



DATAOMBUDSMANNENS BYRÅ

PHARMING, VAD ÄR DET?

Uppdaterad 27.07.2010

www.tietosuoja.fi

VAD ÄR PHARMING?

HUR MAN KAN KAPA DIN DATORANSLUTNING OCH STJÄLA DIN IDENTITET

Du ska köpa böcker via en nätbutik och hamnar på försäljningssidor av en känd butik, och på sidorna bes om dina identifikationskoder för betalning. Att köpa och betala så är behändigt och tryggt – eller är det? Leveransen låter vänta på sig och snart avslöjas även att dina kontouppgifter missbrukats och pengar överförts från ditt konto till andra konton. Det visar sig att en hacker har kapat din dator och lurat dig till sina egna sidor, lagt beslag på dina hemliga identifikationskoder och med hjälp av dem använt ditt konto. Du har råkat ut för kidnappning av din dator och dina datakommunikationer – blivit offer för pharming. Alla som använder sig av Internet och nät-tjänster kan falla offer för detta.

Vad är pharming?

En hacker försöker olovligt överta kontrollen över användarens dator och styra in användaren från korrekt server och webbplats till sin egen server och webbplats. För detta ändamål smyger hackern in ett spionprogram som hjälper till att överta kontrollen över datorn, följa användarens bruk av nätverk och -service samt styra kommunikationen och anlitandet av tjänster till sina egna sidor. Detta kan ske utan att användaren medverkar eller överhuvudtaget märker något.

Hackerns avsikt är att få användaren att överlåta hemliga identifikationskoder och annan information som tillåter hackern att använda bankkonton och utnyttja andra förmåner. *I fall av Phishing förmår bedragaren användaren att öppet överlåta hemliga uppgifter, i pharming försöker bedragaren få information utan att användaren är medveten om det.*

Vilka följder kan pharming få?

Känsliga och hemliga uppgifter om dig kan avslöjas, och om de hamnar i offentligheten kan du få problem såsom dåligt rykte. Din identitet kan bli stulen och missbrukad så att du förlorar pengar eller andra förmåner. Missbruk av dina uppgifter leder vanligen till mycket besvär när du reparerar skadan, byter dina identifikationskoder och rättar till fel. Du kan mot din vilja och vetskap vara delaktig i skadlig eller i värsta fall kriminell verksamhet om din dator används t.ex. till att förmedla skräppost, förhindra tjänster eller bedriva olaglig penninginsamling.

Vilka rättigheter har Du?

Du har naturligtvis rätt att förhindra intrång på din dator, det är förbjudet att installera program eller filer på din dator utan att du vet om det. Utomstående får inte följa med det som pågår på din dator, såvida det inte gäller att garantera funktionen och säkerheten. Du bör vara medveten om denna service och ha möjlighet att påverka den. Ingen utomstående får ta del av din dators användning utan din tillåtelse eller utan lagliga grunder.

Om någon utan tillstånd har stulit och använt dina uppgifter har du givetvis rätt att försöka utreda vem som har försökt lägga beslag på uppgifter och för vilket ändamål dessa uppgifterna använts. Dessutom har du rätt att uppdatera dina uppgifter om de har förändrats eller uttraderats.

Du har rätt att få uppgifter som nåtts via pharming raderade. Om missbruket av dina uppgifter vållar dig skada kan du ha rätt till ersättning för skadan.

VAD KAN DU GÖRA?

1) Håll din dator säker

- Skydda din dator mot utomstående inkräktare, håll din brandmur och ditt viruskydd uppdaterade.
- Använd säkra hjälpmedel och program för dator- och nätverksbruk, kryptera överföringarna av känsliga och hemliga uppgifter på nätet.

2) Minska sårbarheten mot bedrägerier

- Använd skyddsprogram, de avslöjar förfalskade webbadresser, använd även filtreringsprogram som förhindrar sk. popup-fönster som används i pharming-bedrägerier.
- Använd anonym nätverksidentitet om du kan.
- Kontrollera att de sidor och förbindelser du använder är säkra, ta i beaktande att också en bedragare kan använda sig av sidor och förbindelser som ser säkra ut.
- Sträva efter att försäkra dig om äktheten på sidor du anlitar, ta i beaktande att även en bedragare kan ha adresser och länkar som verkar äkta.
- Försäkra dig om att du är på rätt webbplats när du ska kontakta t.ex. din bank och/eller använd telefonnummer vars äkthet du kontrollerat.
- Uppsök aldrig obekanta sidor i onödan.
- Svara inte på oklara kontakter och tro inte på vaga löften.
- Klicka inte på länkar i e-posten, som ber om dina hemliga personuppgifter.
- Överlåt inte personliga uppgifter över nätet såvida du inte försäkrat dig om att mottagaren är behörig.

3) Skaffa färdigheter för att förhindra bedrägeri

- Lär dig att förhindra obehörig access till din dator.
- Lär dig traversera och använda tjänster i nätet på ett säkert sätt.
- Lär dig känna de trygga nättjänsterna.
- Lär dig känna igen bedrägeriförsök.

4) Rapportera osakligheter du upptäckt

- Underrätta upprätthållaren för tjänsten som missbrukats om du misstänker att du har fallit offer för ett pharmingförsök.
- Tag kontakt med den som behandlat dina personuppgifter om de har hanterats otillbörligt. Du kan också kontakta dataskyddsmyndigheterna.
- Kontakta polisen ifall du har blivit offer för ett bedrägeri och förlorat t.ex. pengar.

Se även dataombudsmannens byrås broschyrer på www.tietosuoja.fi:

Identitetsstöld, vad är det?

hoax, vad är det?

Brandvägg, vad är det?

Datorkapning, vad är det?