Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA...

Använda Mobila Appar Säkert

Översikt

Mobila enheter som surfplattor och smartphones har blivit en av de primära technologier vi använder i både våra personliga och professionella liv. Vad gör mobila enheter så mångsidiga är de miljontals appar vi kan välja mellan. Dessa appar gör det möjligt för oss att bli mer produktiva, omedelbart kommunicera och dela med andra, träna och utbilda, eller bara ha roligare. Men med kraften av alla dessa mobila appar kommer risker. Här är några saker du kan göra för att säkert använda och underhålla dina mobila appar.

Gäst Redaktör

Chris Crowley är en oberoende konsult, certifierad SANS instruktör och kurs författare. Han är aktiv på Twitter**CCrowMontance** och på Google plus: **+ChrisCrowley**.

Skaffa Mobila Appar

Det första steget är att se till att du alltid ladda ner dem från en säker, pålitlig källa. Kom ihåg, i stort sätt alla kan skapa en mobil app, så du måste vara försiktig var du får dem från. Cyberbrottslingar har finslipat sina färdigheter till att skapa och distribuera infekterade mobila appar som verkar vara legitima. Om du installerar en av dessa infekterade appar, kan dessa brottslingar ta kontroll över din mobila enhet och läsa din e-post, lyssna på dina konversationer och få tillgång till dina kontakter. Genom att ladda ner appar från endast välkända, pålitliga källor minskar du risken för att installera en infekterad app. Vad du kanske inte inser är att varumärket av den mobila enhet du använder avgör dina alternativ.

För Apple-enheter såsom en iPad eller iPhone, kan du bara ladda ned program från en kontrollerad miljö, Apples App Store. Fördelen med detta är Apple gör en säkerhetskontroll av både mobila appar och deras författare. Medan Apple inte kan fånga alla skurkar eller alla infekterade mobila appar, bidrar denna kontrollerade miljö till att dramatiskt minska risken för att du ska installera en infekterad app. Dessutom, om Apple hittar en app i sin butik som den anser är infekterad kommer de snabbt att bort appen. Windows Phone använder en liknande metod för att hantera applikationer.

Android mobila enheter är olika. Android ger dig mer flexibilitet genom att kunna ladda ner en mobil app från var som helst på Internet. Men med denna flexibilitet kommer mer ansvar. Du måste vara mer försiktig med vilka mobila appar som du hämtar och installerar eftersom inte alla av dem är under översyn. Google upprätthåller en förvaltad App Store som liknar Apples, kallas Google Play. De mobila appar du hämtar från Google Play har haft några grundläggande kontroller. Som

Använda Mobila Appar Säkert

sådan, rekommenderar vi att du hämtar dina mobila appar för Android-enheter endast från Google Play. Undvik att ladda ner Android mobila appar från andra webbplatser, eftersom vem som helst, inklusive cyberbrottslingar, kan enkelt skapa och distribuera skadlig mobila appar och lura dig att infektera din mobila enhet. Som ett ytterligare skydd, överväg att installera antivirusprogram på din mobila enhet.

För att minska risken ännu mer, undvika appar som är helt nya, som få människor har laddat ner, eller som har väldigt få positiva kommentarer. Ju längre en app har funnits eller de mer positiva kommentarer den har, desto mer sannolikt att appen är att lita på. Dessutom endast installera de program du behöver och använder. Fråga dig själv, behöver jag verkligen denna app? Varje app innebär inte bara potentiella nya sårbarheter men också nya integritetsfrågor. Om du slutar att använda en app, ta bort den från din mobila enhet (du kan alltid lägga tillbaka den senare om du upptäcker att du behöver den).

Nyckeln till att säkert använda mobila appar är att installera appar endast från tillförlitliga källor och se till att dina appar uppdateras och du kontrollerat behörigheter.

Slutligen kan du frestas att jailbreaka eller roota din mobila enhet. Detta är en process för att hacka in i den och installera icke godkända appar eller ändra befintlig, inbyggd funktionalitet. Vi rekommenderar starkt mot jailbreaking eller rooting, eftersom det inte bara förbigår eller eliminerar många av de säkerhetskontroller som är inbyggda i din mobila enhet, men ofta också gör garantier och supportavtal ogiltiga.

Behörigheter

När du har installerat en mobil app från en betrodd källa, är nästa steg att se till att den är säkert konfigurerad och skyddar din integritet. Installera och/eller konfigurera mobilappar kräver ofta att du ger vissa behörigheter. Innan du ger tillgång tänk alltid på om din app verkligen behöver dessa behörigheter för att göra sitt uttalade jobb? Till exempel, vissa program använder tjänster för geo-platsinformation. Om du tillåter en app att alltid veta var du befinner dig, kan du låta skaparen av appen spåra dina rörelser, kanske kan de till och med sälja den informationen till andra. Om du inte vill bevilja behörigheter en app begär, shoppa för en annan app som uppfyller dina krav. Kom ihåg att du har massor av alternativ där ute. Apple-enheter tillåter att vissa behörigheter ändras vid inställning eller körning, t.ex. tillgång till geo-platsinformation. Windows och Android mobila enheter är annorlunda, de presenterar dig med en allt-eller-inget tillvägagångssätt. Om du inte ger alla de angivna behörigheterna, kan du inte installera appen.

Använda Mobila Appar Säkert

Uppdatera Appar

Mobila appar, precis som din dator och mobila enhets operativsystem, måste uppdateras för att förbli aktuell. Brottslingar letar ständigt efter och hitta svagheter i appar. De utvecklar sedan attacker att utnyttja dessa svagheter. Utvecklarna som skapat appen skapar också och släpper uppdateringar för att åtgärda dessa brister och skydda dina enheter. Ju oftare du söker efter och installera uppdateringar, desto bättre. På de flesta plattformar kan du konfigurera ditt system att uppdatera mobilappar automatiskt. Vi rekommenderar denna inställning. Om detta inte är möjligt, då rekommenderar vi att du kontrollerar minst varannan vecka för uppdateringar till dina mobila appar. Men när dina appar uppdateras se alltid till att du kontrollerar några nya behörigheter de kan kräva.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhetsbranchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Kassera Din Mobila Enhet:	http://www.securingthehuman.org/ouch/2014#june2014
Säkra Din Nya Surfplatta:	http://www.securingthehuman.org/ouch/2013#december2013
Vanliga Säkerhetsregler:	http://www.securingthehuman.org/resources/security-terms
SEC575: Mobila Enheter Säkerhetskurs:	http://www.sans.org/sec575

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson

