Lock Down a Workstation

Locking down your workstation means protecting your workstation with password while you are away. None of your open programs will be closed, and you will be taken back to exactly where you left off.

“The benefits of locked-down include that they lessen support costs because users can't break things. They also improve security because viruses and malware can't raise havoc with the users' admin rights. And, when all desktops are the same, software updating, and patching becomes far simpler[1].”

How to lock your workstation — Digital Services (jyu.fi)

[1] searchvirtualdesktop.techtarget.com/feature/Why-its-time-for-locked-down-desktops.

Configure Security Options to Ensure Only Authorized Users Have Access

- Create a BIOS password
- Make complex passwords
- Get hardware and/or software firewalls
- Make sure to get all patches and software updates
- Install some sort of anti-virus protection software on computer
- Use email safely and responsibly (be able to identify threats)

These are very important things for businesses to consider to keep their data secure, as well as the data of their employees.

How to prevent unauthorized computer access (computerhope.com)

Configure 802.1x Authentication

802.1x Authentication is useful to businesses because it allows people who are authorized to connect to the network. “It opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network[2].”

Windows-Manual Configuration - Information Technology Services | Binghamton University

[2] www.securew2.com/solutions/802-1x

Connect a Client to a VPN

It is very beneficial for a business to use a VPN. Through a business, sensitive information is always being passed around. That includes customer information, internal documents, internal communication, and other internal functions. A VPN adds a layer of encryption to all of this data that is being sent around.

How to Connect to a VPN on Windows:

1. Open **Settings**
2. Once Settings is opened, head over to **Network & Internet**
3. On the sidebar, select **VPN**
4. Click on **Add a VPN Connection**
5. Enter the information for the VPN connection
6. Once information is filled out, click **Save**

How to Connect to a VPN on Mac:

1. Open the **Apple Menu**, and select **System Preferences**
2. In System Preferences, select **Network**
3. Click the **Add Button** and select **VPN**
4. Enter VPN connection information
5. Click **Apply**, then **OK**

How to Implement SSH (Secure Shell)

SSH is important for businesses because it provides password or public-key based authentication and encrypts connections between two endpoints. Network administrators use it to manage systems and applications remotely, execute commands, move files, and deliver patches. These are all useful for businesses.

winscp.net/eng/docs/guide_windows_openssh_server

How to Implement an IPSEC

"Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs)[3]."

This is useful to a business because through a business, sensitive information is always being passed around. That includes customer information, internal documents, internal communication, and other internal functions. A VPN adds a layer of encryption to all of this data that is being sent around.

Windows 10 IPSec IKEv2 Setup Guide (ivpn.net)

[3] en.wikipedia.org/wiki/IPsec

How to Configure and Secure an RAS (Remote Access Server)

A Remote Access Server is useful to a business because it allows you to accomplish tasks from anywhere, instead of having to be in one place. You have access to all the devices and resources you need and is secure.

Step 1 Configure the Remote Access Infrastructure | Microsoft Docs

Step 2 Configure the Remote Access Server | Microsoft Docs

Step 3 Verify the Advanced DirectAccess Deployment | Microsoft Docs

Configure a Remote Access Policy for L2TP/PPTP

For a business, this adds structure and organization to who can do what within a network. "A remote access policy defines the conditions, remote access permissions, and creates a profile for every remote connection made to the corporate network[4]."

L2TP Remote Access | IT Pro (itprotoday.com)

[4] www.sciencedirect.com/topics/computer-science/remote-access-policy

How an IT Professional Can Analyze the Performance, Efficiency, and Security of the Network Based on Network Monitoring and Diagnostic Software

"Network monitoring software is designed to provide automated support for some, or all of the network management functions. Network monitoring software systems are used to perform some of the functions of monitors and analyzers, identify errors, run diagnostic tests, monitor an entire network, compile statistics, and prepare real-time management reports. Network monitoring software systems are important because they signify improved or deteriorating conditions[5]."

Network Monitoring Software | Network Performance Monitoring (applicationperformancemanagement.org)

[5] www.applicationperformancemanagement.org/network-monitoring/network-monitoring-software