Android Utbildningskompendium (säkerhet och skydd)

Skapat av: Thunbergs Teknikhjälp

Tobias Thunberg

Thunbergs Teknikhjälp

076 838 9441

tthjalp@outlook.com

www.tthjalp.com

Upphovsrätt

Detta material är skyddat enligt lagen om upphovsrätt. All kopiering, distribution eller spridning av innehållet, helt eller delvis, utan uttryckligt skriftligt tillstånd från författaren, är förbjuden. Materialet är endast avsett för personligt bruk inom ramen för den specifika utbildning det har tillhandahållits för.

Innehåll

Vikten av säkerhet på din mobil....3

Så här ställer du in ett säkert lösenord eller skärmlås....3

Så här skyddar du dig mot kapning och bedrägerier....3

Om du ändå blivit utsatt för bedrägeri....4

Säkerhetskopiera din data....4

Så här skyddar du dig mot stöld av din mobil....5

Detta material är skyddat enligt lagen om upphovsrätt.

Vikten av säkerhet på din mobil

Din mobiltelefon innehåller mycket personlig och känslig information, som bankuppgifter, foton, och kontakter. Att skydda din telefon och data från obehörig åtkomst är därför mycket viktigt. Här är några viktiga saker att tänka på för att förbättra din säkerhet.

Så här ställer du in ett säkert lösenord eller skärmlås

1. Öppna 'Inställningar' och gå till 'Säkerhet'.

2. Välj ett skärmlås som passar dig: PIN-kod, mönster, eller lösenord.

3. Skapa ett starkt lösenord genom att använda en kombination av bokstäver, siffror och symboler. Ju mer varierat, desto säkrare är lösenordet.

4. Aktivera ansiktsigenkänning eller fingeravtrycksläsare för enklare och snabbare upplåsning. Detta är smidigt men fortfarande säkert!

Tips: Använd alltid ett starkt och unikt lösenord som är svårt att gissa. Undvik att använda samma lösenord på flera olika ställen.

Så här skyddar du dig mot kapning och bedrägerier

1. Håll din telefon och appar uppdaterade – nya uppdateringar innehåller ofta säkerhetsfixar som skyddar dig mot nya hot. Förklaring: nya säkerhetsluckor upptäcks hela tiden och kan utnyttjas om man inte åtgärdar dessa brister genom uppdateringar.

2. Undvik att klicka på länkar i okända eller misstänkta meddelanden och e-post. ”Pishing” innebär att någon försöker få dig att ange dina personliga uppgifter för att sedan kunna sälja vidare dem eller utnyttja dem på annat sätt.

- Kontrollera avsändaren, är det från en konstig epostadress eller okänt telefonnummer?

- Är språket konstigt? Många misstänksamma meddelanden innehåller oftast konstiga formuleringar och ordval (men inte alltid).

- Är det som efterfrågas i meddelandet rimligt? Använd sunt förnuft här.

Thunbergs Teknikhjälp
076 838 9441
tthjalp@outlook.com
www.tthjalp.com
Detta material är skyddat enligt lagen om upphovsrätt.

- Kontakta alltid själv din bank på officiella kanaler så som deras kundtjänst-nummer om du blivit uppringd av någon som påstår sig vara din bank och du misstänker att det inte stämmer.

3. Aktivera tvåfaktorsautentisering (2FA) för viktiga tjänster som e-post, sociala medier och banktjänster. Det ger ett extra lager av säkerhet.

4. Var försiktig med vilka appar du laddar ner, och ge endast nödvändiga behörigheter till de appar du installerar. Du kan bland annat kontrollera hur många nedladdningar en app har. En app som laddats ner miljoner av gånger anses vara mer säker än en app som laddats ner enbart ett hundratal gånger.

Om du ändå blivit utsatt för bedrägeri

Även om du är försiktig kan du ändå råka ut för bedrägeri. Om det händer är det viktigt att agera snabbt för att begränsa skadan.

1. Kontakta din bank omedelbart och spärra dina kort samt eventuella BankID-tjänster om dina uppgifter kan ha kommit i orätta händer.

2. Polisanmäl händelsen, till exempel via polisen.se eller telefonnummer 114 14.

3. Kontakta Konsumentverkets Hallå konsument på 0771-525 525 för vägledning om dina rättigheter.

4. Byt lösenord på de konton som kan ha blivit kompromitterade och aktivera tvåfaktorsautentisering om det inte redan är aktiverat.

5. Berätta gärna för familj och vänner vad som hänt, så att de också kan vara uppmärksamma om samma bedragare försöker kontakta dem.

Säkerhetskopiera din data

1. Säkerhetskopiera din telefon regelbundet så att du inte förlorar viktig information om något skulle hända. Antingen till molnet (mer om detta senare) alternativt till en dator.

Detta material är skyddat enligt lagen om upphovsrätt.

2. Gå till 'Inställningar' > 'Säkerhetskopiering' för att aktivera automatisk säkerhetskopiering till Google Drive eller andra tjänster.

Så här skyddar du dig mot stöld av din mobil

1. Använd funktionen 'Hitta min enhet' för att spåra din telefon om den skulle bli stulen eller borttappad.

2. Gå till 'Inställningar' > 'Säkerhet' > 'Hitta min enhet' och se till att den är aktiverad.
3. Om din telefon blir stulen eller borttappad, använd en annan enhet för att låsa eller radera data på distans.

Detta material är skyddat enligt lagen om upphovsrätt.