APPS

BARE ET SPIL?

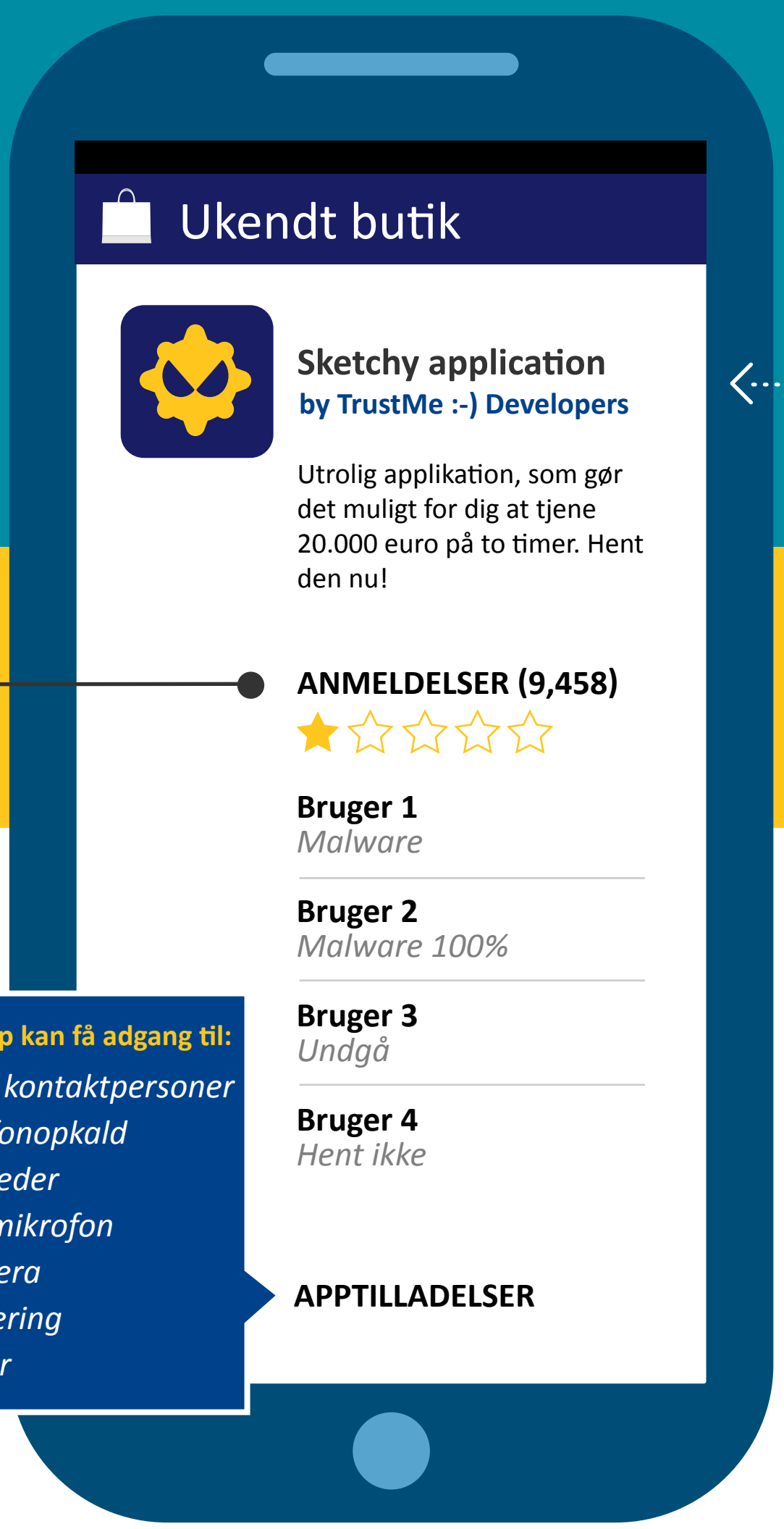
Installer kun apps fra officielle appbutikker

Før du henter en app, skal du undersøge både appen og dens udgivere. Vær forsigtig med links, som du modtager via mails og sms'er, da de kan lokke dig til at installere apps fra tredjeparter eller ukendte kilder.

LÆS SÅ VIDT MULIGT ANMELDELSER OG VURDERINGER FRA ANDRE BRUGERE

LÆS APPENS TILLADELSER

Kontrollér, hvilke slags data appen kan få adgang til, og om den kan dele dine oplysninger med eksterne parter. Kræver appen alle disse tilladelser? Lad være med at hente appen, hvis den gør det.



INSTALLER EN MOBILSIKKERHEDSAPP

Den undersøger alle apps på enheden og hver ny app, som du installerer på et senere tidspunkt, og den giver dig besked om, hvis der findes skadelig software.

EUROPOL EC3 European Cybercrime Centre

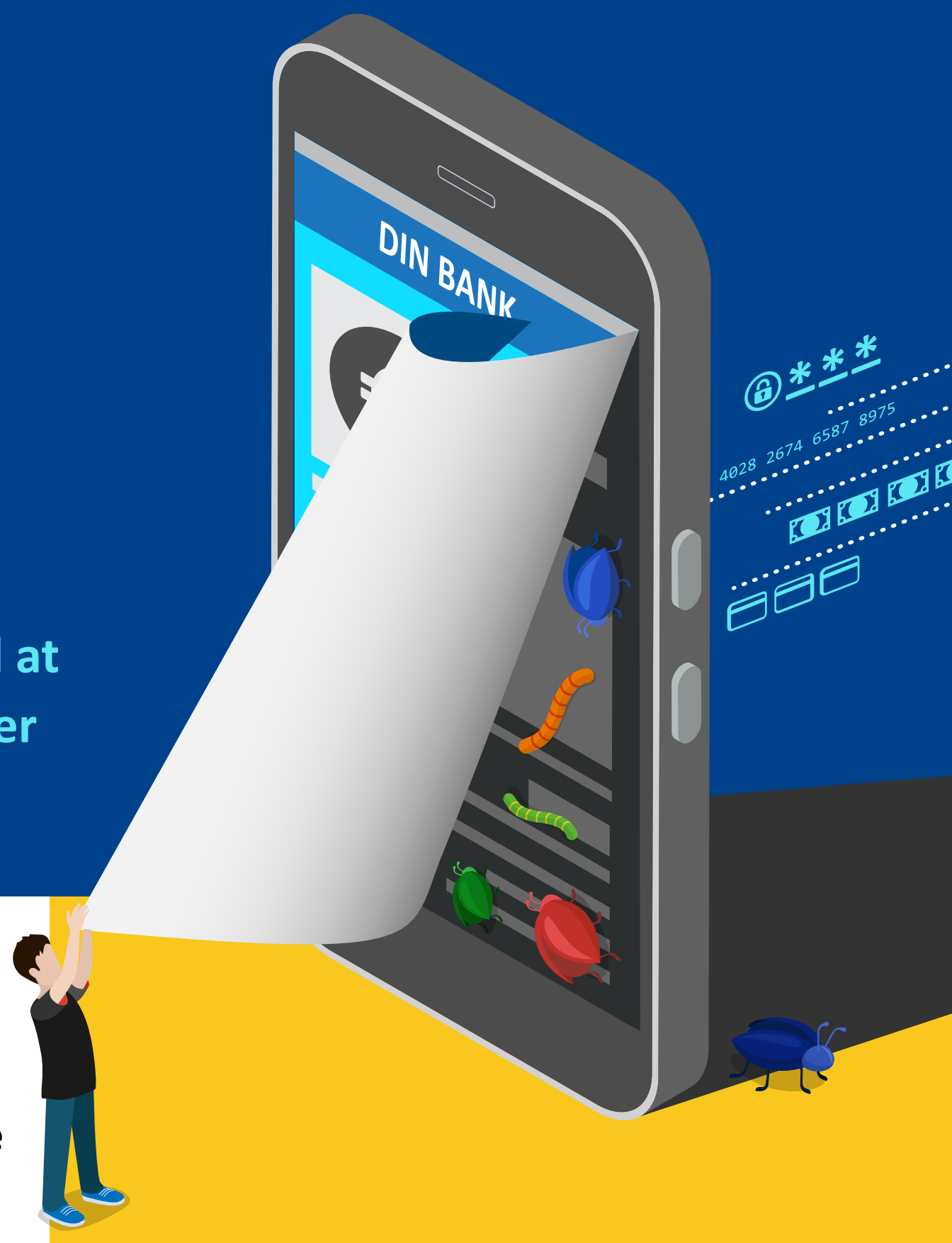
POLITI

#MobileMalware

MOBILBANK-MALWARE

MALWARE KAN KOSTE PENGE

Mobilbank-malware er beregnet til at stjæle de finansielle oplysninger, der er lagret på din enhed.



HVORDAN SPREDES DEN?

Ved at besøge ondsindede websteder

Ved at hente skadelige apps

Ved hjælp af phishing

HVAD ER RISICIENE?

Indsamling af dine personlige godkendelsesoplysninger

Uautoriseret hævning

HVAD KAN MAN GØRE?

https://

Hent din banks officielle mobilapp, og kontrollér, at du besøger det ægte bankwebsted hver gang.

Undgå at blive logget på automatisk af dit online bankwebsted eller bankapp.

Lad være med at dele eller videregive dit bankkortnummer eller -adgangskode til nogen.

Installer så vidt muligt en mobilsikkerhedsapp, som giver dig besked om al mistænkelig aktivitet.

Hvis du mister din mobiltelefon eller skifter nummer, skal du kontakte din bank, så de kan opdatere dine oplysninger.

Del ikke oplysninger om din konto via sms eller mail.

Brug altid et sikkert wi-fi-netværk, når du opretter forbindelse til din banks mobilwebsted eller app. Gør det aldrig fra et åbent wi-fi-netværk!

Kontrollér ofte dine bankudskrifter.

EUROPOL EC3 European Cybercrime Centre

POLITI

#MobileMalware

MOBIL-RANSOMWARE

SIG FARVEL TIL DINE PERSONLIGE FILER

Ransomware tager din mobilenhed og -data som gidsel for en pris. Denne slags malware låser din enheds skærm eller forhindrer dig i at få adgang til nogle af filerne og funktionerne.

HVORDAN SPREDES DEN?

Ved at besøge risikofyldte websteder.

Ved at hente falske versioner af legitime apps.

Ved at klikke på skadelige links og vedhæftede filer, der er integreret i phishing-mails.

HVAD ER RISICIENE?

Du skal muligvis nulstille din enhed til fabriksindstillinger, hvilket medfører tab af alle dine data.

En angriber kan få fuld adgang til din enhed og dele dine data med tredjeparter.

HVAD KAN MAN GØRE?

Sikkerhedskopiér ofte dine data, og hold alle dine apps og operativsystemet opdateret.

Lad være med at købe i appbutikker fra tredjeparter.

Installer så vidt muligt en mobilsikkerhedsapp, som giver dig besked, hvis din enhed er bragt i fare.

Hold øje med mails og websteder, der ser mistænkelige ud eller lyder for gode til at være sande.

Giv ingen person administratorrettigheder til enheden.

Betal ikke løsepenge. Du finansierer så forbrydere og tilskynder dem til at fortsætte med deres ulovlige aktiviteter.

EUROPOL EC3 European Cybercrime Centre

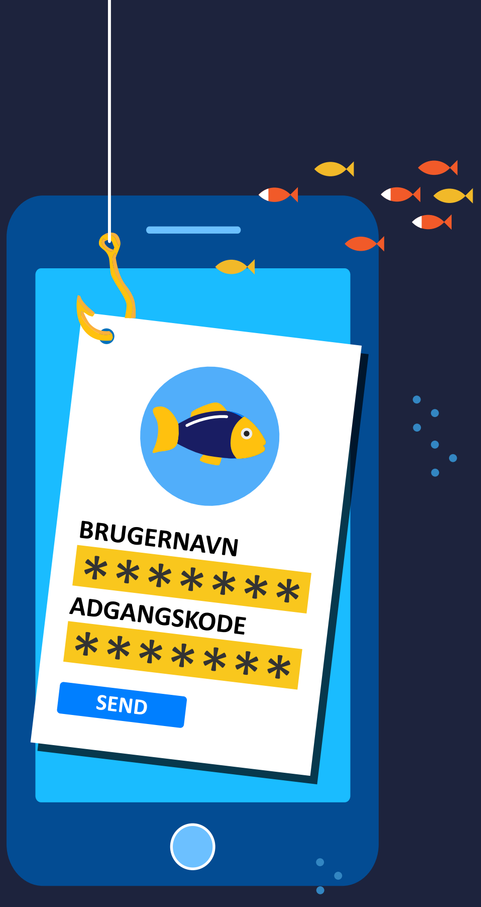
POLITI

#MobileMalware

WEBBASEREDE TRUSLER

KIG TO GANGE, FØR DU KLIKKER

Du kan tabe dine penge, dine personlige oplysninger og endda dine lagrede data, hvis enheden holder op med at fungere. Don't get hooked!



HVORDAN KAN DET SKE?

PHISHING-ANGREB: De lokker brugere til at opgive personlige oplysninger ved at optræde som en pålidelig enhed. De spreder sig via mail, sms eller sociale medieplatforme.

BROWSING AF WEBSTEDER: Din mobilenhed kan inficeres ved simpelthen at besøge et usikkert websted.

FILOVERFØRSEL: Skadelige links og vedhæftede filer kan være direkte integreret i en mail.

HVORFOR ER DET EFFEKTIVT?

Mobilenheder har **KONSTANT FORBINDELSE** til internettet.

ENHEDERNES REDUCEREDE SKÆRMSTØRRELSE er en generel begrænsning. Mobilbrowsere viser webadresser på begrænset skærmplads, hvilket gør det svært at se, om domænet er legitimt.

BRUGERENS ABSOLUTTE TILLID grundet den personlige karakter en mobilenhed har.

HVAD KAN MAN GØRE?

Vær mistænksom, hvis du modtager en sms eller et telefonopkald fra en virksomhed, der beder om personlige oplysninger. Du kan bekræfte, om meddelelsen/opkaldet er legitimt ved at ringe direkte til virksomheden på deres officielle nummer.

https://

Når du browser på nettet på din mobilenhed, skal du kontrollere, at din forbindelse er sikret via HTTPS. Du kan altid kontrollere det i starten af webadressen.

Klik aldrig på et link/en vedhæftet fil i en uopfordret mail eller sms. Slet den øjeblikkeligt.

^BE:%}
W@RY
*)Z#$=

Vær på vagt, hvis du lander på et websted, der har dårlig grammatik, stavefejl eller lav opløsning.

Installer så vidt muligt en mobilsikkerhedsapp, som giver dig besked om al mistænkelig aktivitet.

EUROPOL EC3 European Cybercrime Centre

POLITI

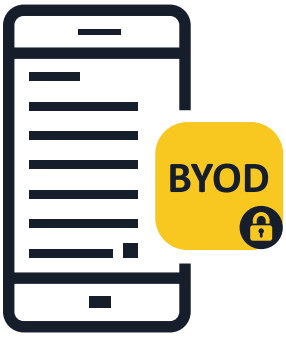
#MobileMalware

MOBILMALWARE

TIPS OG RÅD TIL VIRKSOMHEDER

1 Informer personalet om mobilrisici

- Mobilarbejde udvisker grænserne mellem virksomheds- og personlig brug. Virksomheder kan påvirkes alvorligt af et angreb, der i første omgang rettes mod en persons mobilenhed. En mobilenhed er en computer og skal beskyttes ligesom en.



2 Implementér en BYOD-politik (Bring-Your-Own-Device) i hele virksomheden

- Medarbejdere, der bruger deres egne mobilenheder til at få adgang til virksomhedsdata og -systemer (selvom det kun er e-mail, kalender eller database over kontaktpersoner) skal følge virksomhedspolitikken. Vælg omhyggeligt, hvilke teknologier der bliver brugt til at styre og sikre mobilenheder, og tilskynd personalet til at udøve forsigtighed.

3 Inkluder en politik for mobilsikkerhed som en del af din generelle sikkerhedsmæssige ramme

- Hvis en enhed ikke overholder sikkerhedspolitikken, må den ikke få tilladelse til at oprette forbindelse til virksomhedsnetværket og få adgang til virksomhedsdata. Virksomheder bør installere deres egne MDM- (administration af mobilenheder (Mobile Device Management)) eller EMM-løsninger (administration af virksomhedsmobilitet (Enterprise Mobility Management)).
- Det er meget vigtigt at installere en MTD-løsning (forsvar mod mobiltrusler (Mobile Threat Defence)) for at supplere dette. Dette giver forbedret synlighed og viden om trusler mod applikationer, netværk og operativsystem.

4 Vær forsigtig ved brug af offentlige wi-fi-netværk til at få adgang til virksomhedsdata

- Generelt er offentlige wi-fi-netværk ikke sikre. Hvis en medarbejder får adgang til virksomhedsdata ved hjælp af en gratis wi-fi-forbindelse på et lufthavn eller en café, kan dataene udsættes for ondsindede brugere. Virksomheder anbefales i denne forbindelse at udvikle en effektiv brugspolitik.

5 Hold enheders operativsystem og apps opdaterede

- Anbefal dit personale at hente softwareopdateringer til deres mobilenheds operativsystem, så snart de bliver bedt om det. Vær bekendt med opdateringspolitikken for især Android, netværksudbydere og mobilproducenter. At have de seneste opdateringer sikrer, at enheden ikke blot er sikrere, men også at den har en bedre præstation.

6 Installer apps udelukkende fra kilder, du har tillid til

- Virksomheder bør kun tillade installationen af apps fra officielle kilder på de mobilenheder, der opretter forbindelse til virksomhedsnetværket. Overvej alternativt at bygge en appbutik til virksomhedsbrug, som slutbrugere kan få adgang til, hente og installere virksomhedsgodkendte apps. Spørg din sikkerhedsleverandør om råd til opsætning af samme, eller byg internt din egen.

7 Jailbreaking skal forhindres

- Jailbreaking er processen for fjernelse af sikkerhedsbegrænsningerne, der er pålagt af operativsystemets leverandør for at få fuld adgang til operativsystemet og funktionerne. Hvis du jailbreaker din egen enhed, svækker du dens sikkerhed ved at åbne sikkerhedshuller, der ikke umiddelbart har været synlige. Enheder, der kan rodfæstes, må ikke tillades i virksomhedsmiljøet.

8 Overvej skylager som alternativ

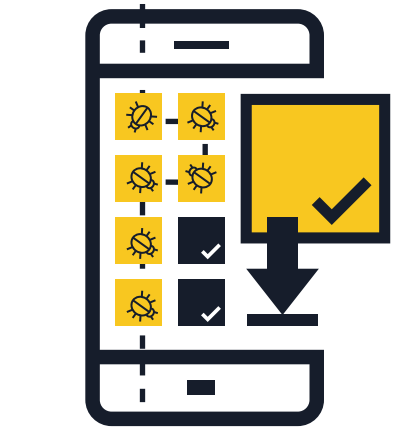
- Mobilbrugere ønsker ofte at få adgang til vigtige dokumenter, ikke kun via deres computere, men også fra deres private telefoner eller tablets, når de er væk fra kontoret. Virksomheder skal vurdere bygning af et sikkert skybaseret lager og tjenester til filsynkronisering for forsvarligt at imødekomme sådanne behov.

9 Tilskynd personalet til at installere en mobilsikkerhedsapp

- Alle operativsystemer risikerer at blive inficeret. Kontrollér så vidt muligt, at de bruger en mobilsikkerhedsløsning, der finder og forhindrer malware, spyware og skadelige apps, sammen med andre tyverisikringsfunktioner og funktioner til beskyttelse af personlige oplysninger.

MOBILMALWARE

TIPS OG RÅD TIL AT BESKYTTE DIG SELV



1 Installer apps udelukkende fra kilder, du har tillid til

- **Køb i velkendte appbutikker** — Før du henter en app, skal du undersøge både appen og dens udgivere. Vær forsigtig med links, som du modtager via mails og sms'er, da de kan lokke dig til at installere apps fra tredjeparter eller ukendte kilder.
- **Læs så vidt muligt anmeldelser og vurderinger fra andre brugere** hvis tilgængelig.
- **Læs appens tilladelser** — Kontrollér, hvilke slags data appen kan få adgang til, og om den kan dele dine oplysninger med eksterne parter. Hvis du er mistænksom eller føler dig utilpas med vilkårene, må du ikke hente appen.

2 Klik ikke på links eller vedhæftede filer i uopfordrede mails eller sms'er

- **Du må ikke stole på links i uopfordrede mails eller sms'er (SMS og MMS)** — Slet dem, så snart du modtager dem.
- **Dobbeltkontrollér forkortede webadresser og QR-koder** — de kan føre dig til skadelige websteder eller hente malware direkte til enheden. Før du klikker, skal du bruge en webadresses eksempelwebsted til at bekræfte, at webadressen er legitim. Inden du scanner en QR-kode, skal du vælge en QR-læser, der giver et eksempel på den integrerede webadresse, og bruge mobilsikkerhedssoftware, der advarer dig om risikofyldte links.

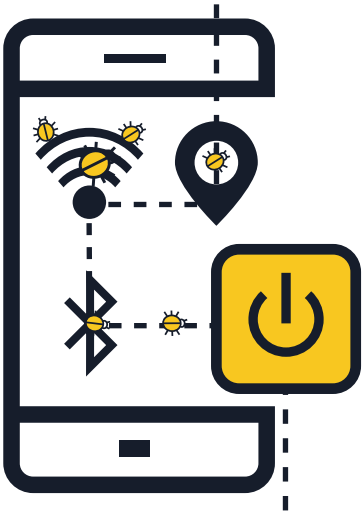
3 Log af websteder, når du har udført en betaling

- **Du må aldrig gemme brugernavne og adgangskoder i mobilbrowseren eller appsene** — Hvis du mister telefonen eller tabletten, eller den bliver stjålet, kan enhver person logge på dine konti. Når transaktionen er udført, skal du logge af webstedet i stedet for blot at lukke browseren.
- **Man må ikke bruge netbank eller købe online ved hjælp af offentlige wi-fi-forbindelser** — Du må kun bruge netbank og udføre onlinetransaktioner på netværk, som du kender godt og har tillid til.
- **Dobbeltkontrollér webstedets webadresse** — Kontrollér, at webadressen er korrekt, før du logger på eller sender følsomme oplysninger. Overvej at hente din banks officielle app for at sikre, at du altid opretter forbindelse til det ægte websted.

4 Hold dit operativsystem og dine apps opdaterede

- **Hent softwareopdateringer til din mobilenheds operativsystem, så snart du bliver bedt om det** — At have de nyeste opdateringer er med til at sikre, at din enhed ikke kun er sikrere, men også at den har en bedre præstation.

5 Slå wi-fi, placeringstjenester og Bluetooth fra, når de ikke er i brug



- **Slå wi-fi fra, hvis du ikke bruger det** — Cyberforbrydere kan få adgang til dine oplysninger, hvis forbindelsen ikke er sikre. Brug så vidt muligt en 3G- eller 4G-dataforbindelse i stedet for hotspots. Du kan også bruge en VPN-tjeneste (virtuelt, privat netværk) til at holde dine data krypterede, når de overføres.
- **Giv ikke apps tilladelse til at bruge dine placeringstjenester, medmindre de skal gøre det** — Disse oplysninger kan deles eller lækkes og bruges til at skubbe annoncer på grundlag af din placering.
- **Slå Bluetooth fra, når du ikke skal bruge det** — Kontrollér, at det er slået fuldstændig fra og ikke kun i usynlig tilstand. Standardindstillingerne er ofte forudindstillet til at give andre tilladelse til at oprette forbindelse til din enhed uden dit vidende. Ondsindede brugere kan muligvis kopiere dine filer, få adgang til andre tilknyttede enheder eller endda få fjernadgang til din telefon for at foretage opkald og sende sms'er, hvilket medfører dyre regninger.

6 Lad være med at oplyse dine personlige oplysninger

- **Man må aldrig svare med personlige oplysninger** på sms'er eller e-mails, der påståes at være fra din bank eller en anden legitim forretning. Kontakt i stedet forretningen direkte for at bekræfte deres anmodning.
- **Gennemgå regelmæssigt dine mobiludskrifter for at kontrollere for evt. mistænkelige gebyrer** — Hvis du identificerer udgifter, som du ikke har betalt, skal du straks kontakte din tjenesteudbyder.

7 Lad være med at jailbreake din enhed

- Jailbreaking er processen for fjernelse af sikkerhedsbegrænsningerne, der er pålagt af operativsystemets leverandør for at få fuld adgang til operativsystemet og funktionerne. — **Hvis du jailbreaker din egen enhed, svækker du dens sikkerhed** ved at åbne sikkerhedshuller, der ikke umiddelbart har været synlige.

8 Sikkerhedskopiér dine data

- **Mange smartphones og tablets kan trådløst sikkerhedskopiere data** — Spørg om valgmulighederne alt efter enhedens operativsystem. Ved at oprette en sikkerhedskopi til din smartphone eller tablet kan du let gendanne dine personlige data, hvis du mister enheden, eller den bliver stjålet eller beskadiget.

9 Installer en mobilsikkerhedsapp

- Alle operativsystemer risikerer at blive inficeret. Brug så vidt muligt **en mobilsikkerhedsløsning,** der finder og forhindrer malware, spyware og skadelige apps, sammen med andre tyverisikringsfunktioner og funktioner til beskyttelse af personlige oplysninger.