The don’ts and don’ts of electronic crime
Scams

• Don’t pay someone who you are trying to sell to
• Don’t buy commodores from Belfast
• Don’t believe that people in West African know how respectable you are
• Don’t use wire transfer to send money to a person you don’t know
• Don’t try claiming a prize for a lottery you didn’t enter
• Don’t return single ring phone calls
Things I will not do

- Believe callers who know there is something wrong with your computer
- Pay for prizes you have won
- Accept that the Tax office emails unsolicited tax return advice
Don’t get hooked by a phish

- Don’t give out your personal information unless you initiated the contact.
- Don’t click on links in emails.
‘Boiler-room’ scams

- Victims approached by overseas callers
- Caller knows the victim’s name and details of their prior shareholdings.
- Opportunity to purchase discounted shares in major overseas companies
- Scammers seeking to purchase worthless shares the victims own and offer blue chip shares at a reduced cost
‘Boiler-room’ scams

- Does that corporation have an Australian Financial Services License with ASIC
- Check via the names index at www.asic.gov.au
Why Scammers use the Internet

• Anonymity – They don’t have to physically deal with the victim in person

• Increased access / use of computers means more people online and more opportunity to scam others

• Jurisdictional protection – Can be difficult to identify them, catch them or prosecute them
Current state of play
Botnets for hire
Compromises in 2010

- 83% of victims were targets of opportunity (<>)
- 92% of attacks were not highly difficult (+7%)
- 76% of all data was compromised from servers (-22%)
- 86% were discovered by a third party (+25%)
- 96% of breaches were avoidable through simple or intermediate controls (<>)

2010 Verizon Data Breach Investigations Report
www.verizonbusiness.com
Malicious code

- **Virus**: Requires a user to do something to continue the propagation – harmful, may destroy data.
- **Worm**: Can propagate by itself - self-propagating malicious code, consumes resources destructively.
- **Trojan**: (Backdoors) - Executable codes installed that enable entry into the infected host without authorisation.
- Malware is sophisticated.
  - New version every 2.5 seconds.
- Malware is profit-driven.
  - Targeted, organised crime.
The response

Public
• Education
• Target hardening

Government
• Education
• Resourcing
• International cooperation
Keep Your Operating System and other software updated
Don’t wait until you’re a victim

• Don’t leave your computer switched on or unattended for prolonged periods - Log off when you are done for the day

• Be alert to unusual behaviour on your computer

• Protect your passwords

• Wireless users must ensure their machines are configured correctly

• Back up your data
Use a Strong Password

- Not birth date, anniversary, mother’s maiden name, name of pet, child or spouse.
- 8+ characters, including numbers or symbols.
- Change your password at least every 90 days.
- Poor passwords: 123456, 12345, 123456789, Password, iloveyou, princess, abc123
### Password strength

<table>
<thead>
<tr>
<th>Password Length</th>
<th>All Characters</th>
<th>Only Lowercase</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 characters</td>
<td>0.86 seconds</td>
<td>0.02 seconds</td>
</tr>
<tr>
<td>4 characters</td>
<td>1.36 minutes</td>
<td>.046 seconds</td>
</tr>
<tr>
<td>5 characters</td>
<td>2.15 hours</td>
<td>11.9 seconds</td>
</tr>
<tr>
<td>6 characters</td>
<td>8.51 days</td>
<td>5.15 minutes</td>
</tr>
<tr>
<td>7 characters</td>
<td>2.21 years</td>
<td>2.23 hours</td>
</tr>
<tr>
<td>8 characters</td>
<td>2.10 centuries</td>
<td>2.42 days</td>
</tr>
<tr>
<td>9 characters</td>
<td>20 millennia</td>
<td>2.07 months</td>
</tr>
<tr>
<td>10 characters</td>
<td>1,899 millennia</td>
<td>4.48 years</td>
</tr>
<tr>
<td>11 characters</td>
<td>180,365 millennia</td>
<td>1.16 centuries</td>
</tr>
<tr>
<td>12 characters</td>
<td>17,184,705 millennia</td>
<td>3.03 millennia</td>
</tr>
<tr>
<td>13 characters</td>
<td>1,627,797,068 millennia</td>
<td>78.7 millennia</td>
</tr>
<tr>
<td>14 characters</td>
<td>154,640,721,434 millennia</td>
<td>2,046 millennia</td>
</tr>
</tbody>
</table>
Managing your on-line identity

• When registering for access consider what personal information you want to provide

• Do not provide your personal information if at all possible – usually it is possible

• Be careful with unsolicited email there may be a Trojan imbedded
Basic tips

• Shred credit card receipts and old bank statements
• Close unused credit card or bank accounts
• Don't give out personal information via the phone, mail, or Internet unless you initiated the contact
• Never respond to an offer you don't understand
• Talk over investments with a trusted friend, family member, or financial advisor
• Require all plans and purchases to be in writing
• Don't pay in advance for services.
The digital divide

- Children understand technology but not necessarily the associated safety issues.
- Many parents, caregivers and teachers do not have the knowledge necessary to give guidance relating to the appropriate use of technology.
- Learn about technology – children are a great resource
How children lost the right to roam in four generations
If reporting to the Police

• Retain e-mails or messages electronically

• Provide verbatim account of what has been said

• Ensure correct spelling

• Provide as much relevant data as possible

• The initial police officer you speak with may not be as IT literate as yourself
Questions