iPhone-toegangscode

Bert van Dijk

Een dief kan je digitale leven ruïneren na het afkijken van de toegangscode voor je iPhone. Dat is rampzalig. Lees hier hoe je het voorkomt en nog meer handige tips!

In een onthullende video[1] van Wall Street Journal zie je wat er allemaal kan gebeuren als je iPhone wordt gestolen en de dief (of een handlanger) kort daarvoor de toegangscode van je iPhone heeft afgekeken of gefilmd. Met die toegangscode kan een dief je iPhone ontgrendelen en het Apple ID-wachtwoord veranderen, zodat je bent buitengesloten in je eigen Apple ID en de daarin opgeslagen foto's. Vervolgens kunnen ze de Zoek mijn-functie uitschakelen en heeft de dief ook toegang tot alle wachtwoorden in de iCloud-sleutelhanger. Ook zal hij vaak in de Foto-app zoeken naar foto's met gevoelige informatie, zoals je BSN waarmee ze je identiteit kunnen stelen en misbruiken. Je iPhone wordt vervolgens gewist en doorverkocht.

Toegangscode en herstelcode resetten

Zonder herstelcode kun je niet meer bij je gegevens als de dief het wachtwoord van je Apple-ID heeft veranderd. Je loopt dan dus het risico om niet alleen je iPhone kwijt te raken, maar ook al je foto's als die je alleen in iCloud hebt opgeslagen. Maar ook als je wel een herstelcode hebt ingesteld, kan het nog misgaan. Het probleem is namelijk dat een dief met de toegangscode van je gestolen iPhone ook een herstelcode kan resetten. Dit is een zwakte waar Apple echt iets moet gaan doen om dit te voorkomen. Alleen als je iPhone zakelijk beheerd wordt, bleek er nog wel een manier te zijn om het resetten van de herstelcode met je toegangscode te voorkomen. Waarschijnlijk houdt dit verband met de mogelijkheid dat de inhoud van dergelijke toestellen vaak op afstand gewist kan worden. Bijkomend probleem is dat na het instellen van een herstelcode ook Apple niets meer kan doen om je te helpen, omdat de gegevens dan versleuteld zijn met een sleutel waar ook Apple geen controle over heeft.

Oplossing

De oplossing die Apple hiervoor zou moeten implementeren, is om voor het instellen of resetten van de herstelcode niet alleen de toegangscode te gebruiken, maar ook een Face-ID of Touch-ID die al geruime tijd op het toestel wordt gebruikt. Zo'n relatief eenvoudige maatregel voorkomt dat een dief hier misbruik van kan maken. Je zult intussen ook wel begrijpen dat je ook onder dwang nooit de toegangscode van je iPhone aan iemand moet geven.

Als extra beschermingsmaatregel zou je ook kunnen overwegen om een lokale back-up te maken van alles wat je beslist nooit kwijt wilt raken. Bij veel gebruikers zal het hierbij met name om de foto's gaan. Een relatief eenvoudige oplossing hiervoor op een Mac is om je Foto-bibliotheek te verplaatsen naar een externe harde schijf en in Foto's al je originelen te downloaden. Als HCC-lid kun je na inloggen op apple.hcc.nl bij downloads voor HCC-leden een hand-out downloaden met slimme back-up-oplossingen voor je Mac, iPhone en iPad. Via de nieuwe menukeu-ze Video's kun je dan ook een opname van de daarbij behorende presentatie terugkijken.

Tip 1 Extra wachtwoord

Omdat dit misbruik steeds vaker voorkomt, verwachten we dat Apple in iOS 17 bij het wijzigen van het Apple-ID-wachtwoord ook gaat invoeren dat je het huidige Apple-ID-wachtwoord moet invullen. De dief heeft dan nog wel toegang tot je iCloud-sleutelhanger (bewaar de meest gevoelige data daarom in een app die niet toegankelijk is met je iPhone-toegangscode), maar je kunt tenminste nog op afstand je iPhone wissen.

Ook zou je via *Instellingen* > *Schermtijd* > *Gebruik toegangscode* voor ´Schermtijd' een schermtijd-wachtwoord van vier cijfers kunnen instellen als extra bescherming. Ga hierna naar *Instellingen* > *Schermtijd* > *Beperkingen* en zet daar de schakelaar voor Beperkingen *aan*. Scrol naar beneden, tik op *Account wijzigingen* en kies daar voor *Sta niet toe*. Nu kan niemand je Apple-ID wachtwoord veranderen zonder deze extra schermtijd-toegangscode. Door deze extra beveiliging is echter je account bovenaan bij Instellingen ook niet toegankelijk en zul je eerst via *Instellingen* > *Schermtijd* > *Beperkingen* de schuif achter Beperkingen weer *uit* moeten zetten.

Tip 2 Sterk wachtwoord

Het is altijd verstandig is om een wat sterker iPhone-wachtwoord te kiezen. Standaard bestaat het iPhone-wachtwoord uit zes cijfers. Kies zeker geen voor de hand liggende codes als 111111 of 123456 die nog gemakkelijker af te kijken zijn. Via *Instellingen* > *Face ID en toegangscode* kun je via *Wijzig toegangscode* en T*oegangscode opties* kiezen voor een aangepaste alfanumerieke code die ook veel langer kan zijn, wat het afkijken iets moeilijker maakt. Maar als het intypen wordt gefilmd, zal ook deze maatregel niet krachtig genoeg zijn.

Tip 3 Contact accountherstel

Ook is het heel verstandig om binnen de instellingen bovenaan bij je Naam via Wachtwoord en beveiliging bij Accountherstel een vriend of familielid aan te wijzen als een accountherstelcontact. Daarmee kun je via die persoon weer toegang krijgen tot je iPhone-data.

Tip 4 Bedieningspaneel uitzetten

Nog een handige tip: zet via *Face-ID (of Touch-ID)* en *Toegangscode* het Bedieningspaneel *uit* (zie afbeelding boven in volgende kolom). Zo kan een dief niet zonder inloggen in het bedieningspaneel de vliegtuigknop indrukken, waardoor je via de Zoek mijn-functie niet meer kunt zien waar je gestolen iPhone is.

Conclusie

De beste en ook eenvoudigste bescherming tegen dit misbruik is om in openbare plaatsen ALTIJD gebruik te maken van Face-ID of Touch-ID. Dan kan een dief niet het wacht woord van je iPhone afkijken, wat hier de sleutel is voor dit misbruik.

Apple_Face_ID_en_toegangscode_Bedieningspaneel

Meer Apple-tips, HCC!apple en HCC-lid worden

Wil je vaker van dit soort nuttige Apple-tips ontvangen? Voeg dan via de website van de Apple-ig[2] of de website van HCC[3] HCC!apple toe aan je lidmaatschap van HCC.

Links:

1. **https://www.wsj.com/articles/apple-iphone-security-theft-passcode-data-privacya-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a**
2. **https://apple.hcc.nl/**
3. **https://hcc.nl/component/hccxmlbeheer/?view=profiel**