

The Cyber Jungle

Protecting Your Personal Information

Contact Information

- Jack Gerbs
- Quanexus, Inc.
- 9090 North State Route 48
- Dayton, OH 45458

- jgerbs@quanexus.com
- 937-885-7272



Disclaimer

- Implementing some or all of the suggestions presented today does not guarantee your information will be safe. There are no guarantees when it comes to protecting your systems and the information stored on your systems.

Goals for this Presentation

- **What do the bad guys want**
- **How are they being successful**
- **How can you protect yourself**

[illegible]

- Anthem Breach (Detection)
- Target
- Home Depot
- Sony
- Identity Theft (False Tax Returns)
- Insurance Fraud

What do the Bad Guys Want?

- Anything and Everything has a price, but the big stuff is:
 - Credit Card number& related info
 - 20 cents to \$1 for a single package that has if you have expiration date, if you have the victim's SSN, expiration date and mothers maiden name.
 - Full Medical Records
 - \$10 to \$500 for a full package
 - Medical Fraud
 - Identity Fraud
 - Reputation and or Finical Damage to the Victim (Hacktivists)

There are Two Basic Threats?

- Advanced Persistent Threat (APT)
 - Governments
 - Large Companies
- Drive-by Threat (can happen to company or anyone)
 - Unsuspecting Victim
 - Easy low hanging fruit

How are the Bad Guys Being Successful

- Unpatched software (not just the OS, third party apps such as Java, Adobe, office suites, Internet forward facing servers, etc.
- Trusted third party vendors
- Social Engineering
 - Phishing
 - Spear Phishing

1. Passwords

- Simple
- Complex
- Passphrases
- Complex Passphrase
- PW Length (minimum 13 characters – 20 is great)
- Managing / Remembering Passwords/Passphrases
 - Keepass
 - Spiral notebook for business



Complex Passphrase Examples

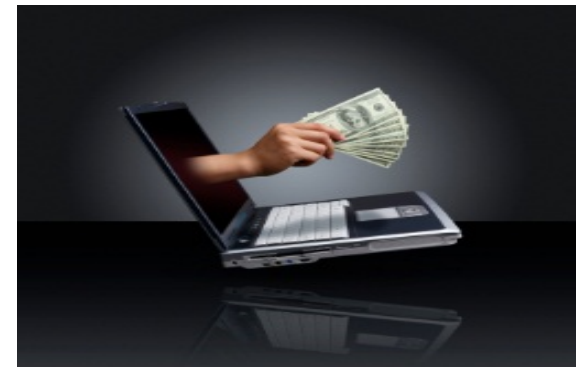
- Create a complex phrase based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the passphrase could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
(sans.org)
- Myd0gBruis3r3ats@11

Passwords Dos and Don'ts

- Do not your personal passwords at work!!!
- Don't share passwords
- Change passwords regularly
- Should be a minimum of 13 characters

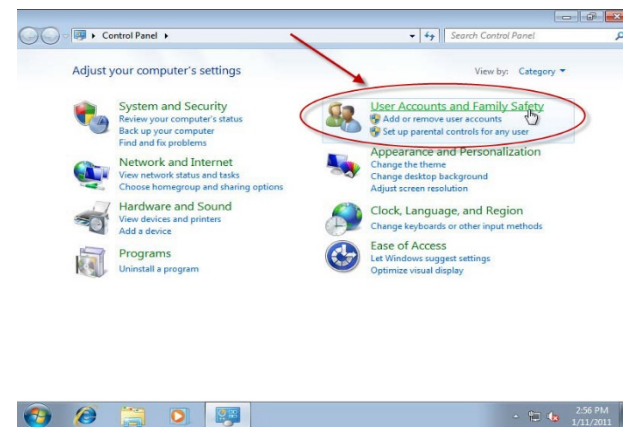
2. On-Line Banking & Other Services

- Re: Social Engineering Demo
- Don't have to use true information for security challenge questions
- Try to use something that you can remember that has a reference to the question
- Use alternative operating system, preferably a live CD



3. Windows User Accounts

- Windows XP, 7 and 8.x support multiple user accounts
 - System is protected leaving only the profile vulnerable
- Delete and recreate profile vs. having to rebuild system



4. Patch Management

- The number one reason for systems getting exploited is poorly written code
- Microsoft, Adobe, Java, etc.
- Printer and Network components are often overlooked
- Managed Solutions – for Small and Medium Sized Businesses



5. Antivirus & Malware Protection

- Goes hand in hand with your patch management solution
- Updates need to be regularly scheduled and verified that the updates were successfully installed
- Business Class vs. Consumer
 - Central Administration
 - Alerting & Logging



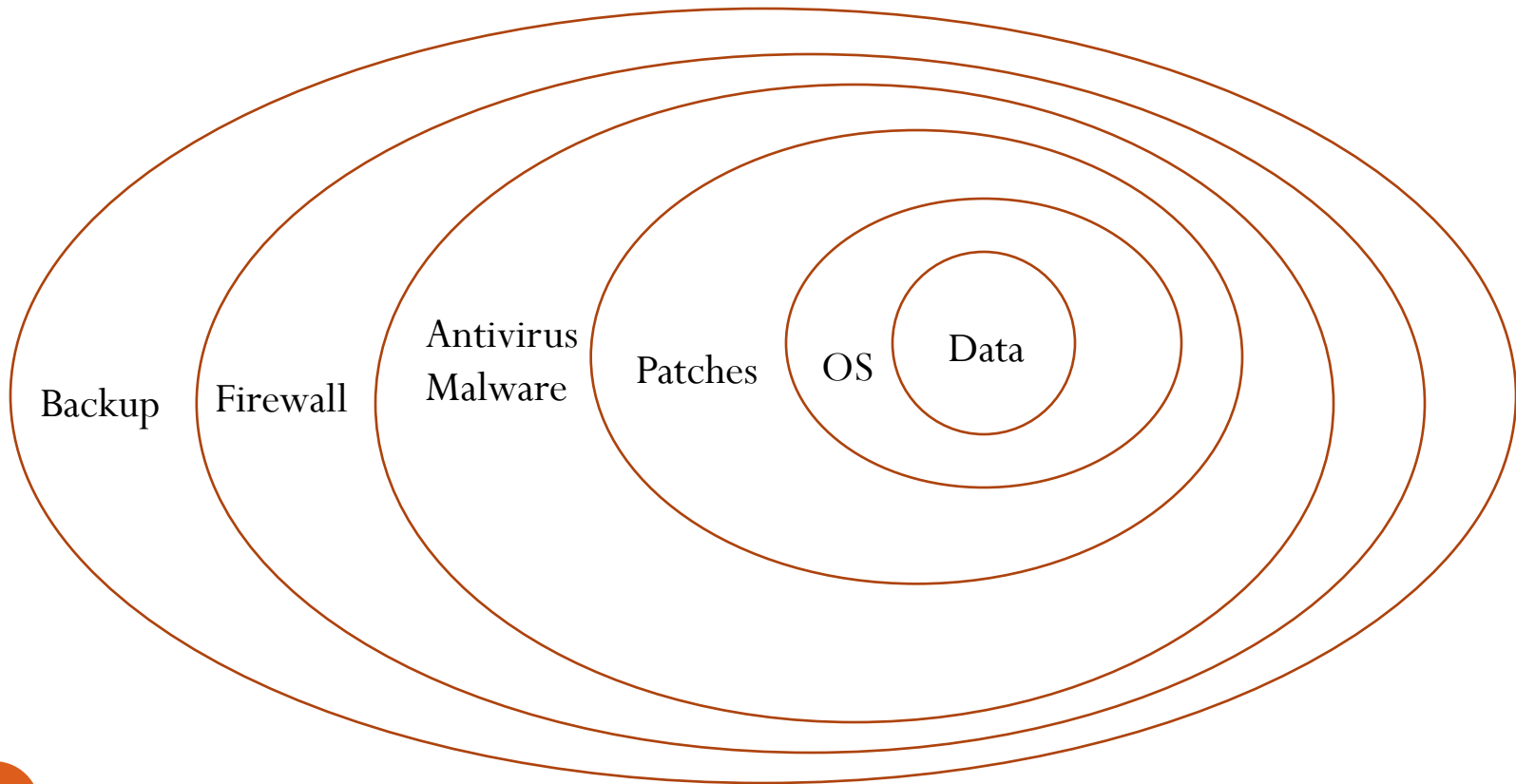
6. Firewall

- The firewall is a fundamental building block for IT Security
- Compared to all other security controls, a business class firewall properly implemented is 86% effective
- New Unified Threat Management technology is now included in many business class firewalls
- AV / IDS / IPS / Filtering / Logging / Altering



Security in Depth & Layered Security

- Protecting your systems, and the information on your systems requires a layered approach



7. Backup and Business Continuity / Disaster Recovery

- There are lots of inexpensive on-line solutions for home users and small businesses
- Considerations:
 - Are you only concerned about the files or the whole system?
 - Online typically backs up only files
 - Local can backup full system image
- Concerns about online backup solution:
 - How they are financed
 - How quick can you recover
- Business concerns - Backup is all about Business Continuance and Disaster Recovery, RTO and RPO
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO)





8. Wireless

- Change the default password!!!
- Home routers should be set to WPA-2 / Personal
- Keys should be 20-characters, consider a good passphrase
- DO NOT USE **WEP!!!**
- For more security turn on MAC address filtering

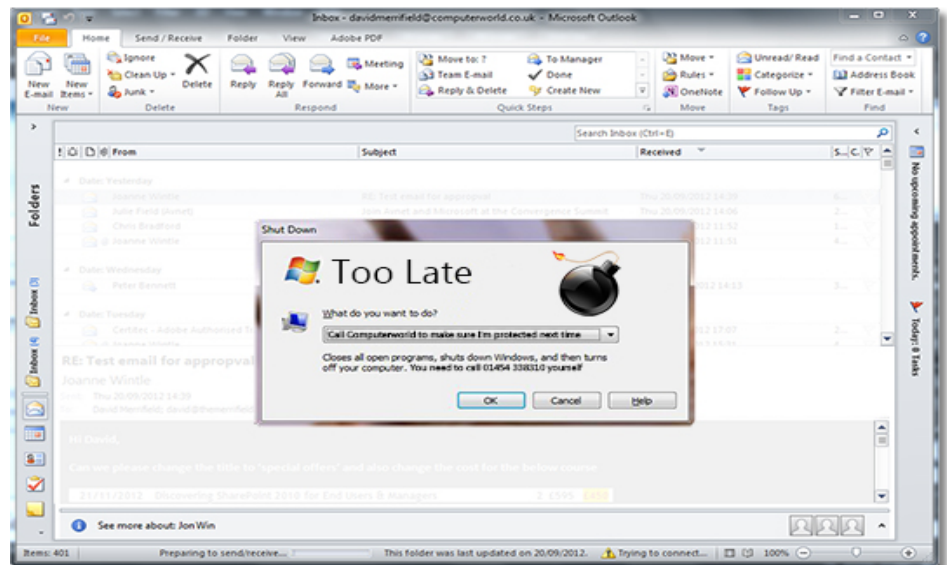
9. Email Part A

- The obvious, don't open links you suspect are bad
- Quick check the link – mouse over the link
 - Things you are looking for, misspelled words and links to foreign countries (qualifiers)



9. Email Part B

- Confidential information should not be sent via email
- Email is sent in clear text
- If you do need to send confidential email, use a secure mail service



9. Email Part C

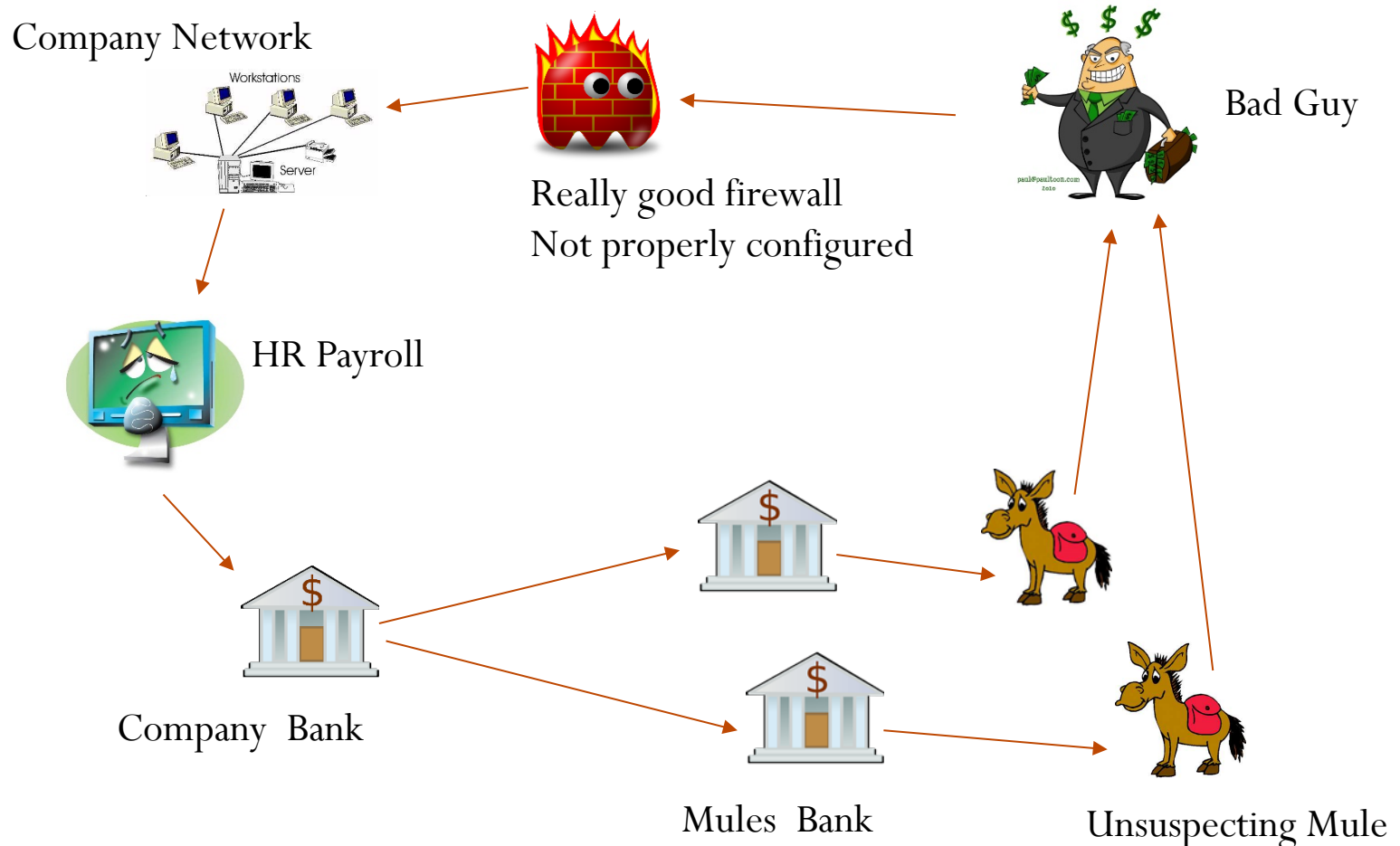
- Don't use your company email account for personal use
 - AFF Example 4,000,000 records stolen

10. Social Media

- Keep personal information personal
- Beware of links sent to you via social media
- Social media represents a major security threat to businesses



11. True Story of a \$280,000 Theft in the Miami Valley Region



Questions?