Ransomware
Pay up or Else!
How the Ransomware Epidemic Can Hold You Hostage & How To Handle It.

Presented by
Darragh Fitzpatrick
Partner & Executive VP
Background

How viruses and malware came about.
History of Viruses & Malware

- **1990s**: Hacking as a hobby
- **2000**: Internet becomes popular
- **2012**: Beginning of Ransomware
The first big hits!
Cyberattacks

The common perception

- Targeted attacks
- Mainly big companies
- Often political/other motivations
Bitcoin

- Completely anonymous
- No central owner/authority
- Enabled Ransomware
The Dangers of Ransomware

- Makes all your files/documents inaccessible
- Spreads itself to other computers
- The only way to get them back is to pay ransom
- Non-targeted
Ransomware as a Business

- Ransomware is a real business, done for-profit
- Hackers are untraceable
- Small companies are just as vulnerable as big ones
- No effective law enforcement to protect us

University pays $20,000 to Hackers

Hospital Pays $17,000 Ransom to Hacker
2. Prevention

How to make sure you’re not vulnerable to attack.
Backups

- Have good “offline” backups
- Use a trusted backup product or service
Security Software

- Watches activity on each PC
- Every PC & server on the network needs AV software
- Antivirus is only the tip of the iceberg, look for software that adds other forms of protection
E-mail Filtering

- Don't only rely on free filters
- Filter content such as ZIP files
- Block access to insecure e-mail systems

Update Your Information Within 48 Hours.

Dear Customer,

We have changed our policy terms, so we need from you to confirm you ID Apple and accept our new terms. **Policy Update.** To learn more about what's been changed, simply Log in to your ID Apple and click on policy updates under the notifications section.

Update Your ID Apple

Sincerely,
Apple Support
Web Filtering

- Ransomware & viruses don’t just come from e-mail
- Web browsers should be secured
Secure Your VPN & Firewall

- An infected computer on a VPN could take down the entire company
- Firewalls need to be checked periodically
• Set group policies to prevent malware from executing in temporary directories on Windows

• Disable unsigned macros in office
Training

- WE are the biggest vulnerabilities on the network
- Implement routine training
Prevention:

Summary

- Backups
- Security software
- E-mail filtering
- Web filtering
- Secure VPN & Firewall
- Block malware from executing
- Training, training, training!
3. Response

What to do if you’re attacked.
Backups

- First, check your backups
- Freeze/preserve them
Determine who’s infected

- Find out which computers are infected
- Disconnect them immediately to stop the spread
If you have good backups...

- Clean out and patch infected computers
- Delete infected files
- Restore from backups
- See "Prevention" steps
If you don’t have good backups...

- DO NOT plead with hackers
- Get Bitcoin and pay the ransom
- Input the decryption code before time runs out
- See “Prevention” steps for next time
Just to wrap up ...

- Ever increasing threat landscape
- Cybercrime is a business on the rise
- Malware is ever changing
- Don’t be Scared, be more Prepared