7 Techniques to Harden Computers

What is hardening a desktop?

Hardening is a process whereby a computer is made more resistant to cyber intrusion from malicious attack and from accidental infection. Hardening acts by remediating known vulnerabilities, by positioning the system to reject certain classes of attack, and by documenting system activities.

1. Create a Non- Admin Account / Standard User Account

- Local Computers / users don’t need administrator rights
- Remove local admin rights, elevate apps for users bypassing UAC password prompts

Create a non-admin account

- Click the Windows key and select Control Panel
- Click the User Accounts setting
- Create a new user, ensure that they are set to be a standard user.

2. Screen Saver Timeouts

- Stop Unattendant Access
- Inactivity Timeout

Recommend Time out 900 secs (15 minutes)

Screensaver Timeout:

- Click the Windows key and select settings
- Click on personalization
- Select Lock Screen on left-side pane
- Click screen saver settings
- Set wait time according to your "display off in power option" and check "on resume, display logon screen", then click ok

3.Use a Password Manager

- Complex Password or Password Phrase
- Two Factor Authentication Method
- Password should expire every 90 Days – Faculty & Students

Use a password manager

- Removes the need to remember a number of passwords
- Creates complex passwords
- Allows for passwords to be easily updated

4. Firewall Setting

- Turn Firewalls ON
- Allow programs or open ports vs turning off firewall
- Create Inbound & Outbound Rules to allow & monitor network traffic
- Block Programs with Remote Access
- Audit / Tune Firewall Rules
- Block Office Application that are not needed
- By default, Cortana, Sticky Notes, Microsoft Photos, 3D Viewer are allowed thru firewall
- By default blocked packets are not logged

Turn on your Firewall

- Open the Control Panel
- Click on System and Security
- Click on Windows Firewall.
- If the Windows Firewall is disabled, the Windows Firewall state will be Off. To turn it on, in the left navigation pane, click on Turn Windows Firewall on or off.
- In the Customize Settings window, select Turn on Windows Firewall and click OK.

5. Enable Full Disk Encryption

- Secure Boot
- Enable UEFI – Bios
- Enable BitLocker
- Encrypted files with EFS (Encrypted Files System)

Enable full disk encryption

- Locate the hard drive you want to encrypt under “This PC” in Windows Explorer.
- Right-click the target drive and choose “Turn on BitLocker.”
- Choose “Enter a Password.”
- Enter a secure password.
- Choose "How to Enable Your Recovery Key" which you’ll use to access your drive if you lose your password.
- Choose “Encrypt Entire Drive,” unless you need your drive to be compatible with older Windows machines, choose “New Encryption Mode.”
- Click “Start Encrypting” to begin the encryption process.

6. Check for Software Updates & Drivers

- Software & Hardware Updates
- Windows Updates
- Install Security Patches
- WSUS Server (Windows Server Updates Server)

Check for software updates automatically

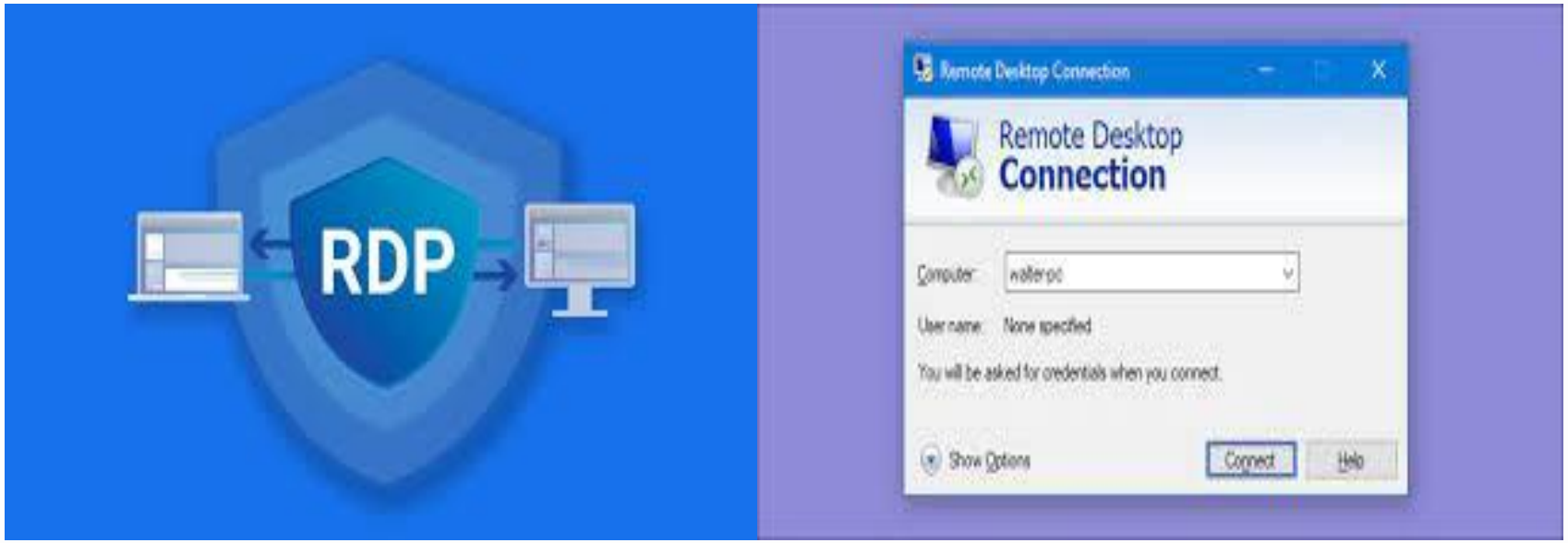
- Click on the Start button and select Settings.
- Click on Update & security.
- Choose Windows Update from the menu on the left
- Click on the Advanced options link on the right
- Select Automatic (recommended) from the drop-down

7. Disable Remote Access

- Disable Remote Desktop (RDP)
- VPN Client (ASA) – Cisco AnyConnect
- VPN Server for offsite network access

Disable Remote Access

- Click the windows key or select the Start menu
- Enter "remote settings" into the search box and select "Allow remote access to your computer".
- Check Don’t Allow Remote Connections to this Computer.



Benefits of Computer Hardening

While computer hardening requires a large, continuous effort, it provides substantial benefits for organizations. Here are several notable benefits:

- A higher level of security—the main purpose of system hardening techniques and tools is to reduce the attack surface. This translates into a significantly lower risk of malware, unauthorized access, data breaches, or other malicious activity.

- Better system functionality—system hardening best practices often involve reducing the amount of programs and functionality. This translates into less operational issues, reduced chance of misconfiguration which can affect user operations, less incompatibilities, and also reduced change of cyber attacks, which in themselves hurt user functionality.

- Simplified compliance and auditing—system hardening techniques can help turn a complex environment into a simpler one with less programs and accounts, and stable, predictable configuration. This translates into a more straightforward and transparent environment which is simpler to monitor and audit.