

How do you deal with Internet fraud?

Summary

Internet fraud should be addressed as two specific issues: fraud that uses Internet technology as an integral part of the fraud; fraud that is already taking place by other means and the Internet is merely another method of delivery.

Methods exist that stop fraudsters misusing the technology, which can be rapidly implemented, but factors such as industry acceptance and concerns over potential liability if previous security claims could be claimed to be inaccurate will delay introduction. Much effort is spent promoting logos and confusing self-regulation, and trying to catch fraudsters, whilst the adoption of formal standards and accreditation for security (such as ISO 17799) are only starting to take place.

New Internet environment crimes may exist, such as defrauding machines or causing business harm by denial of service or virus attacks, and these will require social and legal steps to address them. However, the Internet has provided the fraudster with access to a significantly bigger market than ever before and effort will be required to create an environment where fraud is resisted by design rather than by insurance.

Introduction

Internet fraud is said to be big business. But what is it, and does using the Internet create the fraud, or is the Internet just a different way of delivering 'traditional' fraud.

Fraud is essentially persuading someone of something with intent to deceive, perhaps with criminal intent. The deceit may be to persuade you to part with money, goods, services, rights or information.

For the purposes of this paper we are not going to examine methods of fraud, but look at the general techniques, how they are applied, and how, if at all, the Internet can be used to make those techniques easier for the criminal to use either to carry out a fraud or to escape detection.

General techniques of fraud

The key to fraud is to persuade you that something is real, when in fact it is not. Once you accept that the fake is real then the fraud can take place – whatever it is. Whether you are buying the Eiffel Tower in Paris or the Golden Gate bridge in San Francisco (both are real and have been seen by millions of people – and have been regularly 'sold') the essence is to believe the proposal that is put to you.

Other types of fraud essentially persuade you to do something in the (wrong) belief that it should be done, or to accept something in settlement that proves to be without the value you were led to believe.



But they all come back to the same thing – the fraudster has to persuade you that his vision of the world is the correct one.

How do we normally counter fraud

In ordinary life there are many things set up to help avoid fraud. Mostly we rely upon physical things – buildings (such as banks) help to prove to us that we are dealing with something real – talking to people on the telephone on a number that is in a directory helps us believe that they are who we expect. At a more sophisticated level, businesses have to be registered and the directors names and addresses made public. There are also agencies with a duty to respond to complaints over the trading practices of businesses.

How does the Internet map to the real world

The Internet is rather different. The biggest problem for the Internet user is that there is no physical reference to use. You can't go to a physical bookshop at www.amazon.com. You have to believe what the computer tells you, and that is the start of the problems.

We have many practical examples where people get the physical world wrong – they put their bank cards into fake ATMs and enter their PINs, they tell their friends and children their passwords (sometimes in public), they sign up to 'get rich quick' deals with people they don't know – so how well are we set up to handle the Internet world, where web sites are just exactly as good as their designer intended?

The practical answer is just barely. The Internet is marketed as an anonymous zone. Information is free and users are anonymous. Now some of those features are desirable. When you go into a store it is the store that has to tell you who they are. If you pay with cash they will never know who you are and none of your legal rights are affected. They give you a receipt and you can check any of the details and get corrections made on the spot. If you want credit you have to tell them more about you, but not necessarily very much.

The Internet, by comparison, is anonymous whether you are the seller or the customer. For the seller it is as anonymous as they want to make it. This, of course, might be thought of as attractive to a fraudster.

Avoiding obvious frauds on the Internet

Some potential sources of fraud – misrepresenting a business as that of someone else – are being slowly dealt with. Domain name registration has almost reached the point where there is some certainty that www.harrods.com is the web version of a famous department store in Knightsbridge, London. But it is still very far from being fully resolved. It is still possible to register www.harrodds.com, www.harrodss.com. You can copy the real thing without too much difficulty, and with a bit of luck and some spelling mistakes a fraudster can still be in business.



But this type of fraud could be avoided by legislating to bring web site name registration into line with company registration rules, where similar names and "passing off" are already dealt with. The methods for obtaining web site names that are primarily for 'trade' could also be addressed to ensure that they can only be obtained by registered businesses, and that the link between the domain name and the registered business is a matter of public record.

Some less obvious frauds

The Internet uses a technology called TCP/IP in order to send information between one point on the Internet and another. Unfortunately it was not designed to be secure, it was designed to be resilient. As a result it is possible to read information that travels around the Internet, and also to alter it. Therefore, it is possible both to read information that is not protected and copy information that has been protected using cryptography, (a technique that makes information unreadable to the unauthorized) and to change the unprotected information without being detected.

The effect of this is to create a situation where fraud can be carried out even when a genuine transaction is taking place. Fraud might include putting other recipient's names on the distribution list to make you believe they are also involved or in agreement with what is going on. (This can happen in the physical world – processing a credit card transaction multiple times on paper and forging the signature from the valid bill.)

The fraud is subtle because it is impossible for either party to detect. It is effective because the fraudster may have gathered information that allows them to completely impersonate both parties in the future.

Solutions for technical problems

These frauds require a manipulation of the Internet technologies, and so can be resisted by technology. However, the technology being marketed to solve this problem Secure Sockets Layer (SSL), in the way in which it is usually implemented, has fundamental weaknesses, and has been shown to be capable of being defrauded. Many other schemes, based upon codes of practice and logos shown on web sites, although worthy in themselves, are equally capable of being defrauded. It seems strange that some advertising appears to suggest encryption technology using a 40 bit algorithm is perfectly secure for commerce, whilst also saying that 128 bit algorithms are essential.

Alternative technologies such as those from ArticSoft are being delivered now that allow end users to gain immediate validation of web site content itself. They require software to be present in the machines of the end users to act on behalf of the user to carry out checks that the user can be prevented for doing themselves by competent fraudsters.

They also require competent registration procedures for Internet traders to make it more difficult for a fraudster to enter the system and pretend to be genuine. Such registration procedures are claimed to be in place for SSL.



One of the most important international developments for defining security behaviour has been the adoption of the international standard ISO 17799 Code of Practice for Information Security Management. It is a comprehensive management standard for addressing the full range of issues for protecting information. Sensible adoption and application of the standard could provide significant benefits both to business and consumers. Self regulation schemes would do well to consider adopting it as a means of providing a common frame of reference for security and privacy claims.

Solutions to help user understanding

Web site design

The basic approaches to developing and designing Internet many web sites are based upon ease of implementation for the web site consistent with current 'fashion' for both appearance and implementing the latest technology. The user security experience is largely of unexplained transitions to web site addresses that do not relate to where they started. That contradicts the user's real world experience and actually promotes fraud potential by forcing the user to either accept inconsistency or ignore it. Both positions mean the fraudster can insert his version of reality without ready detection.

The move to adding unexplained pop-up windows, unexplained other windows, moving information and other similar features have to be contrasted with the user confusion of the site he or she is dealing with and the fraud potential that brings. Also the introduction of monitoring software and similar programs can only increase the level of fundamental mistrust the user has in the Internet. From a domestic user point of view this is little short of hacking. So how do you know the good guys from the bad?

Re-making the presence of entire sites overnight contradicts the physical world where change has to be announced and is very evolutionary. It happens in slow time where regular customers build up acceptance and experience. Trying to educate users to live with rapid change is creating cultural change in Japan where new product take-up rates are reducing rapidly.

Security presentation

Security information needs to be proactive and tangible. Security solutions that rely upon static logos or that require the user to perform specific actions and then carry out manual checks of their own are flawed. Physical world checks do not work that way so there is no transfer of experience to the Internet.

Security information goes far beyond making claims about '40 bit SSL' technology. In the physical world you know where the store is and it can't move rapidly. The location of an Internet site is less than clear. Provable information is needed to show the trading address of the business, real contact information, governing law and an effective link from that to any transaction being undertaken.

Security information must be considered when transactions fail to complete just as much as when they succeed. In the physical world the user can see when a transaction has not completed, but the Internet lacks that visual experience.



Forms that re-set without explanation, or fail for reasons that are not explained fully on them, contribute to the inability of a user to detect fraud taking place. Such techniques are commonly used by fraudsters to gain information.

Does the law help users

Considerable efforts are being made by law enforcement agencies to prevent fraud (any many other criminal or civil wrongs) using the Internet and to prosecute wherever possible. Data protection, whether stemming from the European Directive, Human Rights, the US Health Information Portability and Accountability Act (HIPAA), seems to have enjoyed less visible action, although that information is needed in addition to credit card information in order to commit Internet frauds such as identity theft.

The problem the law faces is created by the non-national nature of the Internet, and the national nature of law. Even if there are suitable offences, being able to proceed successfully is difficult, and for the ordinary consumer rather daunting. For the consumer, producing available evidence long after a fraud has been detected is also problematic. The situation is further confused by the desire of valid industry to collect as much consumer information as possible – something the fraudster also wants, but for different reasons.

One also has to be careful that law is not used instead of industry action. Making something an offence does not mean that nothing need be done. The recent US Digital Millennium Act is perceived by some as preventing the exposing of inadequate security mechanisms. Given that the user is actually the one exposed by security inadequacies, careful consideration needs to be given over user reaction to such a situation.

Conclusions

Internet fraud has two distinct strands to it.

One results from the differences between doing business in the physical world and the dematerialized world of the Internet. This gap has been accentuated by the 'world of the Internet' to the point where the user has no conventional reference points. This leaves the user ill placed to make adequate judgments of any kind, not merely about security and the possibility of fraud.

The other results from technical inadequacies in the infrastructure used by the service providers. Lack of clear regulation has allowed registration practices to develop that are not acceptable anywhere else for doing business. Previously available security mechanisms have been implemented in ways that fail to protect the user and which require, if followed, unreasonable user effort and significant user education.

Mechanisms such as the law may be able to provide some assistance, but care needs to be taken that the law is not used as an excuse for inadequate business practices. It would be sensible to ensure that a duty of care to implement best practice is included in legislation to expose any who have failed to protect themselves, their shareholders or their customers.



Self regulation is another essential approach, but it must avoid becoming all self and no regulation if it is to carry real conviction to a suspicious user community, and its practices must be clear, obvious and understandable to the ordinary man. The paper world has already done this so wheel re-inventing is not required.

The introduction of new technologies places responsibilities upon their implementers. The developers have a responsibility to get it technically right. The implementers have a responsibility to deal with its social and cultural dimensions, and cannot stand back and ignore these. Professional web site design carries a great deal more responsibility than merely sorting out key words, search terms and a site map.

References:

- 1 Web spoofing allows an attacker to create a "shadow copy" of the entire site
www.cs.princeton.edu/sip/pub/spoofing.html
- 2 Spoofing the Whole Web. www.bau2.uibk.ac.at/matic/spoofing.htm
- 3 What is web spoofing? www.nmrc.org/faqs/hackfaq/hackfaq-9.html
- 4 Dartmouth PKI Lab Web Spoofing Demonstration
www.cs.dartmouth.edu/~pkilab/demos/spoofing/index.shtml
- 5 Some Web spoofing may be noticeable, so it is helpful to keep these tips in mind: www.washington.edu/computing/windows/issue22/spoofing.html
- 6 Navigator and Microsoft Internet Explorer. Web spoofing allows an attacker to create a "shadow copy" of the entire World Wide Web. Accesses to the shadow Web www.secinf.net/info/www/security16.txt
- 7 The Digital Millennium Copyright Act (DMCA). The DMCA is being used to silence researchers, computer scientists and critics. www.anti-dmca.org
- 8 Provisions in Chapter 12 of the US Copyright Act, enacted in the Digital Millennium Copyright Act ("DMCA") must be repealed or struck down as unconstitutional www.petitiononline.com/nixdmca/petition.html
- 9 The New York lawsuit appears to be the first to use the Digital Millennium Copyright Act (DMCA) to try to restrict a computer program.
www.wired.com/news/politics
- 10 Authentication Who's Site Is It Really? by ArticSoft Published: March 17, 2002 http://techlibrary.corn.com/data/rlist?t=soft_10_136
- 11 The Changing Face of Web Security by ArticSoft Published: March 17, 2002 Document Type: White Paper
http://techlibrary.banktech.com/data/rlist?t=soft_10_136_4
- 12 Credit Card Fraud, Link to Top Ten Home Page. The Bait: Surf the Internet and view adult images
www.ftc.gov/bcp/conline/edcams/dotcon/credit.htm
- 13 Credit card fraud hit 1 in 20 users. And identity theft hit 1 in 50 during past year, study shows. By Bob Sullivan MSNBC.
www.msnbc.com/news/718115.asp



- 14 Around 900,000 victims across 22 countries. The biggest credit card fraud ever. Fraudulent credit card transactions generated using adult web site merchant.
www.faughnan.com/ccfraud.html
- 15 5.2 percent of respondents saying they'd been victimized by credit card fraud in 2001 -- and 1.9 percent said they'd been victimized by identity theft
www.cnn.com/2002/TECH/internet/03/04/fraud.online.survey/
- 16 ISO 17799 (2000) references may be found at www.bsi-global.com and at www.xisec.com