IBM Computer Emergency Response Team A/NZ
Ichthyological anatomy
or
a study of phish

Introduction
History
Techniques
Investigations
Problems
Future vectors
Prevention
History

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

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