



Bengas datorhörna

Så lätt blir din identitet stulen på Internet

Var fjärde ung svensk har fått sin identitet kapad på nätet enligt Datainspektionens senaste undersökning. I USA fick bara i fjol 15 miljoner människor sina identiteter stulna, och i takt med att vi flyttar ut våra liv på nätet ökar risken dagligen för att du blir nästa person som drabbas.

När Olle öppnade sitt e-postprogram en morgon var det fyllt av arga brev. Hur kunde han bete sig så vidrigt och elakt undrade folk? Olle hade ingen aning om vad som hänt. Tills han loggade in på sitt konto på den populära ungdomscommunityn.

Någon hade kommit över hans inloggningsuppgifter och utgett sig för att vara han. Personen hade skrivit vidrigheter om andra, anklagat vänner för att vara rasister och spridit falska rykten om tjejkompisar att de haft sex med främmande killar. Alla trodde det var Olle som spred de falska ryktena och skickade hatbrev.

Många blir förnedrade

Det hypotetiska fallet ovan skulle kunna vara hämtat ur vilket som helst av de många gemenskaper som finns på nätet. Enligt Karolina Blom, som är pressansvarig på Lunarstorm, är det inte alls ovanligt att hemsidans användare får sina identiteter kapade.

– Att folk inte håller i sina lösenord är vanligt. Det vanligaste som händer när en person fått sitt konto kapat är att man lägger upp falsk information, som kan vara förnedrande, eller att man använder kontot för att skriva vidriga saker hos andra medlemmar, förklarar Karolina Blom och fortsätter:

– Vi försöker alltid vara väldigt tydliga med hur viktigt det är att inte ge ut sina inloggningsuppgifter, inte ens till en pojk- eller flickvän. Om du blir utsatt är det viktigt att du kontaktar oss.

Du är hett byte

Exemplet ovan är bara ett sätt som din digitala identitet kan kidnappas via webben.

Konsekvenserna om du slarvar med hanteringen av dina personliga uppgifter kan bli förödande. Dina konton kan tömmas, du kan få klä skott för grova brott och framför allt kan det vara svårt att tvätta bort de falska spåren som "du" lämnat på nätet.

Men trots att både ekonomi och integritet står på spel, anser Per Hellqvist, som är säkerhetsexpert på Symantec, att vi inte gör tillräckligt för att skydda oss.

– Den digitala identiteten är ett hett byte. Samtidigt råder något slags avtrubning. Vi verkar bry oss mindre och mindre om våra uppgifter och registrerar oss både här och där utan eftertanke.

Kanske beror det på att de flesta av oss inte upplevt någon baksida av det här ännu. Eftersom inget hände när jag registrerade mig förra gången så borde det gå bra även denna gång, funderar Per Hellqvist.

Inget sunt förnuft

Anders Ahlqvist på Rikspolisstyrelsen, där man jobbar med storskaliga bedrägerier på nätet, tycker att många datoranvändare skulle behöva ännu mer utbildning.

– Skulle du lämna ut ditt kontokort till en förbipasserande främling i en park? Förmodligen inte. Och då ska du inte göra det på nätet heller, säger han.

Stor ökning

På Brottsförebyggande rådet, Brå, delas statistiken in i olika kategorier beroende på brott.

Enligt den statistik som PC för Alla har tagit del av har brott inom kategorin datorbedrägeri, ökat från 3 588 fall år 2004 till hela 6 236 fall i fjol.

Lägg därtill en ny kategori brott, bedrägeri med hjälp av internet, som lades till i fjol. Fler än fyra brott varje dag anmäldes, hela 1 502 stycken, så är trenden tydlig.

Hjärnan är bästa vapnet

Lösningen är att tänka sig för.

– Lika svårt som det är att stjäla din vanliga identitet, lika lätt är det att stjäla den digitala. Därför är hjärnan ditt bästa skydd, säger Per Hellqvist.

- Behöver du verkligen lämna ut information till den här personen eller hemsidan? Sedan ska du ha en bra lösenordshantering och uppdaterade program, säger Per Hellqvist.

Nätfiske

Bedragare försöker få dig att klicka på länkar till preparerade webbsidor där de kan komma över personlig information. De mest aktuella phishingattacker är de som Nordea råkat ut för, där bedragare försöker lura in Nordea-kunder (och andra) på en falsk webbsida, där kunderna ombeds lämna uppgifter om sina konton.

Skydd: Inga seriösa företag ber dig lämna känsliga uppgifter via mejl. Kasta sådana mejl. Klicka aldrig på länkar i mejl från okända företag. Se till att både ditt e-postprogram och Windows är uppdaterade. I Internet Explorer 7 och Firefox 2 finns skydd mot phishing. Aktivera dessa.

Kontostöld

Webbutiker, pokerhemsidor och liknande kan vilja ha ditt kontonummer. I vissa fall (betalning via nätet) måste du lämna ut det. Men gör det endast när du måste. Kontrollera så att hemsidan använder en säker anslutning (adressen börjar med https://)

Skydd: Skaffa ett särskilt kontokort för Internet utan kredit och normalt utan pengar på. Överför pengar bara när du ska handla på nätet för att minimera risken att bli av med stora summor.

Routerhack

It-brottslingar kan ta sig in i ett stort antal routrar och dirigera om trafik ,så att du när du skriver in en viss adress, i stället skickas till en falsk webbsida. Både Cisco, D-link och Netgear har routrar som kan hackas på detta sätt.

Skydd: Behåll aldrig routerns standardlösenord, som är allmänt känt. Byt omgående lösenordet till något som bara du känner till.

Namnstöld

Genom trojanska hästar, osäkra webbtjänster och genom social hacking (ringa och be att få låna dina uppgifter till en tjänst en kort stund) riskerar ditt namn att användas för sådant som du inte står för.

Skydd: Lämna aldrig ut inloggningsuppgifter till MSN, communitytjänster, Skype eller liknande. Inte ens till nära familjemedlemmar. Ditt är ditt och ingen annans. Anmäl till din tjänsteleverantör om ditt konto på en hemsida missbrukats.

Loggning

Trojanska hästar är små program som följer med e-post, sprids i chattprogram eller finns i program du laddar hem när du fildelar. En trojansk häst installerar sig på din dator och kan sedan se allt du gör på den. Många kan spara allt du skriver på tangentbordet och skicka iväg informationen till en hacker.

Skydd: Klicka inte på bifogade filer från okända människor. Använd ett uppdaterat antivirusprogram och se till att din brandvägg spärrar utgående trafik.

Grannesurf

Om du inte skyddar ditt trådlösa nätverk kan andra människor nyttja det för att begå olagligheter.

Skydd: Kryptera ditt nätverk, helst med wpa eller wpa2-kryptering. Aktivera Mac-adresslåsning i din router så att bara godkända datorer kan använda nätverket.