

## Dataträff den 10 februari 2010

### 7 hot mot mobilen och så kan du skydda dig

Mobilerna blir mer och mer lika datorerna, ju mer de kan uträtta desto större blir risken att de kan utnyttjas för ljusskygga syften. Den största oron är att mobilen ständigt är uppkopplad till ett eller flera datanät och samtidigt kan vara uppkopplad till ett konto med pengar antingen din samtalspott eller kontokort. Därför har mobilen blivit ett högvilt tillfälle för hackare och oseriösa tjänsteleverantörer. Åtminstone i teorin.

#### 1. Bluetooth-attacker

**Vad är det?** Skadlig kod som sprids trådlöst via bluetooth-teknik från telefon till telefon. Det fungerar mer som ett traditionellt virus, eftersom elaka program som utnyttjar bluetooth-tekniken oftast automatiskt söker efter bluetooth-enheter i närheten och skickar sig vidare.

**Hur farligt är det?** Än så länge är det inte så farligt, I dagsläget går de flesta attacker ut på att irritera mer än att länsa kontot. Det handlar mest om prototyper som hackare skriver för att testa hur svårt det är att i framtiden kunna sprida allvarliga virus. Men möjligheten att bli infekterad med ett virus som får mobilräkningen att gå i taket finns där.

**Hur stor är risken att drabbas?** Inte i dagsläget så stor. Bluetooth-viruset som hoppar från telefon till telefon är sällsynta. Du måste vara i närheten av en annan smittad telefon, dels ha din inställd så att anrop kan göras, och slutligen måste du manuellt tacka ja till att ta emot det som sänds. Har du otur och är oförsiktig kan du drabbas.

**Hur skyddar jag mig?** Stäng av bluetooth-funktionen i mobilen helt eller ha den påslagen i ett läge så att din mobil inte kan upptäckas av andra bluetooth-enheter. Det säkraste är att ha bluetooth avstängd utom när du just precis behöver den(det sparar dessutom på batteriet).

#### 2. Skadliga webbsidor.

**Vad är det?** Mobilens webbläsare är, liksom datorn, en möjlig väg för skadliga program att ta sig in.

**Hur farligt är det?** Det rapporteras om säkerhetshål i mobila webbläsare, där elakt skriven kod kan krascha webbläsaren eller systemet. I en tidig version av webb-läsaren till det mobila operativsystemet Android kunde en hackare ta del av allt som användaren skrev i webbläsaren. Lösenord till exempel. Det problemet är dock löst. Faran är dock större att du luras att ladda ner trojanprogram från webbsidor som ser seriösa ut.

**Hur stor är risken att drabbas?** Dock hitintills ganska liten. Men ju mer du surfar i smartphones på den "vanliga" webben och inte på utvalda Webb-sidor, desto mer osäkert blir det. Ett problem med mobiltelefoner är att om ett säkerhetshål upptäcks i en webbläsare, så är det inte lika lätt att få alla användare att installera en uppdatering som löser problemet. Ett konstant nedladdande av program resulterar också i höga kostnader.

**Hur skyddar jag mig?** Ha alltid den senaste versionen av din webbläsare och ditt operativsystem installerad i telefonen. Anslut till tillverkarens servrar och sök efter uppdateringar.

### 3. Trojaner.

**Vad är det?** En trojan är ett skadligt program som du luras ladda hem och installera på din dator eller på din mobil. Trojanprogrammet kallar sig naturligtvis inte "Elaka hacket som förstör din telefon 2,0", utan förklarar sig till ett användbart nyttprogram eller ett spel.

**Hur farligt är det?** En trojan kan få tillgång till alla viktiga funktioner i mobilen. Har du till exempel laddat hem ett chattprogram eller ett spel med en topplista online, så svarar du ju ja på en fråga som "Ska detta program få skicka data över internet?". Sedan är det kört.

**Hur stor är risken att drabbas?** Bland skadlig kod till mobiler är trojaner vanligast. Det operativsystem som är mest drabbat är Symbian Series 60 som sitter i ett flertal smartphones från Nokia och Samsung. Även Symbian UIQ, vanligt i telefoner från Sony Ericson och Motorola, och smartphone-operativet Windows Mobile, har en del virus och trojaner. Den tredje plattformen att se upp med är J2ME, en Java-motor som finns i många mobiltelefoner. Har din telefon Java-stöd är det antagligen denna som används.

**Hur skyddar jag mig?** Installera aldrig program på mobilen som du inte är helt säker på var de kommer ifrån. De stora mobiltillverkarna har egna sajter med program som är kontrollerade och säkra att ladda hem. Kör aldrig program och funktioner som skickas till dig med e-post eller mms, inte ens om du känner avsändaren. Din bekants telefon kan redan vara infekterad.

### 4. Automatiska sms.

**Vad är det?** De flesta mobiler kan ta emot så kallade Class 0 eller Flash sms. Det är sms som inte lagras i mobilens inbox utan visas direkt. En del sådana kan användas för att skicka instruktioner till mobilen, istället för att visas på skärmen. Vanligen används det till att låta mobiloperatören skicka rätt inställningar så att du kan använda mobilsurf och mms.

**Hur farligt är det?** Säkerhetsföretagen varnar för Class 0 i kombination med en trojan. Är du smittad med ett skadligt program kan en hacker skicka sms till din telefon med det programmet i smyg, och därmed fjärrstyra vad trojanen gör.

**Hur stor är risken att drabbas?** Något fall av Class 0 sms-back har inte rapporterats, men säkerhetsföretagen och operatörerna håller uppsikt efter det. Skulle din telefon bli infekterad av en trojan som använder Class 0 sms har du inte mycket till skydd mot eventuella attacker, eftersom samma program redan finns i systemet och kan ändra eventuella inställningar du gjort för att skydda dig.

**Hur skyddar jag mig?** Vissa class 0-sms kallas i telefonen för push-sms, och de kan du oftast välja bort om du tittar i inställningsmenyerna till din sms-funktion. Det viktigaste är att du alltid får valet att acceptera eller inte acceptera nya inställningar, och alltid svara nej tack till allt som du inte vet kommer från din mobiloperatör.

### 5. SMS-spam

**Vad är det?** Spam(skräppost) är mail som översvämmar inboxen med allsköns reklam om allt från pyramidspel till bantningskurer och potenspill. Samma störande informationsflod finns i vissa länder på sms.

**Hur farligt är det?** Det kan ställa till problem om sms-volymen är stor. Sms skickas direkt till din mobil och sparas automatiskt, oavsett om du vill ha dem eller inte. På en telefon med lite minne kan det hända att platsen för sms tar slut. Då kan du missa riktiga meddelande.

**Hur stor är risken?** I Sverige är det här ett minimalt problem, men här i Spanien kan det vara betydligt större risk. Kostnaden för att skicka sms i Sverige är betydligt högre än i många andra länder, som till exempel USA, där det är lättare att skicka sms gratis eller till lågpris, och där spam-eländet är vardagsmat även i mobilen.

**Hur skyddar jag mig?** I länder där sms-spam är vanligt jobbar operatörerna med spamfilter, så att eländet inte ska komma fram. Det finns också program som du kan installera i mobilen som gör samma sak. Två sådana är Webgate SMS Spam Manager som finns för Symbian Series 60 och UIQ, och SMS Spaminator för Windows Mobile. Båda kostar ungefär tio dollar (70 kronor).

## 6. Phishing

**Vad är det?** I mobilvärlden är en vanlig typ av phishing att lura folk att ringa upp dyra betalnummer eller skicka dyra betal-sms. Bedragaren skaffar ett nummer (ofta i ett land där lagstiftningen om sådant luredrejeri inte är helt klar) som kopplas till en betaltjänst.

Den som ringer upp detta nummer åker på en skyhögt minuttaxa. Sedan ringer han upp mängder av mobilnummer och lägger på luren innan de hunnit svara. Det bedrägliga numret dyker då upp som ett missat samtal, och om du ringer upp kan pengarna snabbt ticka iväg. Samma sak gäller sms, ett kort "Hej" kan få många att svara tillbaka med ett "Vem är du?" Och vips har betaltjänsten dragit en femtilapp eller så.

**Hur farligt är det?** Du kan mycket snabbt att komma upp i tresiffriga tal när du luras att ringa ett betalnummer. Den största risken löper du som har ett abonnemang., eftersom det inte finns något tak för vad som det kan komma att kosta.

**Hur stor är risken att drabbas?** Det här är organiserad brottslighet, om än inte i jättelik skala. Under de senaste åren har olika varningar gått ut om betalnummer-bluffar med satellittelefonnummer och bland annat ryska och italienska nummer.

**Hur skyddar jag mig?** Du som är orolig för phishing eller vill hindra att det rings till sådana nummer från en mobil, kan spärra möjligheten att göra det. Alla de stora operatörerna i Sverige erbjuder den tjänsten. Men det kan vara opraktiskt med den tjänsten, ur många andra orsaker. Då är det försiktighet som gäller. Ring inte upp missade samtal från okända nummer eller svara inte på sms från okända.

## 7. Abonnemangs-fällan

**Vad är det?** En hel del av företag säljer spel, nyttoprogram, bakgrundsbilder, skärmläckare och ringsignaler till mobilen. Jamba, Impoc och Boomi är några som erbjuder både nyttiga och kul tillägg till mobilen. Tyvärr lockas många att dra på sig stora kostnader. När man tror att man betalat några kronor för en ringsignal har man i själva verket bundit sig till löpande abonnemang som regelbundet drar pengar från ditt mobilkonto. I juli 2009, på endast en månad, hade t.ex. Jamba.se som fått 27 KO-anmälningar från kunder som anser sig ha blivit lurade på detta sätt. Det är dessutom svårt att bli av med abonnemanget.

**Hur farligt är det?** Det kostar pengar. Tjänsterna i sig och programmen kommer från kända avsändare och får anses som relativt säkra. Du lär knappast få virus från dessa företag.

**Hur stor är risken att drabbas?** Tjänsterna finns där, drivs lagligt och öppet, och för den som är oförsiktig finns risken. Här är det att se upp.

**Hur skyddar jag mig?** Läs det finstilta i avtalet! På Jamba.se, som blivit den tjänst som fått symbolisera problemet är det faktiskt skrivit i klartext när du beställer, att det handlar om ett abonnemang, och vad det kostar. Spärr mot betaltjänster hjälper, eftersom att flera av nedladdningstjänsterna använder sms-betalning.