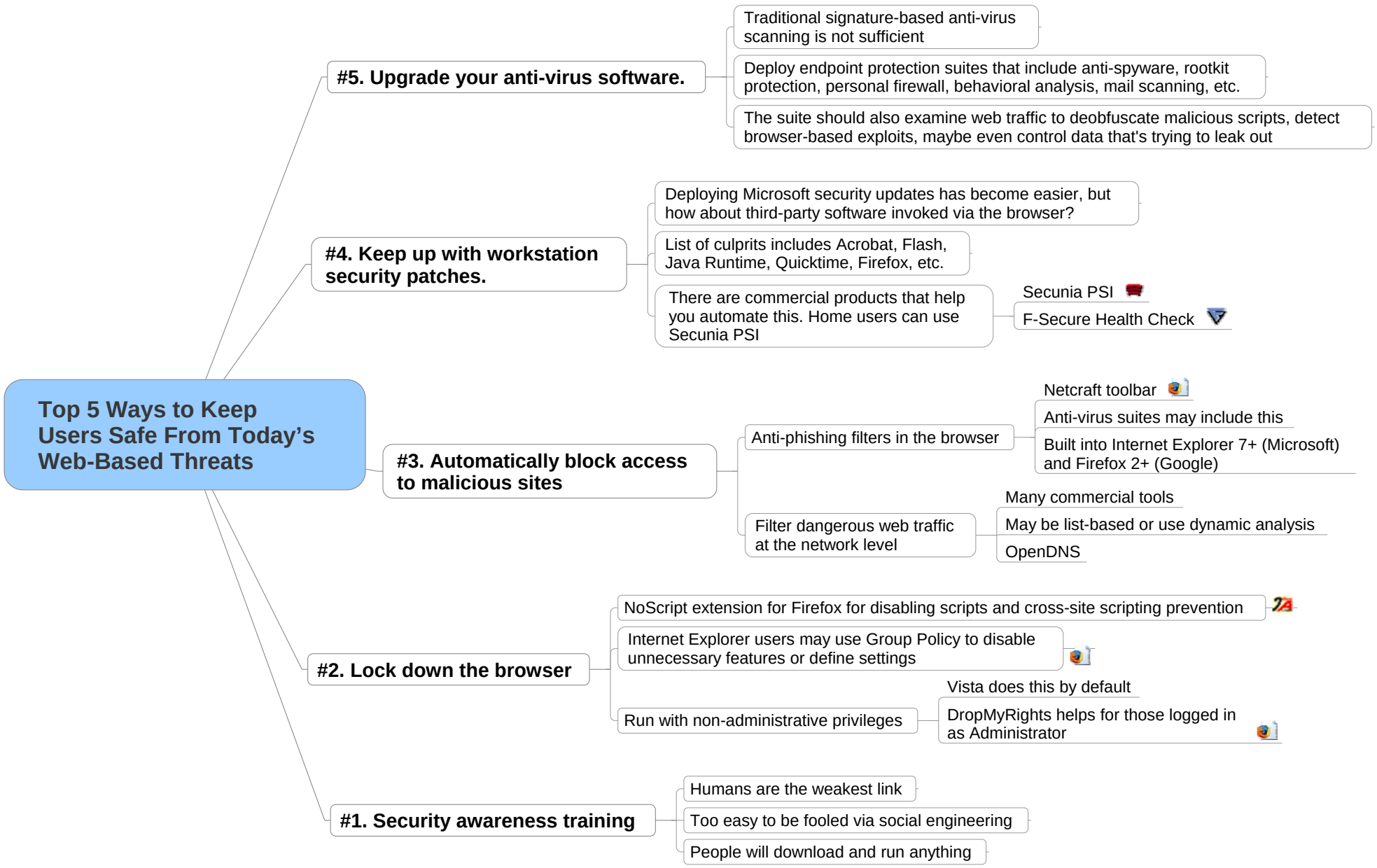
Top 5 Ways to Keep Users Safe From Today's Web-Based Threats
#5. Upgrade your anti-virus software.
Traditional signature-based anti-virus scanning is not sufficient
Deploy endpoint protection suites that include anti-spyware, rootkit protection, personal firewall, behavioral analysis, mail scanning, etc.
The suite should also examine web traffic to deobfuscate malicious scripts, detect browser-based exploits, maybe even control data that's trying to leak out
#4. Keep up with workstation security patches.
Deploying Microsoft security updates has become easier, but how about third-party software invoked via the browser?
List of culprits includes Acrobat, Flash, Java Runtime, Quicktime, Firefox, etc.
There are commercial products that help you automate this. Home users can use Secunia PSI
Secunia PSI
F-Secure Health Check
#3. Automatically block access to malicious sites
Anti-phishing filters in the browser
Netcraft toolbar
Anti-virus suites may include this
Built into Internet Explorer 7+ (Microsoft) and Firefox 2+ (Google)
Filter dangerous web traffic at the network level
Many commercial tools
May be list-based or use dynamic analysis
OpenDNS
#2. Lock down the browser
NoScript extension for Firefox for disabling scripts and cross-site scripting prevention
Internet Explorer users may use Group Policy to disable unnecessary features or define settings
Run with non-administrative privileges
Vista does this by default
DropMyRights helps for those logged in as Administrator
#1. Security awareness training
Humans are the weakest link
Too easy to be fooled via social engineering
People will download and run anything