



ONLINE SECURITY THREATS – ***CURRENT TRENDS AND CONTROL STRATEGIES***

SABRINA SERAFIN, MBA, MPA, CISA
GINA GONDRON, CIA, CISA
FRAZIER & DEETER, LLC

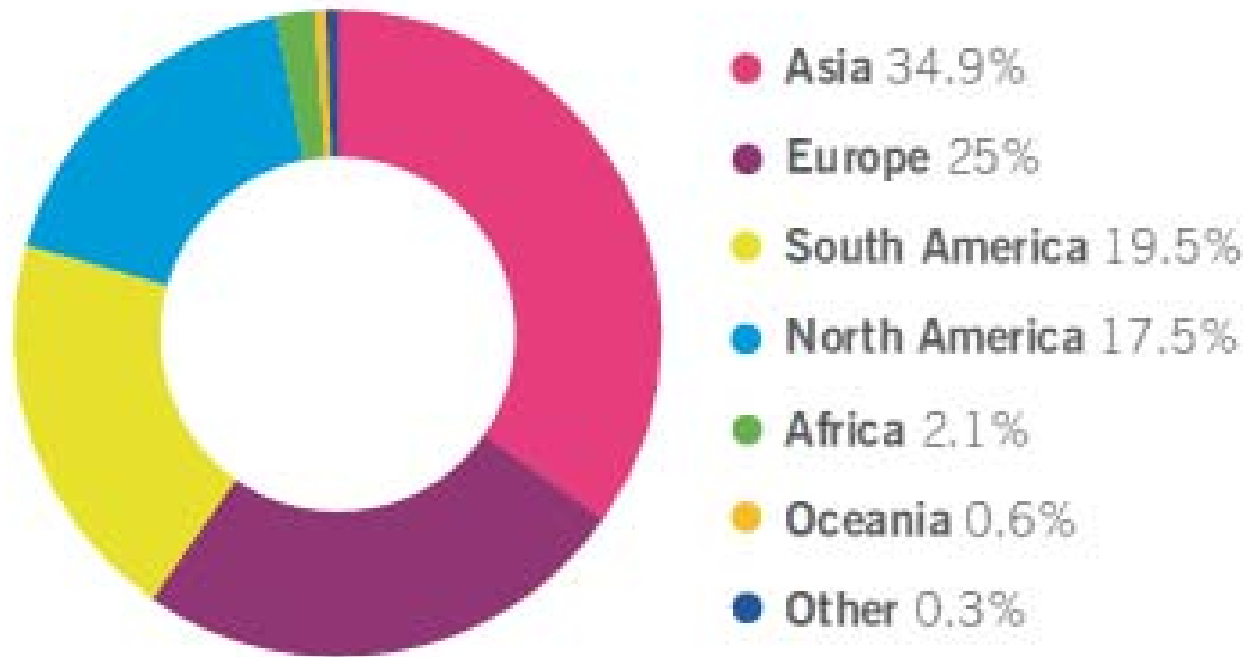
Geek Week 2010

Security Threats -Trends

- **Web Threats:** Biggest vehicle for malware
- **Spam:** Important vector for malware propagation
- **Malware Trends:** Money making machine
- **Windows 7 / Apple Macs:** New platforms, new challenges



Spam



Spam by continent

Source: Sophos Security Threat Report: 2010



Technical Safeguards

- **Reducing Web Risks**
 - Screen web usage by quality web protection technology
 - Carefully monitor access to proxies and control access to malicious or inappropriate sites
- **Spam**



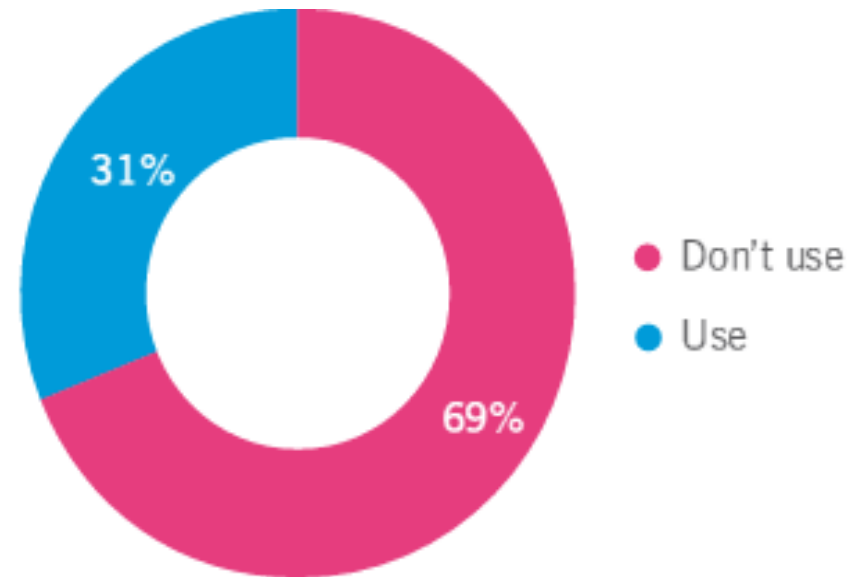
Technical Safeguards, cont.

- **Malware Trends**
 - Restrict user administrative rights
 - Anti-virus and anti-spyware
 - Personal firewalls
 - Web content filtering and blacklisting

- **Windows 7**
 - Reduce security vulnerabilities that led to malware and cybercrime explosion of the past decade
 - UAC System
 - more secure environment, but there is still room for improvement

Apple Macs

- Snow Leopard acknowledgement by Apple that malware does affect its platform
- Only prevents installation of a small election of known
- Need for patching software

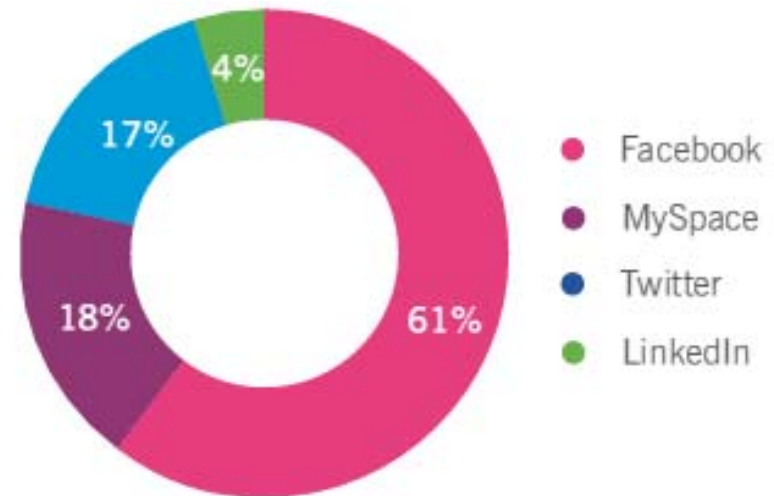


Do you use anti-virus to protect your Mac?

Source: Sophos Security Threat Report: 2010

Online Communities and Collaboration

- **Social Networking:**
 - Widely adopting techniques
 - Malware is biggest concern
- **Spam:**
 - Instant messaging
 - Social networking spam
- **Data loss and encryption:**
 - Data leaks



Which social network do you think poses the biggest risk to security?

Source: Sophos Security Threat Report: 2010



Technical Safeguards

- Protection against Social Networking
 - Granular access control
 - Secure encryption and data monitoring
 - Comprehensive malware protection.

- Spam via Social Networking and Instant Messaging

- Preventing Data loss
 - Encryption - laptops, removable storage devices
 - Extend anti-malware infrastructure :
 - Protect data in motion and data in use
 - Guarantee efficient operations
 - Meet regulatory requirements

Remote Users

- Email threats:
 - Malware spread through attachments and embedded links
- Mobile Devices:
 - Vulnerable to social engineering attacks





Technical Safeguards

- Email threats

- Mobile Devices
 - Technological security measures to protect PII
 - Only access PII, not store or download PII
 - Avoid untrustworthy environments
 - Mobile firewall software
 - IDS

Additional Considerations

- **Cybercrime Economy:** immense monetary profits from cybercrime
- **Cyberwar and Cyber terror:** growing fear of crucial infrastructures vulnerable to attacks





What does 2011 hold?

- Encouraging trends from 2011
- Social Networking Trends
- Government Involvement
- Software Development
- Cloud-based services
- Hacking/virus writing