1) Create a standard user account without administrative privileges

Right click on “My Computer” and select “Manage”

Go to “Local Users and Groups -> Users, right click on “Users” and select “New User”
Type in all the required information and uncheck “User must change password at next logon”

Use a unique, strong password

The blank “New User” form will re-appear, click “Close”
2) Confirm that the computer they will be working from is at the latest service pack level

Right click My Computer and click Properties

Look to ensure it is running the appropriate operating system and Service Pack
- Windows XP Service Pack 3
- Windows Vista Service Pack 2
- Windows 7 **All versions
3) Confirm that the computer is set to automatically check for updates and that patches are applied as soon as the computer makes them available.

Go to Start -> Settings -> Control Panel

Double click “Automatic Updates”
4) Install FileHippo Update Checker to identify the status of 3rd party applications (Java, Adobe Flash/Reader/Shockwave, etc.); It’s imperative that these be updated as this will probably be the primary vector malicious sites will try to exploit.


5) Install Symantec Endpoint Protection (SEP) and run a daily, full scan.

Install- [https://software.udayton.edu/](https://software.udayton.edu/)

In the task bar, right click the yellow shield and select Open Symantec Endpoint Protection
Select “Scan for threats”

Click the “Run Full Scan” link
6) Turn the computer’s firewall on (either Window’s or the firewall that comes with SEP).

Open Control Panel and select Windows Firewall

Ensure “On (recommended)” is selected then click “OK”
7) Use either Internet Explorer 8 or Mozilla Firefox 3.6.8 (or later) w/ default security protections (block up, zone restrictions, no trusted sites, etc.).

Open Internet Explorer, then select Help, About Internet Explorer

Should be running Internet Explorer 8, if not upgrade can be downloaded here: http://www.microsoft.com/windows/internet-explorer/worldwide-sites.aspx
MOZILLA

Open Mozilla Firefox, then select Help, About Mozilla Firefox

Ensure version of Firefox is current, if not upgrade can be downloaded here: http://www.mozilla.com/
8) If using Windows XP, apply the securews security template. Most of the settings are default in Windows Vista and Windows 7.

Start -> Run

Open Security Configuration and Analysis, click Start, and click Run, then type mmc and click OK.
On the File menu, click Add/Remove Snap-in

Click “Add”
Select Security Configuration and Analysis, click Add, and then click OK.

In the console tree, right-click Security Configuration and Analysis, and then click Open Database
Type a name, like “NEW” for a new database and click Open

Select “securews.inf” and click Open
The screen above should tell you the next step which is to configure

Select “Actions -> Configure Computer Now…”
Accept the default and click OK, template has been applied

In Import Template, click a template, and then click Open.
In the console tree, right-click Security Configuration and Analysis, and then click Configure Computer Now.
Do one of the following:
• To use the default log, in Error log file path, click OK.
• To specify a different log, in Error log file path, type a valid path and file name.

9) Disable Autorun for all removable media.

Click Start -> Run
10) Disable NetBIOS/File and Print Sharing. These fall into the category of unnecessary (as well as easily exploited) services.
Right click on one of your connections (this action will be completed on each connection) and select “Properties”

Uncheck “File and Printer Sharing for Microsoft Networks” then highlight “Internet Protocol Version 4 (TCP/IPv4)” and click Properties
Click “Advanced…”

Ensure “Disable NetBIOS over TCP/IP” is selected, and then click OK, OK, OK

11) Periodically run a free, full online scan from another well know, trusted vendor.

For assistance with these procedures please contact:

IT Risk Management Office
itriskmgmt@notes.udayton.edu