Virus Presentation to Business Owners:

Bust the myth – not produced by bored teenagers; organized crime syndicates in Russia, making big money from their efforts

How the virus writers make money:

- Rogue security programs -- $39.95 - $79.95, max out card, sell it on Internet
- Ransomware – FBI MoneyPak, file encryption
- Identity theft, credit card fraud
- Harvesting and selling e-mail addresses from infected computers
- Stealing intellectual property of businesses, oil company example
- Joining botnets, selling access to those infected computers

How a computer gets infected: (80% are, but show no symptoms)

- E-mail attachment
- Link in e-mail
- Malicious code in e-mail (no link or attachment required)
- Link in social media message – mostly Facebook
- Illegal, high-risk web sites – "warez" sites, pirated DVDs, music, software
- Legitimate web sites infected – church/religious, NBC.com, Jay Leno
- Browser hijackers – search result lands on infected site
- Clones of legitimate sites, with common misspellings

22 ways an e-mail can infect your computer (see attached document by Kevin Mitnick, "Social Engineering Red Flags")

Other threats:

- Phone call from "Microsoft partner," claiming to have found viruses
- E-mail "Mugged in Wales" or similar
- Smartphone + Facebook = no privacy, watch this video from November, 2010: http://www.youtube.com/watch?v=N2vARzvWxwY

What you can do:

- Back up your data
- Run anti-virus software (no free ones, recommend VIPRE Internet Security)
- Keep Windows Updates current
- Ditto for Adobe Air, Flash, Reader, Shockwave, Java, etc.
- Use strong passwords on e-mail accounts
- Have computer checked periodically by trained professional