Identity theft

Berni Dwan

Almost every week I hear a news report or read a newspaper article about identity theft. It will either be about yet another person who suffers at the hands of the identity thief, some new software or hardware breakthrough that will foil the activities of the identity thieves, or, a new report or study telling us the cost of identity theft to business. Six men have been jailed after a £345 000 plot to defraud banks by obtaining fake identities over the Internet, said a recent *BBC News* report. The men used house auction websites to find out the details of people who had died. With the information, they forged documents to open bank accounts and receive loans from Lloyds TSB and the Halifax and Co-operative banks. The men were jailed for between 18 months and four-and-a-half years.[1] According to the Federal Trade Commission Identity Theft Data Clearinghouse 215 000 people had their identities stolen in 2003, up from 162 000 in 2002. A third of the thefts were used to perpetrate credit-card fraud, while 21% were used for phone or utilities fraud.

I'm constantly hearing about it because there is money to be made from it, and the perpetrators are correct so far in thinking that it is worth the risk. There are handsome profits to be made from email phishing and Web phishing, and I am continually amazed at the way people can still be tricked into divulging their personal details. To the tune of $53 billion (42.6 billion) in 2002 alone according to the Federal Trade Commission. While traditional dumpster diving, mail theft and the contents of lost or stolen wallets have reaped handsome profits over the years, the digital world offers a lot more opportunities to those with enough imagination and determination. The latest verification scams, according to the Identity Theft Resource Centre include E-Bay, Best Buys, Discover Card, e-gold.com, ebay-verification.net and change-ebay.com. Almost all Internet server names have been used for this scam as well, they say, and companies that have been known to be victims of this scam include: AOL, MSN, Earthlink, PayPay, Discover Card, Bank of America, Providian and Wells Fargo.

Phishing trips take place on email and Web servers, and in both cases the catch can be surprisingly lucrative. Email phishing typically originates with an email that warns of some problems with an account, promotes a special deal, or directs you to a Web page that is identical to the site of the company or bank you normally do business with. These phishers don't miss a trick, and they ensure that the graphics, forms, and links on their rogue Web pages are clones of the real thing. With a note of urgency obviously designed to deter the victim from deliberating for too long, the email often says that account information needs to be updated right away and asks you to click on a link that will take you to the website and an information update form. The linked page will look just like the company's actual website but the information will be sent to waiting identity thieves and not the legitimate company. Here is a typical and recent example given on www.antiphishing.org:

Dear Wells Fargo Valued Customer!

Please read this important message about security. We are working very hard to protect our customers against fraud. Your account has been randomly chosen for verification. ***This is requested to us to verify that you are the real owner of this account.*** *All you need to do is to click on the link below. You will see a verification page.* ***Please complete all fields that you will see and submit the form.*** *You will be redirected to Wells Fargo home page after verification.* ***Please note that if you don't verify ownership of account in 24 hours we will block it to protect your money.*** *Thank you.*
http://www.wellsfargo.com/verify/

From my own perspective, the phrasing and grammar in this letter would have raised my suspicions anyway. Do the sentences in bold read like official bank speak to you?

These identity thieves must have studied the psychology of advertising because they are very aware of the trust consumers' place in well-known trademarks, and they are using that trust against them. Even experts admit that sometimes it is hard to differentiate between real mail and phish. So, in actuality, the ID thieves are committing a double ID theft, first the corporations then, the consumers. The notes appear to be personal, referencing an open account at a bank or website, but they are really just spam. Sent to a wide enough audience, an emailing referencing Citibank or eBay will hit plenty of people who really are account holders. 90 different versions of the scam emails appeared in November and December 2003 and now there are about five new attempts every day according to the Anti-Phishing Working Group. Targeted companies include eBay, PayPal, Citibank, Bank of America, Best Buy, Earthlink, AOL, the FDIC, and AT&T.

Remember, URLs that begin 'http' are not secure. Only those that begin 'https' are secure sites to send sensitive information. It is worth checking to see if that 'http' changes to 'https' when you go from your bank's main Web page to your personal password protected account information. Furthermore, for years, consumers have been told to look in their Web browser's address window to ascertain the veracity of a website. An address that seemed suspicious, perhaps beginning with a numeric address, like 211.154.171.106, or containing a series of stray characters was a sure sign of trouble, suggesting to users they'd land-

ed in a bad place, says Ravalli County Bank in Montana.[2] A simple address like www.msnbc.com was considered a green light. But a flaw in Microsoft's Web browser allows a malicious website operator to "spoof" his/her locations, like for example the email that linked to a spurious www.Earthlink.net, the real site actually sitting on a Web server in China and designed specifically to steal debit and credit card numbers. "These spoofed addresses are incredibly easy to create", says Ravalli Bank, and to prove it they invite you to type http://www.amazon.com@ravallibank.com in the address bar of Internet Explorer. "It looks like it should take you to Amazon.com", they say, "but you'll wind up at our homepage. That's because Internet Explorer ignores everything before the "@" sign – one of the flaws that phishers like to exploit."

Phishing attacks have progressed from the straight email messages with Web links to phony sites. Hackers have now developed two Trojan horse programs known as MiMail and MmdLoad that arrive as email attachments. If you double-click on the attachment, it unleashes a program that not only takes you to a phony sign-on screen but also uses your email client to send a copy of the booby-trapped message to everyone on your contact list. The latest phishing scam targeted at Australian Westpac bank customers is 'smart as a whip.' The architects of the scam adopted a more insidious Web redirection technique to bamboozle victims, reports *ZDNet Australia*.[3] "Activating the link in the email directs the victim to a fake version of the site but also opens an authentic copy of the site in a second browser window behind it. The fake version of the site asks for the victim's account access details but returns an error message if he or she attempts to use it. The victim is then sent to the real site unaware that they've been duped."

A Web phishing scam on the other hand sends you to the real company's legitimate Web page, but a pop-up form asks you to enter personal information like your account name, password, credit card number, or Social Security number. There's no way to tell it's a scam because there is no address bar on the pop-up form, and anyway, it looks extremely convincing. Of course the information you enter is sent to fraudsters and not the legitimate company.

The Identity Theft Resource Centre[4] is a national non-profit organization in the United States that focuses exclusively on identity theft. One of ITRC's co-founders, Linda Foley was herself the victim of identity theft in 1997 when her employer used the information on her tax forms to get credit cards and a cell phone. At that time, there was little information for victims to use and no network of people with whom to talk, and it became apparent to Linda that a specialised programme was needed, focusing on victim assistance and serving as a clearinghouse of information. The ITRC raises some important questions. Why are students, the elderly and the military more vulnerable to identity theft than other groups in society? Who is supporting and who is opposing legislation on identity theft? Who are the identity theft criminals and are there any similarities among them? It is of prime importance therefore, say the ITRC, to understand how thieves steal your information via the telephone and computer systems.

Why are students, the elderly and the military more vulnerable to ID theft than other groups in society?

Financial institutions are getting better at preventing identity theft through improved training and screening, and the use of fraud-detection software that can spot suspicious activity where it is most likely to occur – an impostor opening new accounts with somebody else's personal details. This may improve matters for the victims, who will not notice for some time that their identity has been used to process transactions unknown to them, and when they do find out, the damage has been done. The association of large banks, known as the Financial Services Roundtable[5] obviously thinks that $1.5 million is well spent in establishing the Identity Theft Assistance Centre to help victims, and it will open in May of this year. Wells Fargo & Co. will operate the centre, while other financial institutions will participate on a voluntary basis. Consumers who believe they are victims of identity theft will contact their bank or credit card company, who will record the details on a uniform affidavit, and then contact the Identity Theft Assistance Centre with the information. So, consumers only have to make one phone call and the Identity Theft Assistance Centre will then act as a one-stop shop for the financial institutions reporting the compromised accounts. The centre will then call the victim and gather all the necessary information to establish if their account has been compromised. It will also work with law-enforcement agencies.

The Financial Services Roundtable is establishing the Identity Theft Assistance Center to help victims

"As our reliance on interconnected networks has grown with the rapid mainstreaming of the Internet, the problem of identity theft has been exacerbated", says C. Maxine Most, Principal and founder of Acuity Market Intelligence. In her article, Biometrics and Trusted Identity[6] combating identity theft she says,

"The stakes are higher than ever and the game more compelling for perpetrators of fraud. Instead of grabbing a gun and head-

ing down to the corner convenience store, would be thieves sit in the comfort of their homes and surf their way to mayhem. With a few key bits of information — a social security number, billing addressee, mothers maiden name — identity thieves easily appropriate identities and instantly open credit card accounts, make purchases and apply for loans."

"The Initial focus on combating identity theft has been on addressing consumer complaints", she says, however, broader economic implications and national security concerns are far more insidious and the consequences potentially dire. Consider 9/11 the highest level of disaster possible when identity theft goes unchecked. Hijackers easily obtained the base form of ID in the US; driver's licenses. Why should biometrics vendors care? Successful biometrics market development requires identifying and solving high point-of-pain problems. In this regard, identity theft is a ringer. This is a point of pain that directly ties consumer fear and healthy, sustainable economic development to homeland security. The problem of identify theft is enormous and biometric identification in and of itself cannot prevent the theft or fraudulent use of thieved identities. However, it is highly unlikely that individuals will want to leave biometrics markers behind as they engage in criminal activity."

Mike Small, director of eTrust strategy at Computer Associates, wonders if we are not turning into a Kafkaesque[7] society, where people (victims of identity theft) are unable to prove their identity? "And what if someone steals my DNA, I cannot revoke my DNA identity – unless that is they take me out and shoot me!" "Technology will not solve all the problems. Thieves are clever and will always find the weakest link. Technology can only manage the pieces that it is designed to manage.

We must look at the whole system", says Small, "and the weakest point is people".

The perpetrators of identity theft are also counting on the vulnerability of human emotions in the face of lost credit cards. "They will phone the person whose cards they have stolen, posing as the helpful person who found them. They will then ask you to give details to prove that the card is yours (details they will of course need when they go to use the card themselves). Another weak link occurs when you receive credit card offers by email, and simply discard them in the recycle bin. They are sitting there waiting to be filled in with your details by A N. Other." Alternatively, a fraudster will take over another person's identity or account by finding information out about them and contacting the card issuer for a replacement card.

With identity management it's all a matter of lowering the cost of risk, says Small. The French introduced smart cards as credit cards 10 years ago to counteract identity theft. So why didn't they do the same in the UK? "The amount of fraud suffered didn't warrant the cost", says Small. "Security is about the cost of managing the risks versus the cost of the risk. As risks go up banks tighten the system. Different types of organizations have different attitudes to risk. Banks live with risk – repayment amounts are based on how much they think you are capable of paying back. Government organizations on the other hand behave as if every risk is unacceptable. For them, no measure is too great. Did you know that Bury Council did a risk analysis of Bury taking part in the Britain in Bloom competition? Before putting hanging baskets on the lampposts, the gardening society had to get written reports from the lamp post manufacturers and the contractors who installed the lamp posts to ensure that the hanging baskets could be safely accommodated. Is this appropriate?"

"What context is the identity being used in – a bus pass, a credit card, a passport? Identity is simply an enabler to do with access control, and consequently there has to be a range of solutions. Much more fine - grained methods are needed. There is no absolute answer, only appropriate action. As you connect more and more systems together more vigilance is needed", says Small.

Mathieu Gorge, Managing Director of VigiTrust Pro-Active Enterprise Security says "Identity theft is only one part of a bigger set of risks that need to be addressed, and physical security must be tackled first", says Gorge. "There is no point in having a state of the art IT security system if anyone can walk in the front door. Staff should be trained to foil social engineering tactics. Regarding the management of access / biometric cards, companies need to have audit trails that can guarantee the whereabouts of everyone – a system that can achieve full non-repudiation"

"One problem is how to manage multiple identities accessing multiple systems within the same organization," says Gorge – "people accessing different levels of systems on a need to know basis. An increasing number of customers are looking for two-factor authentication[8] or challenge-response systems for employees remotely accessing the corporate network. The good thing about these systems is that you can easily revoke a users rights if you have any reason to be suspicious."

In fact Vasco[9] has an interesting device called Digipass especially designed to counteract phishing. It is based on the premise that phishing schemes can only succeed if the information the fraudster wants to obtain is static (user id's, PIN codes, credit card information). Digipass creates one-time passwords, changing every 36 seconds. In addition, it calculates digital signatures, allowing bank account holders or credit card users to perform online transaction without revealing any secret information on the Internet.

"The challenge", says Gorge, "is to make sure that you provide the right access levels, accompanied by a clear audit trail that provides accountability. A solution is only as good as the procedures built around it. You must be able to monitor an individuals usage of the corpo-

rate network, building up a profile of his/her habits. Then if the usage pattern suddenly changes it can be flagged on the system. You can then do either of two things – look at the forensics and preserve the evidence, or activate your corporate security response. The idea is to be proactive", he concludes.

References

1 BBC News 2003/11/21

2 www.ravallibank.com – this community bank in the US has a really informative section on identity theft

3 http://www.silicon.com/software/security/print.htm?TYPE=story&AT=39118902-39024655t-40000024c

4 If you think you have received a SCAM, please forward the ENTIRE email to ITRC at: itrc@idtheftcenter.org and they will forward it to the FBI for you and let you know if it is a confirmed scam.

5 www.fsround.org

6 http://www.findbiometrics.com/Pages/feature%20articles/identitytheft.html

7 "I can prove at any time that my education tried to make another person out of me than the one I became. It is for the harm, therefore, that my educators could have done me in accordance with their intentions that I reproach them; I demand from their hands the person I now am, and since they cannot give him to me, I make of my reproach and laughter a drumbeat sounding in the world beyond."

8 Two-factor Authentication is when you have to provide something you know (a password or PIN), and something you have (smart card or token) before being recognised by the system and granted access. Two-factor authentication provides a greater level of security because you need to have both to gain access.

9 See details at www.vasco.com

GETTING THE WHOLE PICTURE

Policy domain mapping

Peter Stephenson

This month's column looks at policy domains and the application of threats and the mapping of interdomain communications.

Last month I introduced you to security policy domains. The notion of policy domains is not new. The CORBA (Common Object Request Broker Architecture) Glossary1 defines it as:

"A domain whose objects are all governed by the same security policy. There are several types of security policy domain, including access control policy domains."

Smith, in a presentation for NIST[2] defines a security policy domain as:

'The scope over which a security policy is enforced. There may be subdomains for different aspects of this policy.'

Sanchez, Waitzman, Condell[3] et al describe security policy domains as:

'…an environment or context that is defined by a security policy, a security model, or architecture, and includes a set of system resources and a set of entities that have the right to access the resources.'

A couple of months back we introduced two additional definitions (SANS and M-Tech). In that issue we posited our own definition, the one with which we will continue to work:

A security policy domain is a set of requirements for system configurations that enforce rules of behaviour for users, administrators and systems intended to protect those systems and the data they contain.

Regardless of the source of the definition, the concept is consistent: security policy domains are those logical and physical components of an enterprise governed by a single security policy. The policy may be explicit, as in a corporate policy, procedure or guideline, or, more commonly, implicit as in the configuration of devices governed by a policy. Typically, for practical purposes, we consider those configurations as the instantiation of the policy. Our working definition reflects this. This week we'll do a bit more work with policy domains including applying threats and mapping interdomain communications.

Identifying policy domains

The process of identifying policy domains has a couple of aspects to it. First, we want to group data (and the devices upon which the data resides) based upon sensitivity and criticality. On the surface that sounds pretty simple. However, we also are concerned with the use to which the data will be put.

For example, we may have data that we consider to be at a level 5 (on a scale of 1 to 5, 5 being the most sensitive) sensitivity and 5 criticality (same scale as sensitivity).