Linnéuniversitetet
Kalmar Växjö

Brott på nätet

Fler anmäler It-relaterade brott

Författare: Alva Fandrey

År: 2018

Universitet: Linnéuniversitetet

Kurs: 1DV527

Program: Webbprogrammerare -16

Inledning

Varje dag använder flera miljoner människor internet, antingen via dator eller kanske mobiltelefon. Ibland behöver vi använda internet till skolan, jobbet eller kanske hemma. Internet för med många fördelar, till exempel har vi en obegränsad tillgång av information som vi kan nå nästan var som helst med hjälp av mobiltelefonen eller att vi har möjligheten att kommunicera med varandra vart vi än i världen befinner oss.
Jag har alltid tyckt att fördelarna med internet är oändliga, men det är viktigt att vi även ser nackdelarna som finns. Idag är merparten av de brott som begås It-relaterade. Enligt Polisen så är några utav de vanligaste brotten på nätet bedrägerier, handel med illegala tjänster, barnpornografi, näthat och våldsbrott.
Trots att vi har It-brott definierat i svensk lagstiftning och det finns en lag som säger att teleoperatörer ska lagra trafikuppgifter i sex månader för en effektivare brottsbekämpning, så är ändå de flesta brotten idag It-relaterade. [1]
Det jag vill ta reda på är, varför det är så lätt att begå brott på nätet?

Brott på nätet ökar

It-relaterade brott är lönsamt

Enligt Anders Ygeman, före detta Inrikesminister, begås merparten av alla brottstyper med hjälp av internet, eftersom förövaren kan befinna sig nästan var som helst i världen. Han tror att det kan många gånger bli lönsamt att begå It-relaterade brott då det innebär en relativt låg risk för att bli upptäckt och man kan vara anonym. [2]
Det kan vara mycket svårare att komma åt någon som begått ett It-relaterat brott. Vid brott som till exempel grooming, då en förövare tar kontakt med barn under 15 år för att längre fram begå övergrepp, uppger förövaren ofta falska uppgifter. [1]

Terrordåd börjar på sociala medier

Idag kan vi se en stark koppling mellan sociala medier och terrordåd som skett. Till exempel använde Anders Behring Breivik sociala medier för att planera och knyta kontakter. Han använde Facebook för att sprida sitt ”manifest” till sina kontakter. [3]

Sociala medier kan självklart användas på ett positivt sätt, även under terrordåd, vilket vi fick bevittna under terrordådet i Stockholm. På Facebook fanns en ”Safety check”-

funktion, där du kunde berätta för dina vänner att du var trygg om du befann dig i närheten av dådet. Eftersom all tunnelbane-, pendeltågs- och busstrafik stoppades hade många boende i Stockholm svårt att ta sig hem. Då öppnade människor upp sina hem för att erbjuda en trygg plats och delade denna information via en hashtag. [4]

Det har flera gånger varit tal om att förbjuda sökord på internet som kan relateras till terror. Till exempel ville EU-kommissionären, Franco Frattini, förbjuda ord som bomb, döda, folkmord och terrorism. [5]

Polisen saknar resurser

Enligt David Beukelmann, chef för ungdomsroteln vid citypolisen i Stockholm, finns inte möjligheterna att de ska patrullera på Facebook. Polisen är medveten om att det finns många misstänkta, målsäganden och vittnen där, men de saknar helt enkelt tekniken och resurserna för att kunna arbeta även på sociala medier.
Problemet med tekniken är att polisens datorer inte går att ansluta till ett vanligt internet eftersom deras datorer innehåller känslig information. På varje station finns dock enstaka datorer med en vanlig internetuppkoppling, tyvärr är de ofta få i jämförelse med de anställda. [3]

Förhoppningsvis kan man utveckla tekniken även hos Polisen så möjligheterna finns för att ha en patrull på internet. Visserligen säger de att det inte finns tillräckligt med resurser, men finns tekniken kanske det kan ge möjligheter till nya jobb. Förmodligen behöver du inte vara utbildad polis för att lära dig och patrullera på internet. Om man skulle starta en yrkesutbildning eller kanske ge en kurs, så skulle man säkert kunna utbilda ett antal människor till att vara spanare åt Polisen på internet.

Polisen stöter alltmer på svårigheter när de ska lösa ett brott. I samband med den tekniska utvecklingen har brottsligheten på nätet ökat och lagstiftningen går i otakt. Flera av brotten på nätet sker på utländska sajter och det är inte alltid deras lagar stämmer överrens med Sveriges lagar. Till exempel brukar amerikanarna inte vara särskilt hjälpsamma med att lämna ut uppgifter om personer, ifall brottet inte anses som straffbart i deras land. [6]

Olika sorters It-brott

I den svenska lagstiftningen finns två It-brott definierade, dataintrång och datorbedrägeri. Ett It-relaterat brott kan vara av vilken brottstyp som helst, men man använder It-teknik för att genomföra eller planera brottet.
För att kunna förebygga It-brott kan det vara bra att först och främst känna till vad som faktiskt räknas som ett brott.

- Näthat – meddelanden som ger uttryck för hat. Räknas tyvärr inte som ett brott förrän det handlar om olaga hot, ofredande, hets mot folkgrupp och förtal, hur obehagliga kommentarer man än kan råka ut för.
- Grooming – någon tar kontakt med barn under 15 år för att längre fram begå ett planerat övergrepp.
- Phishing – när någon ”fiskar” efter privata uppgifter på internet till brottsligt syfte.
- Skimning – bedragaren manipulerar betalkortsautomater eller bankautomater för att komma åt information från magnetremsan.
- Personuppgiftslagen, PUL – information som kan knytas till en fysisk person täcks av PUL.
- Hackers och intrång – angriparen gör en portskanning för att se om de finns en öppen port för angrepp. Hackers går endast under dataintrångslagen om den är avsiktlig eller har medfört skada i de system som blivit angripna.
- Trojan – ett program som används för att ta sig in i annan dator på otillåtet sätt.
- Barnpornografi – bilden är pornografisk och visar ett barn, minderårig.

[1]

Slutsats

Varför är det då så lätt för människor att begå brott på nätet?
Det som förmodligen gör internet till en attraktiv plattform att begå brott på är nog anonymiteten. Förövaren kan låtsas vara vem som helst, befinna sig var som helst och risken för att bli upptäckt är relativt låg. Min åsikt är att anonymiteten på internet behöver försvinna. De enda fördelarna jag kan se med att man kan få vara anonym på internet är att man kan få hjälp med frågor man kanske inte annars vågar ställa, men jag tycker inte att det finns någon fördel som väger upp de nackdelar som finns. Om anonymiteten finns kvar kommer vi aldrig kunna minska brotten som begås på nätet.

En av de förmodligen största anledningarna till att det begås så mycket brott på nätet är nog att vi är alltför dåliga på att skydda oss online. Det räcker inte med att vi litar på att de som skapat webbsidan vet vad de gör, vi måste själva ta ansvar för att vi surfar på ett säkert sätt. Det största felet många gör är att vi byter lösenord för sällan och använder samma lösenord till flera olika sidor, vilket innebär att om en hacker får tag på ditt lösenord så kommer denna förmodligen åt flera utav dina konton.
För att ha ett säkert lösenord ska vi använda små och stora bokstäver, siffror och gärna specialtecken. När du har skapat ett säkert lösenord så ska du heller aldrig använda det igen utan komma på ett nytt till nästa sida och det är nog där problemet uppstår. Hur ska man komma ihåg alla dessa lösenord? Det är ju mycket lättare att komma ihåg sonens eller kanske kattens namn och använda det som lösenord, eller hur? Min åsikt är att skriva ner lösenordet på papper och det kanske inte är så dumt som man tror, det är ju faktiskt bättre än att ha samma lösenord till alla konton.

En annan anledning är att människor är alltför godtrogna och okunniga när det kommer till internet. Kanske får man ett mail som ser ut att vara från en vän, men skulle du gå in och kolla på avsändaren så kanske e-post adressen inte alls stämmer överrens längre, eller så kanske det är din väns e-post som har blivit hackad. En del människor är alltför snabba med att lita på det som dyker upp på internet. Har du till exempel någonsin tänkt på vad som händer när du låter webbläsaren spara din information? Oftast när du loggar in på en sida får du alternativet att spara ditt användarnamn och lösenord, men skulle din dator bli hackad betyder detta att förövaren kan få tag i känslig information. Detta är extra viktigt att tänka på innan du låter en webbsida spara information om ditt kontokort, något som blivit alltmer vanligt.
Jag tror fortfarande att internet är framtiden trots att fler brott anmäls och det är just därför vi måste bli

Jag tror att internet är framtiden, trots att brotten ökar och det är därför vi måste bli bättre på att skydda oss på internet.

Referenslista

[1] Polisen, ”It-relaterade brott – lagar och fakta”, Polisen [Online] Tillgänglig: https://polisen.se/lagar-och-regler/lagar-och-fakta-om-brott/it-relaterade-brott/.

[2] A. Ygeman, ”Brott på nätet”, Regeringen, mars 2015 [Online] Tillgänglig: http://www.regeringen.se/artiklar/2015/03/brott-pa-natet/.

[3] A. Hernadi, ”Polisen står handfallen inför brotten på nätet”, Svenska Dagbladet, augusti 2011 [Online] Tillgänglig: https://www.svd.se/polisen-star-handfallen-infor-brotten-pa-natet.

[4] D. Jörnmark Callstam, ”Så agerar du på sociala medier efter attacken”, Aftonbladet, april 2017 [Online] Tillgänglig: https://www.aftonbladet.se/nyheter/a/Aa6ME/sa-agerar-du-pa-sociala-medier-efter-attacken.

[5] M-L. Hallengren, ”EU-kommissionär vill förbjuda terror-ord på nätet”, Aftonbladet, mars 2011 [Online] Tillgänglig: https://www.aftonbladet.se/nyheter/article11243195.ab.

[6] A. Liebermann, ”Svårt för polisen att lösa brott på nätet”, SVT, december 2012 [Online] Tillgänglig: https://www.svt.se/nyheter/inrikes/svart-for-polisen-att-losa-brott-pa-natet.