

Gordon Govan

With the current threats from cyber crimes how responsible can we be for our own identity? Discuss the above statement citing appropriate references and cases.

Introduction

Cyber crimes have been on the increase ever since they were conceived (Expatica News 2006) and the general public know very little about how to protect themselves from such attacks. Identity theft has also been a very hot topic (James Watson, 2004) and identity theft can be easier to commit online because of the anonymity that the Internet provides. This essay shall discuss the field of cyber crime that relates to identity theft by covering how personal data can be obtained, abused and also methods of such crimes can be prevented or policed. The main question that this essay looks to answer is how responsible is the individual for protecting their own identity.

The three main points I wish to cover are how these cyber criminals obtain personal data, how they then use this data to their benefit and how such crimes can be stopped.

Obtaining personal data online is done in very similar ways to how it would be obtained before the Internet. The two largest methods are through gaining the confidence and trust of the individual or through taking the information through unauthorised means such as breaking through the security on a web server and copying private data.

The use of personal data in cyber crimes is very far reaching. It can range from just selling the data on, using it to register to a website or even going as far as making a bank account in the victims name and applying for loans.

Preventing and policing cyber crime is a difficult task and all the parties involved want to shift the responsibility of these tasks on to somebody else. This last section will look at each party and what they could do to help.

OBTAINING DATA

One of the easiest ways to obtain data is just to take what people openly publish about themselves. Social networking websites are filled with users publishing details about themselves. Some of this data is normally harmless such as their favourite food or colour, other details may be of more use to criminals, there may be information about members of your family such as your mother's parents. Your mother's maiden name is a commonly used security question. No doubt that almost of the information on the page could be used in a criminal way. Details of where you work, live and contact details could be used to commit identity fraud and other information could be used by cyber

Cybercrime and Identity

stalkers or cyber harassers to bully or scare you.

“Facebook, ... allows people to post detailed, personal information about themselves, from their date of birth to all the schools they went to – precisely the information that banks ask for as security questions.”

<http://www.telegraph.co.uk/news/uknews/1556322/Fears-over-Facebook-identity-fraud.html>

There are two scary things about how easy it is for criminals to get information from these sites, the first is that it is the individuals who upload all the information and choose to share it, the second is the number of people that use social networking sites. Social networking is one of the fastest growing sectors of the World Wide Web. Nielsen//NetRatings report that the “top 10 social networking sites collectively grew 47 percent year over year, increasing from an unduplicated unique audience of 46.8 million last year to 68.8 million in April 2006, reaching 45 percent of active Web users”(Nielsen//Netratings, 2006). I expect the figure to be even higher now as newer sites like Facebook and Bebo were not included in those figures and Facebooks statistics show that “Active users [are] doubling every 6 months”(Jeremiah Owyang, 2008).

Keeping your personal data safe on these social networking sites is hard since their whole purpose is about telling people about yourself. Some websites have put in certain security by limiting what users are allowed to see. MySpace allows only direct friends to see the accounts of minors (Gil Kaufman, 2006) and Bebo implements 3 different levels of access security of profiles, some are publicly available for all to see, others are only available for other Bebo members to see and others are only available for direct friends. Trying to prevent access like this a good idea, but many people still accept friends when they don't really know who they are essentially voiding the security put in place. Ultimately it falls to the individual to be responsible for what information they upload.

One of the other methods for obtaining data from people is to ask for it. Walking up to people on the street and asking them a question may get some results but the anonymity of computer communication means that people are unlikely to respond to such questions as it so easy just to delete a message from your inbox. What criminals can do is impersonate somebody else and the anonymity of the internet aids this in the sense that an email sent by your bank can look identical to one sent by an imposter. This is called phishing and it has been receiving more media attention in recent years as more people take advantage of shopping and banking online.

Phishing attacks try to get people to enter personal details on what they think is a secure

Cybercrime and Identity

website run by a company they know and trust but is actually an imitation made to fool them. This is similar to more traditional tricks used by con-men. The idea behind phishing and some other online scams is to gain the confidence of the victims and then use that to gain control on them and use that control for your own benefit. Reports say that “phishing cost the U.S. \$3.2 billion in 2007” (TGdaily, 2007) and that it affected 3.6 million people in the USA alone. The fact that over 2% of adult Americans fall for phishing attacks shows that the criminals are using it successfully and it should be something more people should be trying to clamp down on.

The biggest method used to combat phishing is to educate people. Banks often send out leaflets about phishing and all their electronic corresponding informs people that they will never ask for personal data through any means other than their website. There has even been talk of including how to protect yourself from computer crime into the national curriculum. Websites like Phishtank (www.phishtank.com) even help people talk about phishing alerts and use that to notify the company or website being spoofed.

The last method of obtaining personal data that I shall look at is breaking through security and taking it. This can mean two things, either infecting the individuals computer and watch what the users enter or logging on to a server and copy details off of it. The first is performed by using a key logger which sends a copy of what the user has typed to an email address or server so that somebody can analyse it to try and find passwords and other information that the user has entered. Key loggers can be installed on a users machines by a variety of means, the most common being through a trojan or exploiting a security hole in the users operating system and installing the logger remotely.

Copying data from a server can be a lot more difficult. Servers that contain personal data should always be made well secure and often servers are attended to by a team of dedicated professionals that can actively help keep the server secure. This makes gaining unauthorised access to the server a lot harder. Some sites are less secure than others, a bank has a lot more security in place than a forum about wildlife adventures. Criminals can take advantage of this and also the fact that many people use the same password for different services by breaking into a poorly secured website, stealing personal data, including any passwords if they are available in plain text, and then using that data to try and login to more secure websites such as banks or online stores.

Individuals cannot be expected to be an expert at securing their computers but they can at least take basic steps by installing Internet security software. It is common for a person to be offered

Cybercrime and Identity

an Internet security suite when they purchase a new laptop or PC, software like this automatically updates to protect the computer against newer threats. Server administrators are expert users and as such are responsible for up keeping a much greater degree of security than normal users. If somebody uses an Internet banking web site then they should be able to expect that the server and communications with it are perfectly secure, it is up to the site administrator that this confidence is not misplaced.

USING DATA

One of the biggest uses of the obtained personal data is identity theft or fraud. Crimes like this have wide ranging implications. The first type of identity fraud I shall look at often seems as less serious and is less well documented and that is stealing identity and then impersonating that person in social situations in order to defame that person. This commonly happens on social networking websites. The drive behind this is usually some sort of revenge although it may just be a prank or very commonly a crime of opportunity. Crimes like this can normally be rectified by lodging a complaint with the service provider who will look into it and may close down the account.

The second type of identity fraud is seen as more harmful and involves fraudulent uses of the victim's identity in order to gain goods or services. A 2002 report by the cabinet office "estimated that crime facilitated by identity fraud cost the UK £1.3 billion per annum" (www.identity-theft.org.uk). Individuals can often find themselves out of pocket by £10,000 or more. In one case Nasir Ahmed gave, to what he thought was his bank, some information over the phone. He then "heard nothing for a month, then on opening his credit card statement he found that more than £11,000 had been taken, mostly to buy flight tickets and travellers cheques" (www.id-theft-info.com).

One of the problems with identity fraud is that financial institutions are "responsible for undertaking further verification and investigation, and, as appropriate, reporting cases of criminal activity directly to the police" [REFERENCE]. The police have shifted responsibility for investigating identity fraud away from themselves and on to the banks and companies that are getting duped.

"Cyberstalking is a crime in which the attacker harasses a victim using electronic communication" (searchsecurity.techtarget.com). This is a very general description of cyberstalking.

Cybercrime and Identity

Actual harassments include sending offensive messages or images to the victim, putting up false information about the victim on websites or forums or even trying to lure the victim into a physical meeting. Cyberstalking can also take the form of impersonation, that was discussed earlier, to embarrass the individual. Cyberstalking is seen as a continuation of stalking on to electronic mediums and is seen as no less of a threat than its traditional counterpart. Cyberstalking is fought by the police but is it better to just shrug it off before it goes that far. Cyber stalking makes a great use of private

PREVENTION AND POLICING

Cybercrime is a new crime and as such new techniques are needed to prevent and combat it, although some old techniques are still relevant. A lot of identity theft doesn't start online, it starts with people getting details from physical documents and then moving online to continue gaining information. To stop criminals getting data from physical documents you can use old techniques such as shredding all your unneeded documents and securely storing all the ones you need in a safe. These techniques can be carried on into the digital realm. Keeping your inbox empty and deleting and documents you don't need any more are good examples as well as encrypting documents you intend to keep or moving them to an off-line machine or storage medium. Communications have always been vulnerable to interception or even just people listening in. The anonymity of the internet has aided this but encryption has helped combat it with people able to use software like PGP (www.pgp.com/) to encrypt their emails and SSL (wp.netscape.com) for real-time communications.

Policing cyber crime is hard as many crimes do not just occur in the one country but across the perpetrator can be in one country and the victim in another. Crimes like this are hard to deal with as there may be conflicting laws between the countries and extraditing the criminals may be difficult or impossible to do. The Convention On Cybercrime (conventions.coe.int) was an attempt to bring nations together and help police cyber crime as a group with members of the European Council as well as Japan, Canada and the USA.

Criminals can use the Internet to help cover their trails, using anonymous remailers to send messages, going through proxy servers and often changing where they work from or working from an Internet café where it is hard to find out who has been using the computer. Techniques like this make it harder for people to track them down.

CONCLUSIONS

I see the protecting the identity of the individual falls onto both the individual and service providers.

In the social networking examples the service providers can put in features to stop people looking at the individuals page and it ultimately falls to the individual what to put on their pages and who views them, but any information that they display should be seen as compromised and no longer be used as any security questions.

Phishing again targets the individuals directly, it is all the service providers can do to warn and educate its users. The individual is very much responsible for not falling for phishing attempts and it is up to them to be vigilant at all times even though it is the service providers and banks who take the hit on any costs.

Obtaining data through breaching security systems is something that both the individuals and service providers are responsible for preventing. All the individuals can do in these cases install some security software, regularly update it and follow the instructions for online security given to them by their ISP such as never opening attachments from untrusted sources and always check for the golden padlock when entering personal details. The service providers are responsible to actively keeping on top of security on their servers by checking what processes are running, checking all their scripts for vulnerabilities and keeping on top of exploits found in third party software that they may be using.

Policing cyber crimes is very hard and to make real progress on this there will need to be more international collaborations so that people cannot commit crimes and feel safe just because there are physical borders between them and the victim when there are no such borders online.

In closing, it is up to the individual to do all they can to protect their identity as it is their identity that is under threat but by no means does that mean that service providers should not take any responsibility. Service providers should be protecting all the information that they store as well as educating their customers so that they can make the right choices.

Word Count : 2543

REFERENCES

INTRODUCTION

<http://www.crime-research.org/news/08.07.2006/2109/>

<http://www.vnunet.com/computing/news/2071048/identity-theft-rise-uk>

SOCIAL NETWORKING

http://www.nielsen-netratings.com/pr/pr_060511.pdf

<http://www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/>

<http://www.telegraph.co.uk/news/uknews/1556322/Fears-over-Facebook-identity-fraud.html>

http://news.bbc.co.uk/2/hi/uk_news/6910826.stm

<http://www.mtv.com/news/articles/1534725/20060621/index.jhtml?headlines=true>

PHISHING

<http://www.tgdaily.com/content/view/35326/113/>

IDENTITY THEFT

<http://http://www.identity-theft.org.uk/what-if.html/>

www.id-theft-info.com/Case_Study_3.html

<http://www.identity-theft.org.uk/faqs.html>

http://www.id-theft-info.com/Case_Study_3.html

CYBERSTALKING

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci865159,00.html

http://www.wiredsafety.org/cyberstalking_harassment/csh0.html

<http://lifeandhealth.guardian.co.uk/relationships/story/0,,1986981,00.html>

PREVENTION AND POLICING

<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

<http://wp.netscape.com/eng/ssl3/>

<http://www.pgp.org/>