A brief overview of online gambling scams

The internet has opened new possibilities for the development of online gambling scams, which target a large number of users. The vulnerability of users and the 'credibility' of fraudsters are key elements in online gaming scams. Professor Marc Griffiths, of Nottingham Trent University, examines in detail some of the most common internet gambling scams and how 'technology is being used to exploit and defraud thousands of people'.

Many fraud and scam schemes have moved into technological media, such as the internet. This article briefly overviews some of the main types of gambling fraud that currently operate on the internet including:

- lottery scams;
- fake gambling site scams;
- betting software scams;
- gambling 'bonus' scams; and
- 'twofer' scams.

These are briefly overviewed in turn.

Lottery scams

Many people receive bogus e-mails notifying them they have won a lottery (Griffiths, 2003a; Whitty & Joinson, 2009). The majority of these scams are either the 'Dutch Lottery', 'Spanish Lottery' and 'Canadian Lottery' schemes, although there are many others. The theme is always the same and they appear to make a lot of money for those that instigate the scam. According to press reports a few years ago, the Canadian Lottery scam netted over $5 billion from US victims and was making around £500,000 a month in the UK (Griffiths, 2004). Typically, a person receives an e-mail saying that they have won a lottery and they need to reply to claim their winnings (Whitty & Joinson, 2009). If the person replies, they will then receive emails - or phone calls and faxes - that move the person on to the next phase of the fraud. The person will be told that they need to pay a fee - which can be variable - to cover transfer and administration costs (sometimes termed an 'unlocking fee').

Sometimes the fraudsters ask for a person's bank details so that they can deposit the winnings. When this happens, the fraudsters can also steal money directly from a person's account (Whitty & Joinson, 2008). The obvious reason why such e-mails are fraudulent is that the person has not bought a lottery ticket. However, frausdsters have started to use slightly different tactics. Below is an extract from an e-mail that I received in my inbox:

'We are pleased to inform you of the result of the Lottery Winners International programs held on 14 January. You have therefore been approved a sum pay out of US $500,000. CONGRATULATIONS!! Due to mix up of some numbers and names, we ask that you keep your winning information very confidential until your claim has been processed and your prize/money remitted to you. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 200,000,000 company and 300,000,000 individual email addresses and names from all over the world'.

Here, the person appears to have had their e-mail address randomly selected into a prize draw (rather than having to have bought a ticket). To claim the prize, recipients of the e-mail are again asked to pay an administration fee. One of the more worrying aspects is that those people, who have responded to these types of schemes and frauds before, will find themselves named on 'mooch' and 'sucker' lists that are sold by specialist brokers to the fraudsters. If a person has been duped once, they will almost certainly be targeted again (Whitty & Joinson, 2008). Thankfully, there are now dedicated websites that monitor and list all known lottery scams such as those at Fraud Aid[1].

Fake gambling site scams

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 webpage forgeries, with credible and trustworthy sounding materials/products (Griffiths, 2003b; Australian Competition and Consumer Commission, 2009). One of the most common fraudulent practices is when unscrupulous individuals steal materials from legitimate online gambling sites (Griffiths, 2004; McMullan & Rege, 2007). Whole website designs can be stolen including the graphics and general design. Others may just use accreditation logos from legitimate accreditation organizations such as 'GamCare' or the 'Internet Gambling Commission' (Beginners-Gambling.com, 2009). Such people rely on the fact that many gamblers have made the decision to gamble even before logging on. The urge and desire to gamble can help overcome a person's ability to think rationally and/or their instinctive mistrust of the internet (Griffiths & Parke, 2002). Fake sites have to look safe, reputable and trustworthy. To avoid spending money on website design and development, the fraudsters simply steal existing designs (Griffiths, 2003b). Some fake sites even go as far as making

identical copies of winners' pages and testimonial pages of legitimate sites. This reinforces the idea that the site has hundreds of happy and satisfied customers. Only those who are intimately familiar with the 'host' or original site would notice such a fraud.

Betting software scams

Another popular online gambling scam involves software packages that claim to identify opportunities to consistently win money by gambling (Consumer Action Law Centre, 2008; Gordon, 2009). Internet sports or casino gambling services often require that an individual purchases software. These often involve large up-front fees and ongoing fees and charges (Australian Competition and Consumer Commission (ACCC) 2009). This supposedly enables an individual to predict the outcome of horse races or lotteries.

However, it is not possible to predict the outcome of random events such as horse races with any certainty. Betting software is often marketed by showing what an individual would have made had they invested money in the previous year (Gordon, 2009). Here, it is easy for the fraudster to demonstrate that a lot of money could have been made when they know which horse won every race. A variety of overseas lottery tickets are also marketed and sold by direct mail in many countries (ACCC, 2009). Very few are legal and fraud is often involved.

Gambling 'bonus' scams

Many online gambling sites offer incentives to get the gambler to play on their site. These include legitimate schemes such as VIP membership, loyalty schemes, and various types of deposit bonuses - i.e., the gamblers get a cash bonus if they register with the site (Griffiths & Wood, 2008). One of the legal (but highly exploitative) ploys to get people to gamble, are those sites that require excessive play (or to have gambled a pre-set amount of money), before the cash bonus is awarded. However, there are some 'bonus' practices that go beyond exploitation and are clearly fraudulent. One of the simplest - and most effective - of the bonus scams is targeted at players that have been banned from a casino (Take1Look.net, 2009). Since online casinos are always in need of known paying customers, this works by drawing in banned gamblers who have moved on to other sites. The gamblers receive an e-mail offering them a cash bonus if they deposit money into their existing account. However, after the gambler has deposited the money, they do not get their bonus. The online casinos tell the player they are not eligible to receive a bonus because they were banned. Gamblers then tend to play their deposit anyway - which is exactly what the operators were hoping for. Furthermore, some online casinos cite 'bonus abuse' as the reason for not paying winnings, knowing there is no governing body that can act against them (Griffiths, 2004).

Frauds rely on gullibility of the victim and the credibility of the criminal engaging in the fraudulent activity

The 'twofer' scam

Another unscrupulous tactic is where online gambling sites that have conned a gambler once, do it again - a 'two-for-one' scam (Take1Look.net, 2009). If a gambler has signed up to a particular online casino that takes all their money and then disappears, there is little a gambler can do. Quite often, months after, a gambler may start to get e-mails from a new gambling site set up by the fraudsters who conned the gambler in the first place (although the gambler is unlikely to know it is the same organisation). They know where to reach the gambler because of the registration form that the gambler initially filled out to join the now disbanded online casino. The fraudsters will e-mail compelling offers, rewards packages, and CD software - basically, anything to get the gambler back. The fraudsters then do exactly the same again. Another variation of the 'twofer' scam is when gambling operators invite their former scammed customers (by using the information the gambler provided before at a previous site), under the ruse of 'bonuses', telling the gamblers how sympathetic they are about them being scammed, and offering a bonus if they play on their website instead (Take1Look.net, 2009).

Concluding comments

This article highlights that technology is being used to exploit and defraud thousands of people. There appears to be one major reason why gambling is such a growth area for fraud. This is the fact that many gamblers themselves want to get a huge reward from a small outlay (just as the fraudsters do). As long as there are people who are prepared to risk money on chance events, there will be those out there who will want to fraudulently take their money from them. To date, there is almost no empirical data on any of these criminal practices and it is hard to assess the extent to how widespread any of these fraudulent online gambling practices are. There is clearly a need to examine this area empirically and for research to be initiated in this newly emerging area of criminological concern.

Dr Mark Griffiths Professor
NottinghamTrent University
mark.griffiths@ntu.ac.uk

1. See, for example, www.fraudaid.com/scamspam/lottery/lottery_scam_names.htm