Exploitation and Fraud on the Internet: Some Common Practices

Mark Griffiths

Most people who e-mail and use the Internet regularly are bombarded daily with spam (ie, junk e-mail). Many of these offer "get-rich-quick" schemes or offer so-called "investment opportunities" that look too good to be true. Thankfully, most of us become accustomed to these types of Internet scam and, apart from clogging up our e-mail boxes, there is little in the way of long-term damage. There is also the general issue of unscrupulous operators who take money from customers for some kind of service, and then fail to deliver that service. The best pre-emptive way to deal with these types of exploitation is to trade with known companies - preferably those who have an offline trading arm. However, there are many types of Internet exploitation and fraud that are much harder to spot. This short article attempts to highlight some of these practices including both legal and illegal.

Commercial Exploitation and Online Tracking

Perhaps one of the most worrying concerns about Internet exploitation is the way sites can collect many types of data about their customers. Customer data are the lifeblood of any company. Internet customers can provide tracking data that can be used to compile customer profiles. Such data can tell commercial enterprises (such as those in the sex and gambling industries) exactly how customers are spending their time in any given financial transaction (ie, which sites they are accessing, for how long, and how much money they are spending etc). This information can help in the retention of customers, and can also link up with existing customer databases and operating loyalty schemes. Companies who have one central repository for all their customer data have an advantage. It can also be accessed by different parts of the business. Many consumers are unknowingly passing on information about themselves which raises serious questions about the gradual erosion of privacy. Customers are being profiled according to how they transact with service providers. Linked loyalty schemes can then track the account from the opening established date.

The technology to sift and assess vast amounts of customer information already exists. Using very sophisticated software, companies can tailor its service to the customer's known interests. When it comes to some activities (Internet gambling, for instance), there is a very fine line between providing what the customer wants and exploitation. The gambling industry sell products in much the same way that any other business sells things. On joining loyalty schemes, customers supply lots of information including name, address, telephone number, date of birth, and gender. Those who operate Internet gambling sites will be no different. They will know your favourite game and the amounts you have wagered. Basically they can track the playing patterns of any gambler. They will know more about the gambler's playing behaviour than the gamblers themselves. They will be able to send the gambler offers and redemption vouchers, complimentary accounts, etc. Supposedly all of these things are introduced to enhance customer experience. Benefits and rewards to the customer include cash, food and beverages,

entertainment **and** general retail. However, **more** unscrupulous operators will be able to entice known problem gamblers back onto their premises with tailored freebies (such as the inducement of "free" bets in the case of Internet gambling).

This is not just a concern for adults. The US Center for Media Education (CME) claim advertisers used a variety of online methods (like "infomercials") to collect detailed data about children and compile individual child profiles. This information is then used to establish direct and **intimate** relationships with children online. The CME **claims** children's privacy is routinely threatened in encouraging them to disclose personal information about themselves and their families with some sites offering gifts and prizes. This technology makes it possible to monitor every interaction between the child and the advertisement allowing firms to create personalized marketing for a child. The CME have urged the US Federal Trade Commission to develop safeguards for children and claim that **these** advertisements would infringe American regulations **that** put safeguards on broadcast media like the television. They recommend that there should be no children's content directly linked to advertising and that direct interaction between children and product spokescharacters (like Kellogg's *Tony the Tiger* and Frito Lay's *Chester Cheetah)* should not be allowed.

Finally, consumers are not always as anonymous as they might think when they visit health sites because some sites share visitors' personal health information with advertisers and business partners without consumers' knowledge or permission. Some sites allow third-party advertisers to collect visitors' personal information without disclosing this practice. As a result, visitors often get e-mails from advertisers about **their** products and services. Information can be collected during a variety of tasks including the visiting of chat rooms and bulletin boards, searching for information, subscribing to electronic newsletters, e-mailing **articles to friends** or filling out health-assessment forms. This allows third parties to **build detailed,** personally identified profiles of individual's health conditions and patterns of Internet use. There are also some Internet marketing companies whose aim is to locate individuals who have not even registered for specific products. These companies use "search robots" that trawl the Internet for specific types of information (like the **names and** e-mail addresses of those who post at certain discussion lists). The information is then collated to generate lists for specific products.

Investment Scams

A known fraudulent use of the Internet concerns investment scams. One popular technique is to put out an advertisement on the Internet looking for backers for new products. Many people take the bait by sending in cheques. One such high-profile case was that of Matthew Bowen who set up a company called *The Next Microsoft!*[1] and advertised for investors in a new product he claimed he had designed. Over 150 potential investors sent cheques to Bowen totalling $150,000. Bowen was eventually caught and sentenced to 10 years in prison. This was a very important case with regards to Internet fraud in that it was one of the first to give out a very harsh prison sentence. Another high profile case involved a huge $100 million scam masterminded by David Laing who set up a fake company called Personal Choice Opportunities. The company concerned speculation about peoples' life insurance policies and managed to attract over 1500 investors across the US. The Internet was deliberately used to feed into a wide and diverse range of investment broker networks. David Laing was eventually caught after spending $26 million gambling in Las Vegas and was given a 10-year prison sentence for the Internet fraud.

Share Ramping

Another well-known scam is "share ramping" where fraudsters buy shares in particular companies and then spread rumours about those companies on the Internet which subsequently increases the share value prices of those companies. The fraudsters then sell the shares they **bought** for a big profit. There have been hundreds of instances of this "pump and dump" strategy.

Embedding

One seemingly common exploitative practice is the hidden "embedding" of certain words on an Internet site's webpage **through** the use of "meta-tags". A meta-tag is a command **hidden in** the Web page to help search engines categorize sites (ie, **telling the** search engine how they want the site indexed). One common way to get extra traffic flowing through a webpage is to embed common words that people might be searching for on the Internet (eg, "Disney"). Some Internet sex and gambling sites use this practice to their advantage. For instance, if an Internet casino used the word £compulsive gambling" embedded in their webpage, what they are saying is "index my casino site in with the other compulsive gambling sites" so people will "hit" this site when they are looking for other information related to compulsive gambling. Someone looking for help with a gambling problem will get these sites popping up in front of them. This is a particularly unscrupulous practice that at the moment is perfectly legal.

Internet "Webpage" Forgery

Frauds rely on **gullibility** of the victim and the credibility of the criminal engaging in the fraudulent activity. On the Internet, this might perhaps translate into having very state-of-the-art webpages on the Internet with credible sounding backers. Another technique employed is the creation of false company reviews by pretending they are from the webpages of established and well-respected Internet business and investment magazines. Copycat forgeries on the Internet of bona fide investment magazines have occurred and investors have no real way of knowing that the page they are reading is a fake. This practice could only happen on the Internet as it is impossible to run a similar fake story in a printed newspaper without someone spotting it.

Circle Jerks

Another potentially unscrupulous tactic used by both Internet sex and gambling sites is telescoping windows often referred to as "circle jerks". If someone online accesses a particular type of site and try to get out of it, another box offering a similar type of service will usually "pop up". Many people

find that they cannot get out of the never-ending loop of sites except by shutting down their computer. Obviously, those sites that use "circle jerks" hope that a person will be tempted to access a service they are offering while their site is on the screen.

Although this is not an exhaustive list, it has hopefully provided a brief overview of some of the main types of Internet exploitation-some of which is clearly criminal. Until **those in the** criminal justice system familiarize themselves with the **methods** and practices of those in search of making money in any way possible on the Internet, those in the fraud and exploitation game will always be quick to capitalize on legal loopholes.

Mark Griffiths is a Professor in the Psychology Division at Nottingham Trent University.