Protect Computing Devices

(1) Turn on Firewall : even if it is software or hardware to protect router
(2) Install Antivirus or AntiSpyWare : we must download them from trusted website and use them to provide another protect layer
(3) Manage Operating Systems an browsers : Turn on Security setting and always make Them Up to date
(4) Password Protection : you must use a strong password that has a combination of small and capital letters , Symbols and Numbers & it is preferable to doesn't make it with anything in your real life.
(5) We must set IoT devices in an isolated network as it is always connected to the internet and we can't handle any attack that affect it in the same time or easily

Secure Organization

Security appliances Standalone devices

(1) Routers : make basic traffic filtering
(2) Firewall : it looks deeper into network traffic it identifies malicious behavior that has to be blocked it also has sophisticated policies to apply on traffic
(3) Intrusion Prevention System IPS: use asset of traffic signatured match and block malicious traffic and attacks which mismatch the signatures
(4) Virtual Private Network VPN : let remote employees use secure encrypted tunnel from their mobile devices and secure connect back to organization network, it also interconnects branch offices with central office network
(5) Antivirus: system use signature behavioral analysis of application to identify and block malicious code from being executed
(6) Other : web & e-mail Security Appliances , Client Access Control , Security Management & etc …