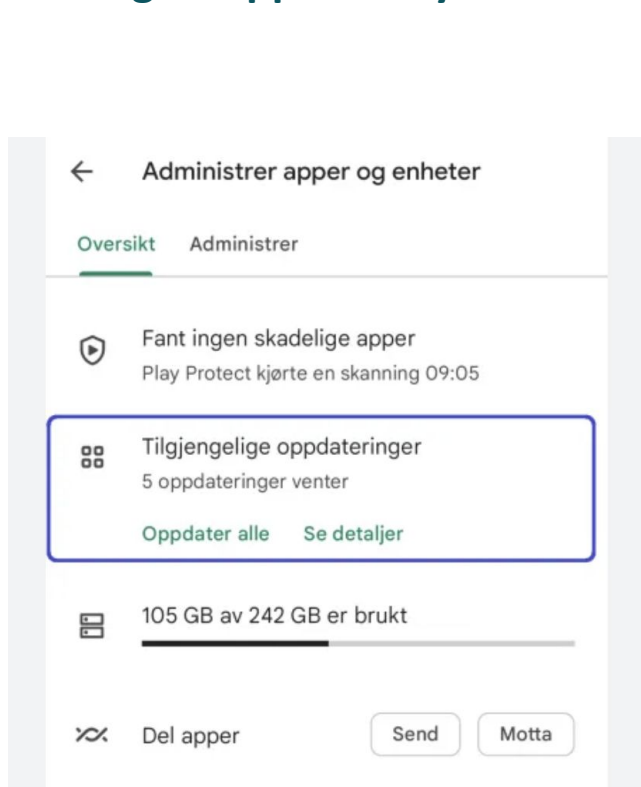
- ✓ Gjør regelmessige appoppdateringer og slett apper som ikke lenger er i bruk.
- ✓ Normalt sender operativsystemet et varsel så snart oppdateringer er tilgjengelige.

For å oppdatere apper manuelt åpner du PlayStore (Android) eller AppStore (iOS).

3. Sikker bruk av mobile enheter

3.3 Virus og trojanske hestekreps

Manuell oppdatering av apper i PlayStore



3. Sikker bruk av mobile enheter

3.3 Virus og trojanske hestekreps

Bruk antivirus-apper

For å oppdage og fjerne skadelig programvare anbefales det å installere et antivirusprogram eller aktivere det i innstillingene. Dette har den fordelen at alle prosesser kan undersøkes i bakgrunnen og farer kan identifiseres og elimineres. Alle antivirusprogrammer tilbyr automatisk oppdatering, noe du absolutt bør bruke.



3. Sikker bruk av mobile enheter

3.4. Tips for å gjøre mobilenhetene dine trygge

Lås mobilenheten (innstillingsappen)



- ✓ Bruk av PIN-kode, passord, -mønster eller biometriske opplåsingsalternativer beskytter dataene på din mobile enhet
- ✓ Installer en skjermlås for å beskytte enheten din mot uautorisert tilgang på din innstillinger og bruksområder

Bruk sterke passord



- ✓ Sikre passord består av en kombinasjon av bokstaver (helst store og små bokstaver og små bokstaver), tall og spesialtegn
- ✓ Jo lengre passordet er, desto sikrere er det (bedre 14 enn 8 tegn).
- ✓ Bruk minst to forskjellige passord: konto og en eller flere for alle andre applikasjoner
- ✓ Bruk en passordadministrator-app for å administrere flere passord på en sikker måte og for å slippe å lære dem utenat

3. Sikker bruk av mobile enheter

3.4. Tips for å gjøre mobilenhetene dine trygge

Hold personlige tilgangsinformasjon (f.eks. PIN-kode, passord) hemmelige.

Vær forsiktig når du bruker offentlige enheter



- ✓ Hvis du har logget inn på et bestemt nettsted (f.eks. en e-postleverandør, et sosialt nettverk) på en annens enhet, bør du alltid logge deg ut.
- ✓ Ikke la fremmede se deg over skulderen når du legger inn personlig informasjon.

Installere oppdateringer

Oppdateringer gir nye funksjoner og tetter sikkerhetshull, og operativsystemet varsler når oppdateringer er tilgjengelige.



- ✓ Installer oppdateringer umiddelbart eller
- ✓ Aktivere automatiske oppdateringer på enheten

3. Sikker bruk av mobile enheter

3.3. Tips for å gjøre mobilenhetene dine trygge

Last bare ned apper fra leverandørens offisielle appbutikk.

Kontroller tillatelser

Apper trenger ulike autorisasjoner (f.eks. tilgang til mikrofon, kontakter, Internett).



✓ Kontroller og tilpass tillatelsene for appene dine

Deaktiver tjenester

Mobile enheter kan utveksle data via ulike tjenester. Apper kan for eksempel bestemme posisjon og opprette bevegelsesprofiler via GPS og WiFi-nettverk.



✓ Aktiver Wi-Fi, Bluetooth og GPS bare når det er nødvendig.

3. Sikker bruk av mobile enheter

3.3. Tips for å gjøre mobilenhetene dine trygge

Håndter pasientenes og organisasjonens data med forsiktighet.



- ✓ Ikke overfør data via offentlige WiFi-nettverk (f.eks. helseapper)
- ✓ Ta hensyn til GDPR og handle deretter

Regelmessige sikkerhetskopier

Hvis du mister mobilenheten din, den blir stjålet eller ødelagt, er alle dataene dine borte - med mindre du sikkerhetskopierer dem regelmessig.



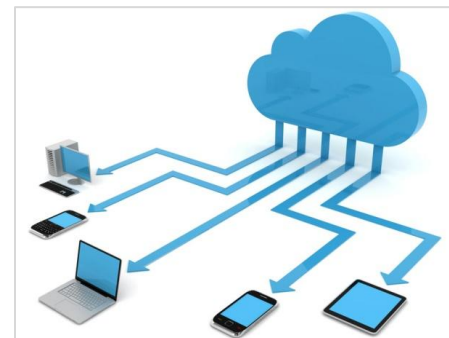
- ✓ Overfør data til en datamaskin via kabel
- ✓ Bruk en skytjeneste for sikkerhetskopiering av data, og aktiver automatisk synkronisering for kritiske data.

3. Sikker bruk av mobile enheter

3.3. Tips for å gjøre mobilenhetene dine trygge

Regelmessige sikkerhetskopier

Hvis du mister mobilenheten din, den blir stjålet eller ødelagt, er alle dataene dine borte - med mindre du sikkerhetskopierer dem regelmessig.



- ✓ Overfør dataene dine til en datamaskin via kabel (USB), innstillingene vises på skjerm for mobilenhet - gi tilgang via datamaskin
- ✓ Bruk en skytjeneste for sikkerhetskopiering av data, og aktiver automatisk synkronisering for kritiske data.
data / mapper (leverandører: Dropbox, Google , Apple, Microsoft,)

3. Sikker bruk av mobile enheter

3.3. Tips for å gjøre mobilenhetene dine trygge

Installer antivirusprogramvare



- ✓ Hold alltid antivirusprogrammet oppdatert, slik at nye trusler oppdages og forebygges

Aktivere tyveribeskyttelse

Det finnes ingen app som beskytter mobilenheten din mot tyveri, men det finnes programmer som gjør det lettere å finne den. Denne "tyverisikringsappen" kan fjernlokalisere den tapte eller stjålne enheten, låse den eller til og med slette data. Den er ofte inkludert i antivirusprogramvare.



- ✓ Installer eller aktiver tyverisikringsapp/-funksjon og aktiver GPS på enheten.
- ✓ Noter deg serienummeret til smarttelefonen din (IMEI-nummeret), i fall du vil anmelde et eventuelt tyveri

3. Sikker bruk av mobile enheter

3.3 Tips for å gjøre de mobile enhetene dine trygge

Slik finner du serienummeret til smarttelefonen din (IMEI-nummer)



- ✓ Android-smarttelefon - Innstillinger → på telefonen
- ✓ iPhone - Innstillinger → Generelt → Info
- ✓ *Eller:* Tast inn følgende kode på telefonens numeriske tastatur: *#06#

3. Sikker bruk av mobile enheter



3.5. Nyttige lenker

Denne lenkesamlingen fungerer som et eksempel og må tilpasses i det enkelte partnerland.

https://www.forbrukertilsynet.no/vi-jobber-med/netthandel/avslor-nettsvindel	Innformasjon om nettsvindel
https://www.politiet.no/rad/beskytt-deg-mot-svindel-og-id-tyveri/	Informasjonsplattform om internettsvindel og svindelliknende nettfeller i Norge

Takk for din deltakelse og dine ideer!

