



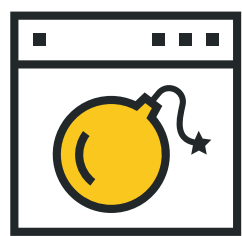
LØSEPENGEVIRUS PÅ MOBILEN

SI FARVEL TIL DINE PERSONLIGE FILER

Løsepengevirus holder mobilenheten og informasjonen på den gissel mot betaling. Denne typen malware låser enhetens skjerm eller forhindrer deg i å få tilgang til noen av filene og funksjonene.



HVORDAN SPRES DET?



Besøke kompromitterte nettsider.

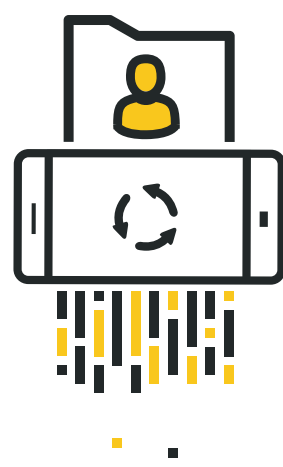


Laste ned falske versjoner av legitime apper.



Klikke på ondsinnede lenker og vedlegg i phishing-e-poster.

HVA ER RISIKOEN?



Du må kanskje tilbakestille enheten din, og miste alle dataene.



En angriper kan ha full tilgang til enheten din og kan dele dataene dine med tredjeparter.

HVA KAN DU GJØRE?



Sikkerhetskopier dataene dine hyppig og hold alle appene og operativsystemene dine oppdaterte.



Unngå å handle i tredjeparts appbutikker.



Hvis tilgjengelig, installer en App for mobilsikkerhet som vil varsle deg hvis enheten din har blitt kompromittert.



Vær skeptisk til e-poster og nettsider som ser mistenkelige ut eller høres for godt ut til å være sant.



Ikke bevilg administratorrettigheter til alle.



Ikke betal løsepengene. Du finansierer kriminelle og oppfordrer dem til å fortsette deres ulovlige aktiviteter.