How to Not Login as Administrator (and still get your job done)

What’s wrong with running as administrator?

Both Windows and Max OS X make the initial user account created during setup an administrator. This is necessary, as many actions can only be performed by an administrator and every machine needs at least one such account. However, neither operating system does a good job educating users as to why they should not want to use this account as their primary account. Microsoft has recommended for years that users not operate their computer as an administrative user.

Because administrative accounts are granted the ability to do essentially anything on the computer, every computer has one, and the majority of users use one as their sole/primary account, many forms of malware depend on using these accounts to wreak havoc. With an administrative account, malware has an easier time:

- Installing keyloggers, back doors, and root kits
- Hiding itself, modifying event logs, and covering activity
- Creating new administrator accounts
- Accessing privileged services
- Entrenching itself so it's harder (impossible) to remove without reformatting
- Using an infected computer as a launching point to infect other computers on the network

The difficulty involved in tracing what a piece of malicious software has done when it has administrator access is so hard, it's often not worth it and is really impossible to ever be sure that some piece hasn't been left behind. A more secure option is to use a normal, non-privileged account for day to day activity, and use an administrator account only when required. Most of the time, this doesn't involve any extra work, just a bit of setup in advance. For an example of the difference this can make, consider Avecto's analysis of the vulnerabilities published in 2014 by Microsoft, in which they found that simply running Windows under an account that does not have administrative rights mitigates:

- 98% of critical vulnerabilities affecting the Windows operating systems
- 99.5% of vulnerabilities affecting Internet Explorer
- 95% of critical vulnerabilities affecting Microsoft Office
- 97% of the critical vulnerabilities reported in 2014
- 80% of all Microsoft vulnerabilities published in 2014

So what is an administrator account anyways?

On a standalone machine, not part of an Active Directory, an Administrator is an account that is a member of the Administrators group as illustrated below. Users may also be designated as Administrators in the User Accounts section of the Control Panel.

On computers that are joined to an Active Directory, Administrator accounts are members of the Local Administrators or Domain Administrators group.

An Administrator account is one that has been granted the ability to administer the computer through the Accounts pane in System Preferences as illustrated in the screen shot below.
**What can an administrator do?**

The answer here is really anything. There's nothing an Administrator account *cannot* do. So while some specific examples are presented below, keep in mind that Administrators aren't limited to these tasks and the list is by no means comprehensive.

<table>
<thead>
<tr>
<th>Windows</th>
<th>Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Install and update applications for all users ✅ Install new services and applications that run at start up ✅ Windows Updates ✅ Install drivers for new hardware devices (e.g. printers) ✅ Create and modify user accounts ✅ Change network settings</td>
<td>✅ Install applications that modify the system (i.e. it has an installer) ✅ Install and update applications for all users ✅ Apple Software Updates ✅ Enable network services (e.g. SSH, AFS, etc.) ✅ Create and modify user accounts ✅ Make changes to any setting available in System Preferences</td>
</tr>
</tbody>
</table>

**How do you not run as administrator?**

<table>
<thead>
<tr>
<th>Windows</th>
<th>Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guide to not running as administrator for Windows</td>
<td>Guide to not running as administrator for Mac OS X</td>
</tr>
</tbody>
</table>