



Pacific Islands Telecommunications Association

8th Fl, Dominion Hse
PO BOX 2027, Govt Bldg
SUVA, FIJI Islands

PHONE : (679) 331 1638
FAX : (679) 330 8750
E-mail: pita@connect.com.fj

www.pita.org.fj

INVITATION TO PARTICIPATE IN RAISING AWARENESS OF CYBERCRIME AND CYBER SECURITY

The Pacific Islands Telecommunications Association is organising a Cyber crime Cyber security seminar on the 24th November 2009, at the Main Convention Centre, Tanoa International Hotel, Nadi.

The main objective of this seminar can be summarised as follows:

- a) to raise awareness of cybercrime and cyber security risks at the Service Provisions and Policy Making levels of the communications industry, for necessary actions, and
- b) to provide networking opportunities and cooperation with stakeholders and peers in efforts against cybercrimes and online security.

With the lessons from the boom of cybercrimes and issues of cyber security globally, there is a critical opportunity for developing and 3rd world countries including the Pacific to **“nip the issues in the bud”** with the internet not having fully reached its potentials yet, and where the internet has not reached every home and every citizen of their countries.

According to studies, the 3 big developments that will help cyber crime and raise the risks of cyber security are:

- increasing number of IT professionals skills
- the drive to bring to everyone Broadband Internet and ICT benefits
- new technologies including the web 2.0 and the Trojan technologies

Already new policies driving these developments are now prevalent in our developing countries, with drives to implement the following already ongoing:

- National ICT plans, by each country either already formulated or being developed, and assisted by regional organisations and experts, to promote ICT nationally
- the regional Digital Strategy by the regional government and agencies to provide everyone with equal access to ICT and its benefits,
- the initiatives of Telecentres¹, rural internet services and OLPC², providing rural and remote areas with internet, and
- the rise of tertiary and vocational institutions offering IT programs, and
- the competitiveness of the communication industry, and the commercial operators in pushing new online services and online shopping to the populations. (ADSL³ and Wireless Broadband, including 3G Mobile Broadband are now already on offering for urban and quickly moving to major rural areas in Fiji and French Polynesia.)

These developments and the policies that drive them will actually place our world on the chart of countries with significant effects from cybercrimes if the implications of cybercrime and online security risks are not inclusive. The internet is a global network and with it the cause and effect of cybercrime and cyber security issues are no longer isolated to developed countries.

¹ Telecentres are public places where people can access computers, the Internet, and other digital technologies.

² OLPC - One Laptop Per Child

³ ADSL – technology to allow copper carry high speed communication, examples; data, multimedia

But unlike the developed countries, are we appropriately equipped to deal with it?

According to forecasters Cybercrime trends will worsen, with more and more computers connected into the net compromised and becoming vehicles of fraudulent and criminal network of operators.

What is Cyber Crime?

According to the Wikipedia definition, Cyber crime can broadly be defined as criminal activity involving an information and communication technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

Cyber crime encompass a broad range of potentially illegal activities, some examples include crimes that target computer networks or devices directly; and other crimes are facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

"It is an already common knowledge that the use of technology, and particularly with the internet has taken over our every day interactions. Now we can sit in the comfort of our houses and carry out various activities such as banking, shopping and long distance communications almost instantly."⁴

Two countries in the Pacific have already been hit at national levels with DDOS attacks, crippling the national internet email grid and resulting in no emails going in or out of that country for a few days.

Recently phishing attacks targeting online banking website of a credible regional bank resulted with very anxious customers, and the bank issuing warning to its customers of the scare.

According to Security Threat reports, the United States has bypassed China as the biggest purveyor of malware as well as sends the most spam worldwide

"Not only is the USA relaying the most spam because too many of its computers have been compromised and are under the control of hackers, but it's also carrying the most malicious web pages," said a report from Sophos Security Threat. "We would like to see the States making less of an impact on the charts in the coming year. American computers, whether knowingly or not, are making a disturbingly large contribution to the problems of viruses and spam affecting all of us today."

What can we say for our own countries?

Cybercrime and security seminar

This seminar in its efforts to raise awareness for actions will:

1. Discuss overview of cyber crime and cyber security and how these work, and how they have become significant, with organised networks of cyber criminals being formed around the world and a strong underground economy.
2. Discuss the various cybercrime activities and risks of security and safety online, and what they do to impact on individuals and country, and furthermore,
3. Discuss the efforts and initiatives made to address growing cybercrimes and security issues, with some case studies.

Time for Questions and Answers and meeting with key speakers and peers will be provided during breaks and social reception.

⁴ Quotes from Diplo-Foundation

Key Speakers will be from the:

1. AusCERT

AusCERT is the national Computer Emergency Response Team (CERT) for Australia and a leading CERT in the Asia/Pacific region. As the national CERT, we are the primary Australian contact for dealing with Internet security threats and vulnerabilities affecting Australian interests. We operate within a worldwide network of information security experts and provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia.

2. TEAM CYMRU

Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. By researching the 'who' and 'why' of malicious Internet activity worldwide, Team Cymru helps organizations identify and eradicate problems in their networks

3. **ITU:** The International Telecommunications Union on regional initiative for Pacific CERT
4. **Fiji Director of Public Prosecutions:** on country initiatives and directions Fiji is taking with the cybercrimes provisions and the roles in enforcements
5. **ANZ Bank:** online threats and concerns
6. **CISCO expert**

See Tentative Program enclosed

Register now!!

And join the efforts and be part of the solutions against cybercrime and cyber-security risks.

To register: go online at this link below:

<http://www.pita.org.fj/index.cfm?action=eventregistration&id=B11FCE86-1A64-2584-D8E0B4771322A33D>

Registrations is free

This seminar is supported and made possible by the following organisations:



(more supporting organisations are being invited)

Cybercrimes and security Stakeholder seminar

Main Convention Centre, Tanoa International Hotel, Nadi, FIJI
24 November 2009 @1400-1730pm

Tentative Agenda (draft copy)

1. **Welcome by host**
 2. **Guest Speaker and opening remarks**
 3. **Cybercrime and Organised crime**
 - i) **Online crime and the Underground Economy in 2009**
 - The marketplace for stolen data is as lively as ever. Miscreants make a handsome living by stealing and trading personal data. They are not stopped by boundaries or laws of any kind. This presentation will give insight into the way criminals operate online and exchange valuable data**Marcel van den Berg, TEAM CYMRU**
 - ii) **Cybercrime and implications on businesses**

During this presentation focusing on keyloggers and phishing, AusCERT will show the massive scale of the phishing and malware problem from their perspective. And even then, this perspective is still probably only the tip of the iceberg. This includes the advances in the complexity of phishing and malware attacks. I'll also look in detail at some of compromised data and what this might mean for network operators, governments and anyone who is looking to conduct their business on line.

Robert Lowe, AusCERT
- Tea Break (1530-1550)
4. **The Internet**
 - i) **The internet impact**
Dr Philip Smith, CISCO Systems
 - ii) **Online banking threats and concerns**
Veilawa Rereiwasaliwa, ANZ
 - ii) **A view into badness, pictures say more than a thousand words.**
 - This presentation will show a visual representation of various types of 'bad' activity we have seen on the Internet**Marcel van den Berg, TEAM CYMRU**
 5. **Initiatives and efforts to address cybercrimes and cyber security**
 - i) **Provisioning for cybercrime and enforcements**

case study of the new cybercrime provisions and role of e-crimes enforcements in Fiji

John Rabuku, Director of Public Prosecutions, Fiji
 - iii) **Empowering countries and multi-stakeholders to deal with cybercrimes and security**

The Global Cyber-security Agenda (GCA) & Pacific CERT

International Telecommunications Union (ITU)
 6. **Questions and Answers** (1730)
 7. **Social reception** (1800)

About the Speakers

Marcel van den Berg

Marcel is an analyst at Team Cymru and a former police officer at the Dutch National High Tech Crime Centre currently living in New Zealand.

Robert Lowe.

Robert is an Information Security Analyst for AusCERT and has been involved in a variety of AusCERT's work, from incident coordination and assistance to systems administration and programming. Recently, his focus is international outreach and the AusCERT conference. He has been with AusCERT since 2003 and during this time, witnessed the explosive growth in online organised criminal activity.

Prior to joining AusCERT, Robert was a Senior Client Services Engineer for an Internet gambling software provider.

Robert graduated from the University of Technology, Sydney in 1999 with a Bachelor of Science (Computing) and holds the CISSP and CISA security certifications.

Dr Philip Smith

Philip has been with Cisco Systems since 1998. He is part of the Internet Infrastructure Group in Corporate Consulting Engineering. His role includes working with the ISPs and Service Provider operations groups around the world, specifically in network design, configuration, scaling and training.

Prior to joining Cisco, he spent five years at PIPEX (now part of UUNET's global ISP business), the UK's first commercial Internet Service Provider. He was one of the first engineers working in the commercial Internet in the UK, and played a key role in building the modern Internet in Europe.

John Rabuku

John is currently the Acting Director with the Office of Public Prosecutions, an independent body responsible with the criminal prosecution work in Fiji.

Veilawa Rereiwaliwa

Veilawa is the head of the IT departments in ANZ, a regional bank having presences in 8 countries of the Pacific Islands.

International Telecommunications Union (ITU)

Is a [United Nations](#) agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services