FRAUD FACTS

Fraud Advisory Panel

Issue 4 October 2009

INFORMATION FOR INDIVIDUALS

Cybercrime – social networks and virtual worlds

The increasing popularity of cyber-communities such as social networks and virtual worlds has been accompanied by a growth in new forms of cybercrime. This factsheet highlights some of the common types of fraud committed in cyber-communities and gives tips for individuals on how to avoid falling victim to them.

What is cybercrime?

The term 'cybercrime' is often used to describe frauds that are attempted or committed using a computer and/or the internet. It covers a range of activities, including computer hacking, virus attacks ('botnets', 'malware' and 'adware'), fake websites, cyber-stalking, email scams, and cyber-extortion, to name a few. In most cases these activities are designed to steal a victim's personal, bank account or credit card details for use in fraudulent activities, or to use their computer in an attack on someone else.

Cyber-communities

Social networks

There are a diverse range of social networking platforms available which allow people to connect online and share messages, pictures, and videos, as well as chat and play games.

In the UK the most popular social networks are Facebook, MySpace, and Bebo. Other specialised networks include the school reunion site Friends Reunited, much publicised micro-blogging site Twitter, and business networking site LinkedIn.

Virtual worlds

Virtual worlds are computer-simulated landscapes in which users can interact and manipulate the environment around them. The most popular virtual world is Second Life, with other examples including the Sims games, and Sony's Playstation 3 virtual world Home.

Some virtual worlds are Massively Multiplayer Online Role-Playing Games (MMORPGs). The most popular is World of Warcraft, but there are numerous other multiplayer games available.

Virtual worlds differ from social networks in that they enable users to create their own virtual appearance (known as an avatar), which can be completely different from their 'real world' identity – including gender and species. Although each virtual world varies, most offer the user the opportunity to enhance their environment or character. Sometimes these enhancements can be earned by completing tasks, or they can be bought for a small cost.

Common types of fraud

Virus and spyware infection: You share links and files with other users which are exploited by cybercriminals to spread viruses and spyware. Keylogging trojan viruses are currently popular with fraudsters in virtual worlds. These capture the login details for your accounts, which are then sold for profit.

The 'Koobface' virus is just one example of how social network users can be vulnerable to viruses. Victims were sent messages such as 'Hey, I have this hilarious video of you dancing. You should check it out', containing a link to a website where users were told to download a flash player to view the video. The downloaded file contained a virus which turned the victim's computer into a zombie which was used to spread the virus.

Identity fraud: A fraudster collects your personal identity details that are available online and uses them, often with other information obtained elsewhere, to fraudulently purchase goods and services or to access facilities in your name.

People often give away more information than they intend on social networks, such as their name and address, date of birth, and telephone numbers.

You should be cautious of the information you share as part of your status updates. Status updates such as 'Laura is queuing at Terminal 5', or 'Adrian is celebrating his 30th birthday' might seem harmless, but when used with other information can be a useful resource to a fraudster, either now or in the future.

Social engineering to aid identity fraud: A fraudster uses 'live chat' facilities on social networking websites to try to persuade you to disclose personal

information. He/she may use a false identity to make it easier to get to know you.

For example, a seemingly innocent conversation about horoscopes could be used to extract your date of birth, or a conversation about previous schools could be used to identify your place of birth – valuable information for identity thieves.

Impersonation: A fraudster impersonates you on a social networking website and asks your friends for money to help 'you' out of a difficult situation.

Money laundering: A fraudster converts the proceeds of illegal activities into online currency, which is then used to purchase goods and/or services from you before being exchanged into real world currency.

Pyramid schemes (sometimes called 'chain-gift' schemes): For a small fee you are invited to join an online 'virtual' scheme which offers you commission based on the recruitment of new members or gamers.

How to protect yourself

DO:

- ✔ Ensure that you have a personal firewall and adequate virus protection installed on your computer, and make sure you update it when prompted.
- ✔ Make sure you are using the most recent version of your internet browser; browser updates often include security patches which will help keep you safe online.
- ✔ Be suspicious of anyone asking you for money online, even if they claim to be your friend!
- ✔ When setting up online accounts, make sure you choose strong passwords and change them regularly. A strong password should contain a combination of letters, numbers, and other characters, and be something that is difficult to guess. Fraudsters will often try to access your email accounts and other accounts using the same credentials – don't make it easy for them!
- ✔ Restrict your profile, so that only people you accept as friends can view your details.
- ✔ Consider how much information you post on your profile; there is a careful balance between giving people enough information to recognise you, and posting details that a fraudster can utilise.
- ✔ If you post status updates or Twitter messages, double-check that the information you share is not inadvertently giving more information than you intend.

DO NOT:

- ✗ Accept 'friend' requests or reply to messages from people you don't know.
- ✗ Accept large amounts of money or join get-rich-quick schemes in any virtual world; if something seems too good to be true, it probably is!
- ✗ Be tempted to share your card details with others 'in world'. Some games require payment; make sure you give out credit or debit card details only to the official virtual-world owner.

Advice for businesses

Think about whether you wish to allow staff to access virtual worlds or social networking websites during work hours. These websites can affect employee productivity, and create risks – both legally and to your brand or company's reputation.

Used properly, social networks can help promote your business and develop relationships with contacts. If you decide to allow access to social networks and virtual worlds, you may want to consider training staff to make them aware of both the benefits and dangers.

Further information

Card Watch
www.cardwatch.org.uk

Consumer Direct
www.consumerdirect.gov.uk

Fraud Advisory Panel
www.fraudadvisorypanel.org

Get Safe Online
www.getsafeonline.org

Identity Theft
www.identitytheft.org.uk

The Fraud Advisory Panel gratefully acknowledges the contribution of Laura Brown (www.192business.com) in the preparation of this Fraud Fact Sheet.

Fraud Advisory Panel, Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Registered Charity No. 1108863

Distributed by