

# Online Fraud

## Computer Security Day 2006

Monday 27 November 2006

Presenter: Tony Patrick  
Forensic Computer Analyst  
Computer Crime Unit  
Queensland Police Service

# Functions of the Computer Crime Unit

- Investigate fraud related offences committed on eRetailers, eCommerce or on Internet users in general.
- Investigate Computer hacking
- Investigate Denial of Service Attacks
- Investigate Internet Stalking offences
- Investigate internet scams
- Online operations targeting organised crime syndicates.

# Security threats

- Loss of laptops
- Loss of flash drives
- Loss of printed reports
- Internet surfing policies in the workplace.
- Poor password security
- Leaving computers unsecured
- Letting another person use your password
- Shortcutting policy and installing software.
- Corrupted employees
- Using home computers to do company work.

# What are computer criminals after?

- Corporate data
- Personal data of employees
- Personal data of customers
- Usage of company computer facilities
- Corporate extortion
- Banking information
- Espionage
- Deface web site
- Destroy corporate data

# Most popular sites criminals use to infect computers:

- Adult sites
- Dating services
- Joke sites
- Download free software
- Bulletin Boards
- Download music/ movies
- “Fringe sites”
- Chat Rooms
- Screensavers/ Wallpaper

# Case Study

- June 2005: PWSteal.Bancos virus was identified.
- Website [www.vladivostock.com](http://www.vladivostock.com) has list of approximately 800 Australian user names and passwords.
- Passwords covered bank account, security investments and numerous sites that contained personal details of victims.

- One victim was a major IT company whose system administrator password was found.
- In most instances, the victim had used a computer that had weak security.
- The virus had been delivered hidden in an e-greeting card.
- When victims were spoken to, none knew their details had been stolen.
- Many had no idea of online security.

# How much computer crime is going on????

- In 2006, 62% of business identified they had been a victim of computer crime.
  - 58% of respondent companies had laptops stolen.
  - 64% had been infected by computer viruses.
  - 14% had confidential data stolen.
- 
- Source: Australian Computer Crime and Security Survey 2006.



- 38% of computer attacks were by people that had no specific motive.
- 26% of attacks were to use the companies computer resources.
- 55% of attacks were to cause malicious damage.
- 20% were to obtain illicit financial gain.

- Source: Australian Computer Crime and Security Survey 2006.

# Current trends in computer crime

- Identity theft of businesses as well as individuals.
- Cyber extortion.
- More sophisticated viruses, spyware etc.
- Denial of service attacks becoming more sophisticated.
- Phishing attacks targeting bank account user names and passwords. (157477 attacks in 2005). *“Symantec Internet Security Report 2005”.*

# Computer Security

- 80% of computers on the net have spyware installed.
- In the past year, 86% of personal computers have been targeted for viruses etc.
- Thirty of the top 50 malicious code attacks identified in 2005 targeted personal data.
- Spam makes up 54% of all email traffic.
- *Symantec Internet Security Report 2005*

# Hackers attitude to the public

- “Most of the people I infect (with viruses) are so stupid they really ain’t got no business being on the internet in the first place”. *“Invasion of the computer snatchers”*. [Online], Available: <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14AR20060214013>, [Accessed 28 September 2006].
- This person controls 13,000 personal computers in 20 countries.
- Examples of information he collects includes passwords to PayPal, eBay, Bank of America, Citibank etc.

# Cyber Extortion

- “Cyber extortion is becoming a favourite crime because it is isn’t violent, promises lucrative payouts, and normally guarantees anonymity.”

“The Fraud Magazine” Association of Certified Fraud Examiners “Extortion by computer and internet”. Pg 21

March/ April 2006.

- Companies vulnerable include:
  - : Those holding large volumes of sensitive data.
  - : Those planning an IPO.
  - : Gambling sites before a major event.
  - : Online businesses.

# Phishing

- Phishing involves sending out spam that purports to be from a particular company, informing people that they need to click on the link included in their message and enter their account details”. Pearce J.2004 “Crime gangs go phishing”. [Online], Available <http://www.zdnet.com.au/news/communications>, [Accessed 01/03/2005].

# Example targeting Westpac clients.

- Dear Valued Customer,  
Financial institutions around the world have always been subject to attempts by criminals to try and defraud money from them and their customers. These attempts can occur in a number of ways (eg credit card fraud, telephone banking or Internet scams).

As a part of our ongoing commitment to provide the "Best Possible" service and Protection to all our Members, we are now requiring each member to validate their accounts once per month. To validate your personal Westpac online banking account follow the link. [Sign in to Secured Online Banking](#) .

(Remember Failure to verify your account details may lead to account Suspension for security Reasons)

Thank you.

Online Banking Security Team

Westpac Online .

© Westpac Bank Limited ABN 92 055 513 070 AFS Licence No. 240997



## Westpac Australia's First Bank



### Main menu

#### Online Banking

- ▶ Online Broking
- ▶ Apply Online
- ▶ Shop Online

- Home Loans
- Personal Loans
- Credit Cards
- Transaction & Savings Accounts

- Investment & Superannuation
- Insurance

- International Services

- ▶ Today's Rates
- ▶ Calculators
- ▶ Privacy Policy

home

### Internet Banking Sign In

#### Customer Sign In

Customer No.

Password

sign in

#### Terms & conditions have changed

If you have forgotten your password, please call our Internet Help Line on 1300 655 505.

**Internet Banking customers**  
Find out how to [protect yourself](#) from Internet fraud attempts, including emails which appear to be from Westpac.

#### Are you new to Internet Banking?

- Find out the [benefits](#) and how to [register](#).
- Read about our Internet Banking [security guarantee](#).
- In need [help](#) is always available.

#### Internet Banking services

- View our [User's Guide](#) explaining the services available.

#### Active demonstrations

- Our [active demonstrations](#) can help you learn how to use Internet Banking.

#### Security

- Discover guidelines on how to ensure your [Internet Banking Security](#).
- Other general tools and tips to bank safely can be found in our [Security and Technical Guide](#)

#### Business customers

Do you own or operate a business? Sign in to [Online Banking here](#).

#### Investment customers

Share trading made simple. Sign in to Westpac Broking.

Managed investment transactions. Sign in to BTOOnline.

#### Terms & conditions

[View or download](#) the current, full terms & conditions.

[View the changes to](#) Internet Banking terms & conditions, applicable from 8 February 2004.

#### ▶ Ask Westpac

General advice on this website has been prepared without taking into account your objectives, financial situation or needs. Before acting on the advice, consider its appropriateness. Consider our [disclosure documents](#) which include the Product Disclosure Statements for products. These disclosure documents (including PDS) are relevant when deciding whether to acquire or hold a product.

By accessing and viewing this website you agree to be bound by the [Terms and Conditions](#) of this website.

Copyright © 2004 - Westpac Banking Corporation ABN 33 007 457 141 also trading as Challenge Bank and Bank of Melbourne.



# What happens once the offender has the user name and password of an internet bank user?

- The offender has full access and privileges to the bank account of the victim including access to overdrafts etc.
- “Microsoft's general manager of technology care and safety, Ryan Hamlin, said that phishing was stealing more than \$13.3 billion a year in the United States.”
- Phishing the net and trawelling for fraud. [Online], Available [www.theaustralian.com.au](http://www.theaustralian.com.au) [Accessed 28/08/2005].

# Trojan Viruses can also be used to obtain your banking details

- “Trojan Viruses are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage.”
- DNK Technology, Computer Security---Viruses, worms and Trojan Horses. [Online], Available: <http://www.dnktechnology.com/framemaincinfo.htm>, [Accessed 22 February 2005].

- A common Trojan virus is a keylogger that monitors the keystrokes on a computer.
- The virus recognises key words such as “bank”, “online”, “password” or the name of selected financial institutes.

# Jackson suicide spam hides virus



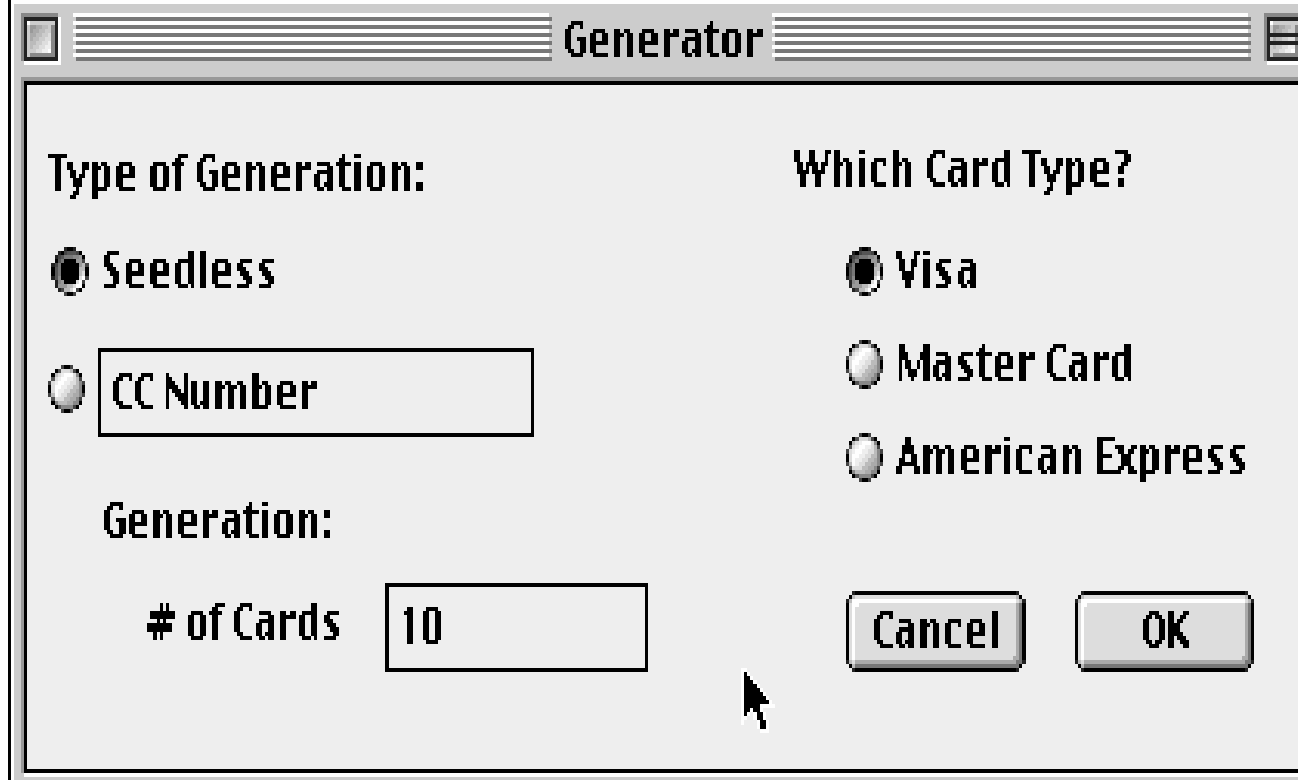
- **A Windows e-mail virus is trying to ensnare victims by claiming that Michael Jackson has attempted suicide, say computer security firms.**
  - **The message hopes to catch people's attention because of the huge interest in the on-going child abuse trial.**
  - **The fake message contains a web link that supposedly links to Mr Jackson's suicide note.**
  - **But anyone clicking on the link will have their PC invaded by a virus that gives others access to that machine.**
- 
- **BBC News International Friday, 10 June, 2005, 12:34 GMT 13:34 UK**

# Credit Card Generators

Generating real credit card numbers (yours?)

Generating previously unused credit card numbers

Generating false credit card numbers



The "Generator" dialog box is a standard Windows-style window with a title bar. It contains two main sections. The "Type of Generation:" section on the left has two radio buttons: "Seedless" (selected) and "CC Number" (unselected). The "CC Number" option is followed by an empty text input field. The "Which Card Type?" section on the right has three radio buttons: "Visa" (selected), "Master Card" (unselected), and "American Express" (unselected). At the bottom left, the "Generation:" section includes a label "# of Cards" followed by a text input field containing the number "10". At the bottom right are "Cancel" and "OK" buttons. A mouse cursor is visible near the bottom center of the dialog.

**Generator**

Type of Generation:

☒ Seedless

☐ CC Number

Generation:

# of Cards 10

Which Card Type?

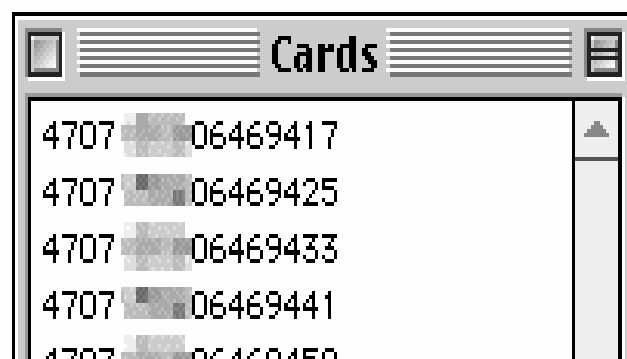
☒ Visa

☐ Master Card

☐ American Express

Cancel OK

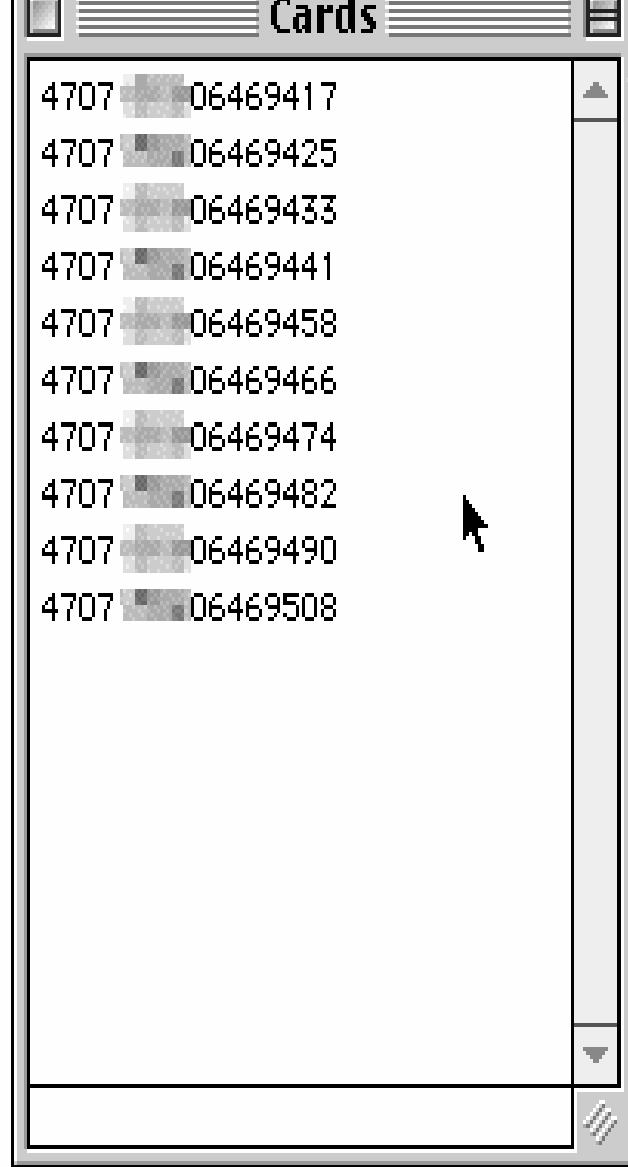
**This dialog box is accessed via a menu command called "Make New Cards."**  
**By default it will generate 10 Visa card numbers...**



The "Cards" window is a small application window with a title bar. It contains a list box with five entries, each showing a card number. The first four entries are visible, and the fifth is partially cut off at the bottom. Each entry consists of a four-digit prefix, a masked area (represented by a grey square), and a seven-digit suffix.

**Cards**

|      |          |
|------|----------|
| 4707 | 06469417 |
| 4707 | 06469425 |
| 4707 | 06469433 |
| 4707 | 06469441 |
| 4707 | 06469450 |



... And here are the resulting well-formed Visa card numbers.  
(I've obscured some of the digits for obvious reasons.)

# On line scams:

- Nigerian Fraud
- Lottery
- Online romance
- Phishing
- Auction
- Seeking donations for charity



# Offender methodology

Victims are located through:

- Mass email campaign from harvested addresses.
- MSN chat, particularly in lonely hearts scams – dating websites
- Chat Rooms
- Usage of a “suckers list”

# Why do people respond to scam emails???

- Gullible
- Greed
- “Take a punt”
- Financially desperate
- Conned
- Wish to help disadvantaged
- Lonely

# Key Facts learnt:

- People will send all their money to people they do not know, with identities they cannot confirm, to countries they cannot locate on a map.
- Victims will often not listen to warnings from police.
- The more money they have sent, the less likelihood they will accept they have been scammed.

# Key facts learnt (cont)

- Many people will believe anything and everything they read on the internet.
- Advance fee proposals are viewed like a lotto winning, the answer to solving all their financial problems.
- Victims want to believe the proposals are true and will make no inquiries to independently verify the claims made.

# Questions???