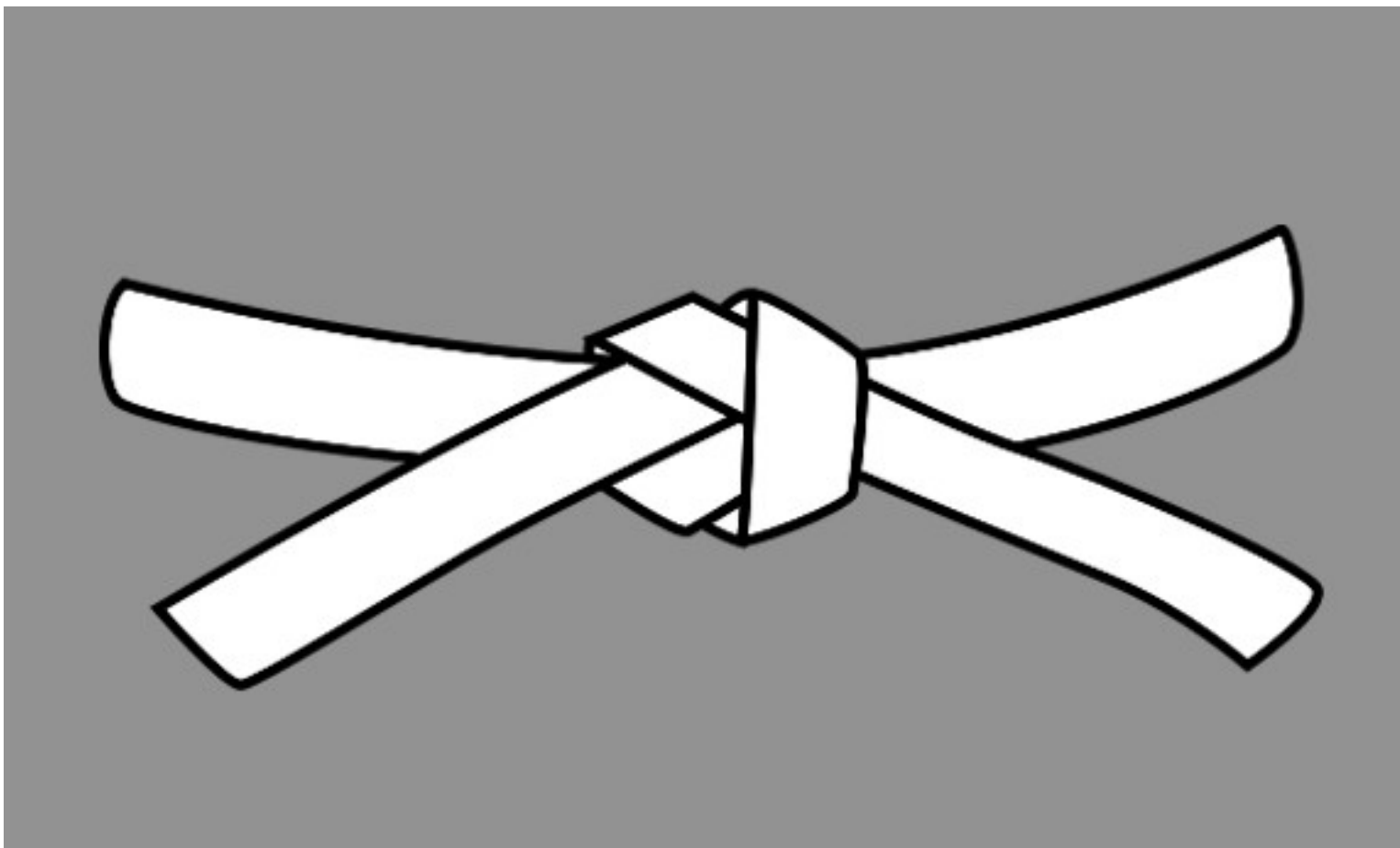
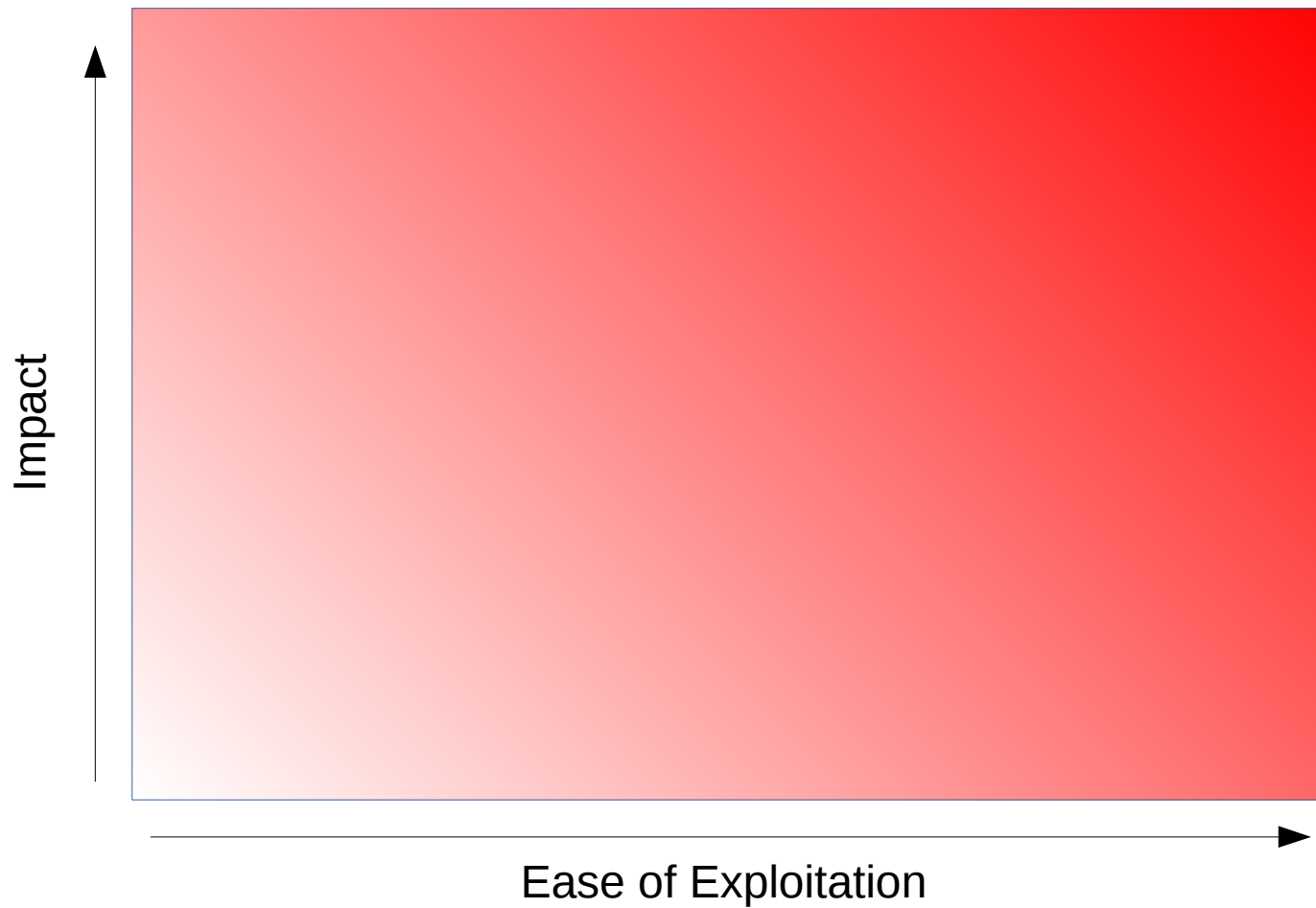


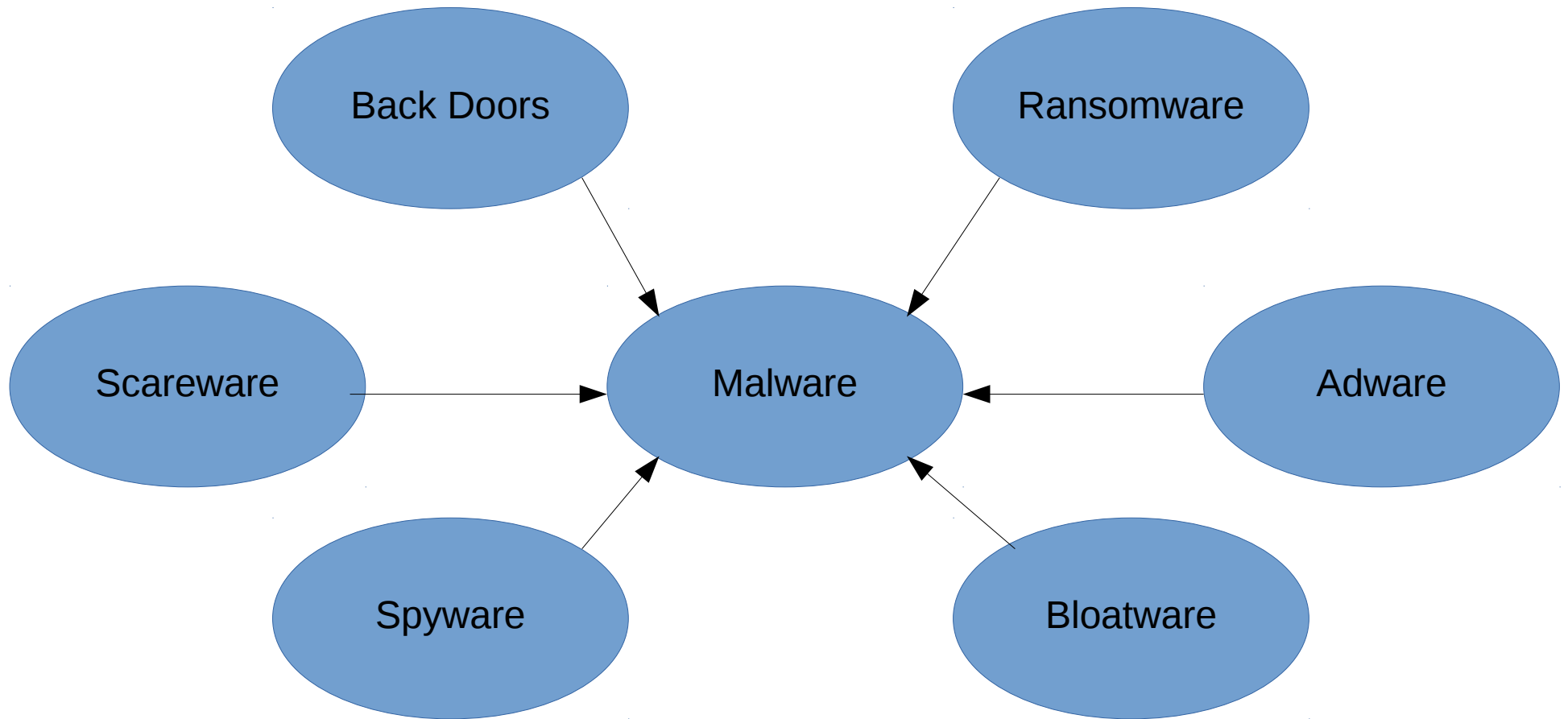
# Online Self Defense White Belt Level



# Assessing Your Risk



# Malware



# Phishing and Spear Phishing



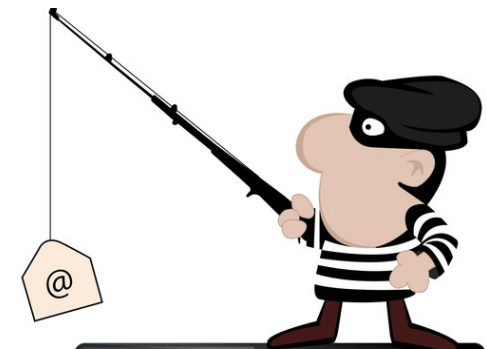
# Avoiding Phishing

- **Identify phishing emails**
- **Never click on links in emails**
- **Be suspicious of email attachments**
- **When in doubt contact the company that an email claims to be from**



# Phishing Response

- **Do Not click on any links**
- **Forward the email to [spam@uce.gov](mailto:spam@uce.gov)**
- **Contact the bank or company that the email claims to be from to alert them**
- **Do Not respond to the email**



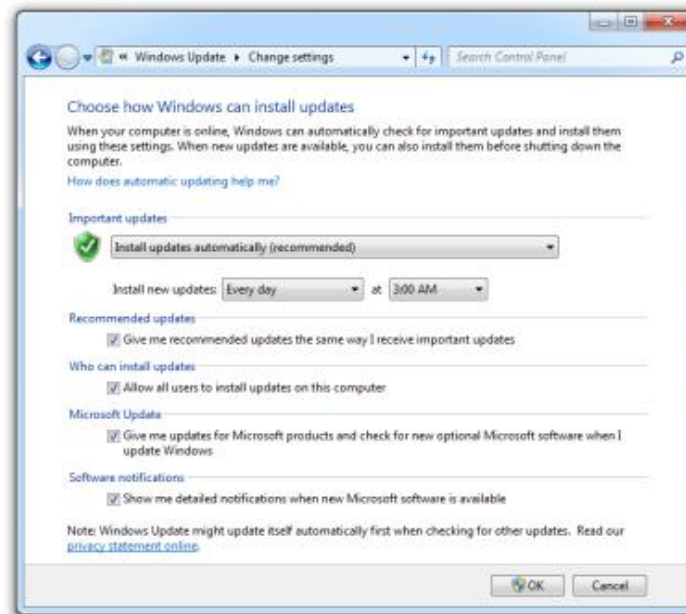
**Update ALL of your software**

**98% of software  
exploits are already  
fixed**



# Windows Updates

**Start button → Control Panel →  
Systems and Security → Windows  
Updates**





# Which Antivirus software to use

- Cost
- Ease of Use
- System Resources



# Backups

## 3-2-1 Rule

**3** Copies of data

**2** different types of media

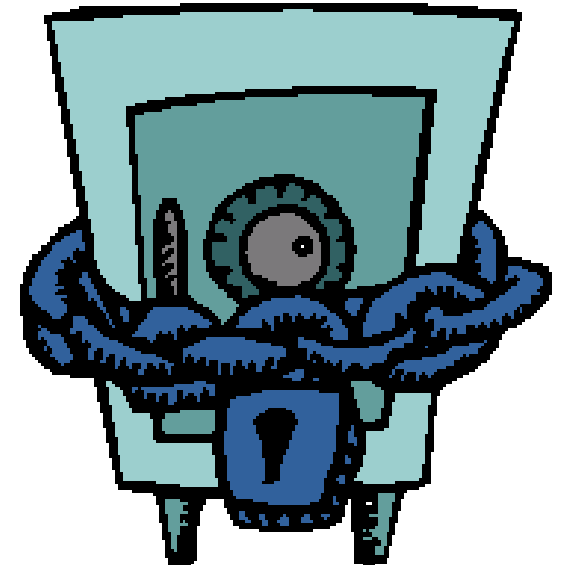
**1** copy offsite





# Safely Storing Passwords

- **Write it down**
- **Use a password vault**
- **Use two factor authentication**



# Questions



**Chuck McAndrew**

**[Chuck.mcandrew@leblibrary.com](mailto:Chuck.mcandrew@leblibrary.com)**

