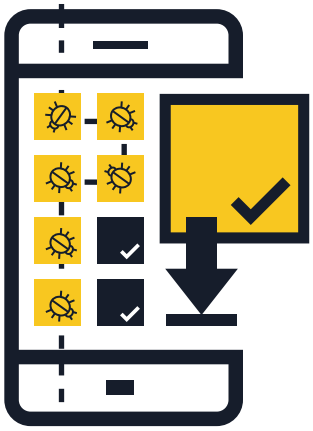
SKADEVARE PÅ MOBILEN

TIPS OG RÅD FOR Å BESKYTTE DEG SELV

1 Installer kun apper fra betrodde kilder



- **Last ned apper fra de offisielle butikkene** — Undersøk både appen og dens utgivere før nedlasting. Vær forsiktig med lenker du mottar på e-post og tekstmeldinger som kan lure deg til å installere apper fra tredjeparter eller ukjente kilder.
- **Sjekk andre brukeres vurderinger** hvis tilgjengelig.
- **Les appens tillatelser** — Sjekk hvilke typer data appen har tilgang til, og om den kan dele informasjonen din med eksterne parter. Hvis du er skeptisk eller ukomfortabel med vilkårene, ikke last ned appene.

2 Ikke klikk på lenker eller vedlegg i uventede e-poster eller tekstmeldinger

- **Ikke stol på lenker i uventede e-poster eller tekstmeldinger** (SMS og MMS) — Slett dem så snart du mottar dem.
- **Dobbeltsjekk forkortede URL-er og QR-koder** — de kan føre deg til skadelige nettsider eller direkte nedlasting av skadevare til enheten din. Før du klikker, bruk en URL-forhåndsvisningsside for å bekrefte at nettadressen er legitim. Før du skanner en QR-kode, velg en QR-leser som forhåndsviser den innebygde nettadressen og bruk mobilsikkerhetsprogramvare som advarer deg om risikable lenker.

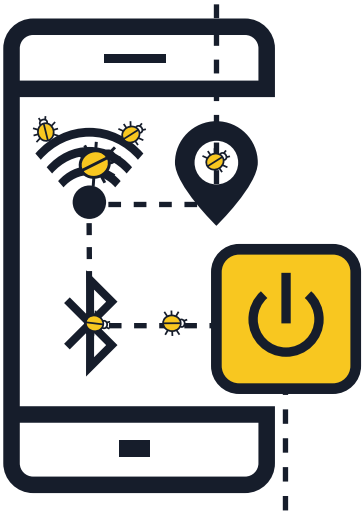
3 Logg ut av sider etter at du har foretatt en betaling

- **Lagre aldri brukernavn og passord i mobilnettleseren din eller apper** — Hvis du mister eller blir frastjålet telefonen eller nettbrettet, kan hvem som helst logge på kontoene dine. Så snart transaksjonen er fullført, logg ut av siden istedenfor bare å lukke nettleseren.
- **Unngå å bruke banktjenester eller å handle på nett ved hjelp av åpne trådløse nett** — Utfør kun banktjenester og transaksjoner fra nettverk du kjenner og stoler på.
- **Dobbeltsjekk sidens URL** — Påse at nettadressen er korrekt før du logger inn eller sender sensitiv informasjon. Vurder å laste ned din banks offisielle app for å sikre at du alltid er koblet til den ekte siden.

4 Hold operativsystemet og apper oppdatert

- **Last ned oppdateringer for din mobilenhets operativsystem så snart du blir bedt om det** — Har du de nyeste oppdateringene, sikrer det at enheten din ikke bare er mer sikker, men også yter bedre.

5 Slå av WiFi, stedtjenester og Bluetooth når de ikke er i bruk



- **Slå av WiFi hvis du ikke bruker det** — Cyberkriminelle kan få tilgang til informasjonen din hvis tilkoblingen ikke er sikker. Hvis det er mulig, bruk en 3G- eller 4G-tilkobling istedenfor åpne trådløse nettverk. Du kan også velge en virtuell privat nettverk-tjeneste (VPN) slik at dataene dine er krypterte når de sendes.
- **Ikke la apper bruker stedtjenestene dine med mindre de må det** — Denne informasjonen kan deles eller lekkes og bli brukt til å vise annonser basert på hvor du befinner deg.
- **Slå av Bluetooth når du ikke trenger det** — Påse at det er slått helt av og ikke bare i usynlig modus. Standardinnstillingene er ofte forhåndsinnstilte for å la andre koble seg til enheten din uten din viten. Ondsinnede brukere kan potensielt kopiere filene dine, få tilgang til andre enheter som er tilkoblet eller til og med få ekstern tilgang til telefonen din for å foreta anrop og sende tekstmeldinger, noe som fører til dyre regninger.

6 Unngå å oppgi personlig informasjon

- **Svar aldri med personlig informasjon** på e-poster eller tekstmeldinger som utgir seg for å være fra banken din eller annen legitim virksomhet. Kontakt isteden virksomheten direkte for å bekrefte forespørselen.
- **Gå regelmessig gjennom mobilutskriftene dine for å se etter noen mistenkelige gebyrer** — Hvis du identifiserer utgifter som du ikke står bak, kontakt tjenesteleverandøren din umiddelbart.

7 Ikke jailbreak enheten din

- Jailbreaking er prosessen der man fjerner sikkerhetsbegrensningene påtvunget av operativsystemselgeren, og som gir full tilgang til operativsystemet og funksjonene. **Jailbreaking av din egen enhet kan betydelig svekke dens sikkerhet,** og åpner sikkerhetshull som ellers ikke er åpenbare/tilgjengelige.

8 Sikkerhetskopier dataene

- **Mange smarttelefoner og nettbrett har mulighet for å ta sikkerhetskopi trådløst** — Se på alternativene avhengig av din enhets operativsystem. Ved å opprette en sikkerhetskopi for din smarttelefon eller ditt nettbrett kan du enkelt gjenopprette dine persondata hvis enheten noen gang forsvinner, blir stjålet eller skadet.

9 Installer en app for mobilsikkerhet

- Alle operativsystemer står i fare for infeksjon. Hvis tilgjengelig, **bruk en mobilsikkerhetsløsning** som oppdager malware, spyware og ondsinnede apper, i tillegg til andre personverns- og tyverisikringsfunksjoner.

EUROPOL EC3 European Cybercrime Centre | POLITIET KRIPOS - NCIS NORWAY | CCIS | NTNU Norwegian University of Science and Technology | NorSIS Norsk senter for informasjonssikring

#MobileMalware