Anbefalinger til **mobil sikkerhed**

Gode råd inden for:

- Malware- og virusangreb
- Adgang
- Indholdspolitik
- Netværkssikkerhed
- Datahåndtering
- Privatliv

telenor erhverv

Malware- og virusangreb

Hold enheder opdateret

De mobile enheder bør ikke anvende et styresystem, som ikke længere opdateres af producenten. Vær derfor varsom med at bruge ældre enheder. Kontrollér regelmæssigt, om der er opdateringer - både til styresystem og til installerede apps. Slå altid automatiske opdateringer til, når det er muligt.

Opdateringer er vigtige, både i forhold til at lukke sikkerhedshuller, men det kan også være en forudsætning for at kunne anvende nogle apps og funktioner.

De digitale trusler udvikles og ændres hele tiden, men med automatiske opdateringer sikrer I den nyeste beskyttelse på jeres mobile enheder.

En Mobile Device Management-løsning kan også give jer den fulde kontrol over software og opdateringer på alle jeres mobile enheder.

Lad jer ikke narre

Vores adfærd som brugere af mobile enheder udgør det svageste led over for digitale trusler. Risikoen er stor for virksomheder af alle størrelser. Angrebsmetoderne udvikler sig hurtigt, og i en travl hverdag kan det være virkelig vanskeligt at have opmærksomhed på viden om nye trusler.

Der er mange måder at blive snydt gennem mails, sms'er, telefonopkald fra, hvad der ligner pålidelige numre, falske profiler osv. Det er derfor vigtigt, at I holder jer opdateret omkring de forskellige metoder, IT-kriminelle anvender.

Adgang

Adgangskoder

Det mest grundlæggende, I kan gøre for at sikre jeres mobile enheder og dermed den information, der ligger derpå, er at kræve en adgangskode. Mobiler og tablets giver ofte adgang til mails, arbejdsrelaterede apps, og I bruger dem måske også som ekstra sikkerhed til to-faktor-godkendelse.

I og jeres medarbejdere skal derfor vælge en god, sikker kode. Koden skal være svær at gætte – selv for folk, der kender jer godt. Brug ikke den samme kode til jeres private enheder og arbejdsenheder. I kan vælge en stærkere type password i enhedernes indstillinger, der fx består af både tal og bogstaver.

Med en Mobile Device Management-løsning forbedres sikkerheden, idet I fx kan styre, at alle enheder skal være beskyttet med adgangskode. I kan også stille krav til kodens kompleksitet samt hvor ofte, den skal fornyes.

Uvedkommende smugkig

Vær varsom med, hvor I bruger jeres mobile enheder, så uvedkommende ikke kan opsnappe informationer om jer eller jeres arbejde. Mobile enheder har tendens til at få os til at føle, at vi er i et "privat rum", men står du i metroen eller sidder i et fly eller tog, er det nemt for andre at få et glimt af dine aktiviteter. Her kan et privacy cover være en god investering.

Ligger den mobile enhed tilgængelig et sted, hvor andre kan se den, kan notifikationer også afsløre meget. Det er en god idé, at slå dette fra for hver applikation, så følsom information ikke kan ses på den låste skærm. Dette kan gøres i enhedernes indstillinger.

En Mobile Device Management-løsning kan hjælpe jeres virksomhed ved at samle kontrollen over notifikationer på mobile enheder på ét sted.

Indholdspolitik

Download af Apps

I bør aldrig benytte apps, som kommer fra en ukendt tjeneste eller et mistænkeligt link – især hvis I bliver bedt om at ændre sikkerheds-indstillingerne inden installation. I skal kun downloade apps de steder, I har tillid til. Får man installeret en ondsindet app, kan IT-kriminelle potentielt overtage enheden og downloade følsomme data, fx brugernavne og adgangskoder.

Vi anbefaler, at I først og fremmest kun installerer apps fra Apple AppStore og Google Play. Både Apple og Google scanner nemlig alle apps og opdateringer for skadelig kode, før de bliver tilgængelige til download. Med et Android-styresystem har man mulighed for at installere apps fra forskellige kilder, så her skal I især være opmærksomme.

Vi anbefaler også en Mobile Device Management-løsning, så I kan begrænse jeres medarbejderes muligheder for at installere apps, som virksomheden ikke har tillid til eller ikke har godkendt. Ydermere kan I forhindre ændringer i sikkerhedsindstillingerne, så det ikke bliver muligt at downloade apps, via links eller filer installeret direkte på enheden. I kan også blackliste specifikke apps, som I ved er usikre. Dermed forbedres jeres sikkerhed markant.

Privat og arbejde

Både store og små virksomheder bør adressere, hvordan de private og arbejdsmæssige digitale liv holdes adskilt. Vi anbefaler som minimum, at I opsætter konkrete retningslinjer for jeres medarbejdere. Den enkelte medarbejders adfærd har stor betydning for sikkerheden på dette område.

I skal være opmærksomme på, at både private personlige data og virksomhedsdata kan være følsomme eller værdifulde. Hvis I mister en mobil enhed, der både bruges privat og professionelt, skal I derfor også være parate til potentielt at miste private fotos eller andre data, som ligger på enheden. Med en Mobile Device Management-løsning kan I opdele enheden i et privat- og arbejdsområde og håndtere disse særskilt. Det kan for eksempel forhindre, at data bliver kopieret på tværs, og så kan I samtidig sætte retningslinjer for indholdet i den arbejdsrelaterede "container".

Netværkssikkerhed

Sikkerhed på farten

Vi anbefaler, I undgår at benytte offentlige netværk, da der er risiko for, at andre kan overvåge jeres aktiviteter på nettet eller placere virus eller malware på jeres enheder. Hvis I alligevel gør det, er det vigtigt at kryptere de informationer, I sender og modtager. En VPN-løsning krypterer jeres data og sikrer, at ingen kan opsnappe disse, og den skjuler samtidig jeres færden på nettet.

Med en Mobile Device Management-løsning fra Telenor Erhverv, kan I nemt definere hvilke applikationer, der skal bruge VPN, og hvilke, der ikke skal. Løsningen kan også styre, om der overhovedet kan oprettes forbindelse til åbne WiFi-netværk. Derved sikres jeres mobile enheder bedst muligt.

Vær også opmærksom på, at jeres mobile enheder kan snydes til at benytte et usikkert netværk. Det kan ske ved, at et offentligt tilgængeligt netværk udgiver sig for at være et netværk, du tidligere har været logget på, uden du opdager det. Slå automatisk etablering af forbindelse (auto-join) til Wi-Fi fra i jeres enheders indstillinger og undgå at logge på WiFi, hvor der ikke skal bruges et password for at få forbindelse.

Desuden bør I benytte den nyeste netværksteknologi, når det er muligt. 5G er fx mere sikkert end 4G, der igen er mere sikkert end 3G osv.

Sikker adgang fra distancen

En af de mest populære og effektive måder at give fjernadgang til medarbejdere på er via en VPN-forbindelse (Virtual Private Network). Det fungerer som en sikret tunnel mellem hjemmearbejdspladsen og virksomhedens systemer og data.

Med en VPN-forbindelse sikrer I, at I har styr på, hvem der tilgår jeres interne systemer. Dog kan det være relevant at tænke over, hvad I gerne vil tillade adgang til fra distancen. Man kan normalt sætte begrænsninger op for, hvad VPN-brugere har adgang til. Det vigtige her er dog, at I rent faktisk anvender VPN-forbindelsen. Med en Mobile Device Management-løsning kan I netop sikre, at en VPN-forbindelse er en betingelse for, at kunne logge på jeres interne systemer.

Datahåndtering

Backup

Ved backup af mobile enheder er det vigtigt, der er styr på opdelingen af privat og arbejdsrelateret data.

I takt med at mobile enheder bruges både privat og på arbejde, opstår der nye problematikker. Et eksempel er, at I har en medarbejder, der regelmæssigt laver en iCloud-backup af sin iPhone uden at opdele privat og arbejdsrelateret data. Hvis denne medarbejder stopper, afleverer sin firmaudleverede iPhone og derefter bliver ansat hos konkurrenten, hvor de udfører udfører en restore fra backuppen, så er jeres data pludselig havnet et meget uhensigtsmæssigt sted.

Derfor er vores anbefaling, at I ikke slår backup til, med mindre I har styr på opdelingen af data.

Sletning af data

Alle medarbejdere bør være klar til at slette indholdet på deres mobile enheder, hvis de mister dem. Her anbefaler vi, at I gør jer overvejelser om, hvor meget I må blande jeres private data med firmarelateret data.

Selvom I lukker alle adgange til systemer, kan der stadig ligge indhold lokalt på medarbejderenheder, fx i mails eller billeder, som man skal sørge for at få slettet.

Med en Mobile Device Management-løsning kan I altid låse eller slette indhold på jeres mobile enheder – også i tilfælde af, at der skulle opstå en konflikt med en medarbejder.

Identifikationsdata

Det er altid vigtig at holde jeres personlige data fortrolige og utilgængelige for uvedkommende. Hvis I handler på nettet, er det fx en god idé at sikre jer, at modtageren har den rette sikkerhed til forsvarligt at varetage jeres data.

I kan kigge efter hængelåsmærket, og I kan også tjekke, om adressen i adressefeltet ændrer "fornavn" fra http til https, som er en mere sikker standard.

På https://haveibeenpwned.com/ kan I nemt tjekke, om jeres emailadresser og loginoplysninger har været en del af et datalæk og dermed er blevet eksponerede.

Vi anbefaler desuden, at I løbende holder øje med jeres bankkonti for at tjekke, at der ikke foregår svindel. Mange små beløb kan let gemme sig over en længere periode.

Google Chrome og dens Password Manager fortæller jer desuden, hvis I bruger det samme password for mange gange, og på den måde gør jer mere udsatte.

Lokalitet og aktiviteter

I bør gennemgå jeres apps én for én og for hver af disse vælge og fravælge adgang til lokalitets- og andre typer data, så der ikke opsamles unødvendig data. For dem, I tillader, bør I huske kun at slå dem til i relevante situationer.

Desuden bør I være varsomme med at dele informationer om jeres eller medarbejdernes færden på sociale medier, da hackere også kan bruge dette som information til deres angreb. Det kan derudover også være interessant for konkurrenter at kunne identificere samarbejdspartnere og kunder gennem deres lokalitet.

Hvorfor skal du vælge Telenor som sikkerhedspartner?

Bred erfaring

Telenor hjælper alt fra iværksættere og globale virksomheder til offentlige myndigheder med sikkerhed

Dyb viden

Vi har **sikkerhedskonsulenter** der er specialister i at koble sikkerhedsprocesser, teknologi og mennesker sammen i integrerede løsninger, der passer til din virksomhed.

Bedste MDM løsning

Med Telenor Mobile Device Management (MDM) får du beskyttet din virksomheds data på en fremtidssikret måde tilpasset din forretning. Og du behøver ikke engang være mobilkunde

LÆS MERE

Klik på nedenstående link, hvis du vil læse mere om vores sikkerheds-løsninger:

www.telenor.dk/erhverv/sikkerhed

KONTAKT

Ring til 72 128 890, hvis du vil høre mere om, hvordan I kan bruge MDM til at sikre jeres forretning: