Defending against direct download damage

CSC 7: Email and Web Browser Protections

Email and Web Browser Protections **Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**	
Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.

http://www.cisecurity.org/controls/

Defending against badness

CSC 8: Malware Defenses

Malware Defenses **Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**	
Utilize Centrally Managed Anti-malware Software	**Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.**
Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
Configure Devices to Not Auto-Run Content	**Configure devices to not auto-run content from removable media.**
Enable DNS Query Logging	**Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.**
Enable Command-Line Audit Logging	**Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.**

http://www.cisecurity.org/controls/