Part 1

a. Since Bob is requesting Alice use a SHA-256 HMAC based on the same secret key she generated, this can potentially compromise the safety of the message because by using the same secret key to generate the HMAC, it provides to an attacker potential information about each block of the encrypted message (since they are using AES in CBC mode). Bob instead should request Alice to use a different key to generate the SHA-256 HMAC to increase the security when transmitting the message.

b. Since Alice has no knowledge of the CA, she has no way to check if the certificate from the CA is correct because she has no information about the CA and if the certs are valid. Therefore, if her certificate is tampered by an attacker, the attacker can draw information easily from her. Bob should make sure that the server sends the certs to Alice, along with both public keys and a signed version of the certificate to avoid tampering and ensure validity of certs.

c. Due to the fact that the hash and salt is being handled on the client's side, an attacker can intercept both and use the hash to brute force salts to access other passwords on the server. Bob should just request Alice the password being sent to the server, and the server should hash and salt it before storing it. This way it is safer because the hash and salt is being done locally on the server instead of receiving it through a package, which could be easily intercepted by an attacker.

d. Bob should not use an encryption mechanism to store Alice's password. If Bob uses encryption for passwords, that means he would need to store the encryption key in the server as well, which allows attackers to have access to it and possibly decrypt all the passwords on the server. Instead, Bob should hash and salt Alice's password to store it safely instead of encrypting it.

Part 2

a. Since Superfish is installed as a CA on the Lenovo computers, it adds a new security certificate to Windows. Therefore, whenever the computer tries to establish a SSL connection, the software steps in acting as MITM and issues a public key and then authenticates that it is valid. This allows Superfish to decrypt the content and inject ads to the message before re-encrypting everything. As the CA system is all based on trust, the browser doesn't know that the content was changed and goes on.

b. An attacker plays the role of MITM, so if an attacker somehow has the private key of Superfish, the attacker can pretend to be Superfish and sign a certificate for the attacker's website. Therefore, Lenovo users will see that website as secure when in reality it is a fake valid certificate generated by the attacker to make users think it is a safe website.

c. When a user notices that the amount of advertisements are showing while using a browser are more than normal, it might be the case that the computer is infected by Superfish. Then, the user can proceed to check the "Trusted Root Certification Authorities" from the certmgr.msc (on Windows) to search for Superfish Inc. If Superfish is installed, then the user can delete it there. Also, the user can check the certificates on the browser and distrust the one related to Superfish.