

# IBM Computer Emergency Response Team A/NZ



CONFIDENTIALITY  
INTEGRITY  
AVAILABILITY



# Ichthyological anatomy or a study of phish

**Introduction**

**History**

**Techniques**

**Investigations**

**Problems**

**Future vectors**

**Prevention**

No Entry


# History

- AOL
- Global Banks
- International Banks
- Building Societies/S&L



# Techniques

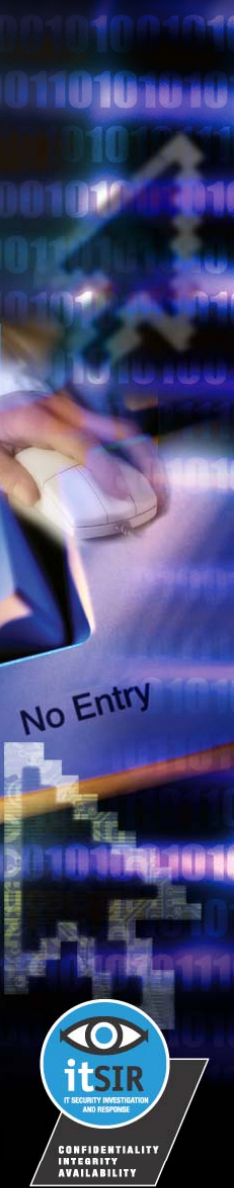
- Email
- Websites
- HTML email
- DNS poisoning (pharming)
- Trojans/keyloggers
- Telephone
- IVR
- Evil twins



No Entry

# Investigations

- Static analysis
- Simulation/sandbox



# Problems

- Short-term events
- Differential jurisdiction
- Security-aware code



# Future vectors


- Instant Messaging
- E-cards





# Prevention

- Dual factor authentication
- Out-of-band communication
- Mule-hunting
- Public education



No Entry





# Questions and comments

