Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

Uw mobiele apparaten beveiligen

Gastredacteur

Lance Spitzner, directeur bij SANS Security Awareness, is al meer dan 20 jaar actief betrokken in de wereld van cybersecurity. De afgelopen tien jaar met een sterke focus op de menselijke kant van cybersecurity. Volg Lance via @lspitzner.

Overzicht

Mobiele apparaten maken het op een eenvoudige manier mogelijk te communiceren met vrienden, online te winkelen of bankieren, films te kijken, spelletjes te spelen en tal van andere activiteiten te ontplooien. Aangezien uw apparaten zo'n belangrijk onderdeel uitmaken van uw leven volgen hier een aantal eenvoudige stappen om ervoor te zorgen dat u en uw apparaten veilig en betrouwbaar zijn en blijven.

Uw apparaten beveiligen

Op de vraag wie het grootste risico vormen voor uw mobiele apparaat kan een verassend antwoord volgen. Wellicht zal het u verbazen dat het zeer waarschijnlijk geen hackers zijn, maar uzelf. Er is namelijk veel meer kans dat u een mobiel apparaat verliest of vergeet dan dat iemand het apparaat daadwerkelijk hackt. Het belangrijkste wat u moet doen om uw apparaten te beschermen is dan ook het automatisch vergrendelen van het scherm mogelijk maken, vaak een screenlock genoemd. Concreet betekent dat, telkens wanneer u uw apparaat wilt gebruiken, u het scherm moet ontgrendelen, zoals met een sterk wachtwoord of uw vingerafdruk. Dit helpt ervoor te zorgen dat wanneer uw apparaat verloren of gestolen is, niemand er toegang toe heeft. Aanvullend zijn hier nog een aantal tips om uw apparaten te helpen beschermen:

Updaten

Schakel automatisch updaten op uw apparaten in zodat ze altijd beschikken over de nieuwste versie van het besturingssysteem en apps. Aanvallers zijn altijd op zoek naar nieuwe zwakke plekken in de software, en leveranciers geven voortdurend nieuwe updates en patches uit om deze te verhelpen. Door altijd het nieuwste besturingssysteem en mobiele apps te hanteren, maakt u het voor anderen veel moeilijker om uw apparaten te hacken.

Traceren

Installeer of activeer software die het mogelijk maakt uw apparaat via internet te kunnen traceren. Wanneer uw toestel verloren of gestolen is, kunt u op deze manier via internet verbinding maken met het toestel en de locatie ervan vinden. In het ergste geval kunt u zelfs al uw informatie op afstand wissen.

Vertrouwde Apps

Download alleen apps die u nodig heeft en afkomstig uit vertrouwde bronnen. Voor iPads of iPhones betekent dit het downloaden van apps uit de Apple App Store. Voor Android download u apps uit Google Play en voor Amazon

tablets uit de Amazon App Store. Hoewel u ook apps van andere sites kunt downloaden, worden deze niet gescreend en is het veel waarschijnlijker dat ze besmet zijn. Voordat u een app downloadt controleert u of deze veel positieve recensies heeft en actief wordt bijgewerkt door de verkoper. Blijf uit de buurt van gloednieuwe apps, apps met weinig reviews of zelden bijgewerkte apps. Tot slot, ongeacht waar u uw app heeft gedownload, raden wij u aan de app te verwijderen van uw apparaat zodra u deze niet langer nodig heeft of niet actief meer gebruikt.

Privacy-opties

Beoordeel de privacy-opties wanneer u een nieuwe app installeert. Een voorbeeld: heeft de app die u zojuist geïnstalleerd heeft werkelijk toegang nodig tot al uw vrienden en contactengegevens? Ook raden wij u aan om locatiegegevens delen standaard voor alles uit te schakelen en vervolgens de locatie alleen in te schakelen voor apps waarbij u dat nodig vindt. Op het moment dat u zich niet prettig voelt bij de toestemmingsvereisten van een app, ga dan op zoek naar een andere app die aan uw behoeften voldoet. Controleer ook periodiek of de rechten van een app niet zijn gewijzigd.

Back-ups

Maak altijd een back-up van uw gegevens. Voor mobiele apparaten geldt dat een groot deel van uw informatie automatisch wordt gebackupt, zoals uw foto's of berichten. Back-ups slaan echter ook uw configuratie, apps en andere apparaatinformatie op, waardoor het veel gemakkelijker is om deze te herstellen in het geval van een verloren apparaat of de overgang naar een nieuw apparaat.

Werk

Wees tijdens het werk extra voorzichtig en neem nooit foto's of video's die per ongeluk gevoelige informatie kunnen bevatten, zoals foto's van whiteboards of computerschermen.

Uw mobiele apparaten zijn een krachtig hulpmiddel, waarvan wij willen dat u er plezier aan beleeft en er gebruik van maakt. Alleen al het volgen van deze eenvoudige stappen zijn een juiste stap om u en uw apparaten veilig te houden.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Hulpmiddelen

Wachtwoordzinnen:	https://www.sans.org/u/A3E
Back-up / Herstel:	https://www.sans.org/u/A3z
Uw mobiele apparaten verwijderen:	https://www.sans.org/u/A3u
Veilig gebruik van mobiele apps:	https://www.sans.org/u/A3p
SANS Security Tip van de dag:	https://www.sans.org/tip_of_the_day.php

License

 Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Vertaald door: Tamara Brandt, Sven Jacobs