

## Re: Basic Security Help

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-06/0150.html>

---

**From:** Kymberley (Kymberley\_at\_discussions.microsoft.com)

**Date:** 06/07/05

Date: Tue, 7 Jun 2005 04:40:03 -0700

The info provided to 'eddie' sounds experienced & educated. I have a question of my own. I did a dumb thing and i don't know how to "undo" it. i set up a system password – and promptly forgot it – ; I also changed the logon screen from "welcome" to the more secure logon screen using a username and password.. I have no idea how to get around it. Please help!!! Can you help me? Can I reload my windows xp application cd and get around the login password that way.?

"Steven L Umbach" wrote:

- > *There are plenty to great articles as shown in the links below. The main*
- > *things that you can do to start are the following many of which are common*
- > *sense items that need to be implemented and used. By far the biggest risk to*
- > *a network is weak or no passwords followed by malicious user on your*
- > *network.*
- >
- > *-- Use password policy to enforce strong passwords in the domain by enabling*
- > *password complexity and using password no less that seven characters in*
- > *length. Be sure to educate users of any pending changes to password policy*
- > *and get users to think of pass phrases instead of passwords.*
- >
- > *-- Be sure that computers are kept current of critical security updates from*
- > *Windows Updates or using a SUS server to authorize and distribute security*
- > *updates which can be done automatically with Automatic Updates.*
- >
- > *-- Have virus protection on all of your computers that also is kept current*
- > *with virus definitions, scans all emails, and does scheduled full system*
- > *virus scans.*
- >
- > *-- Modify the user rights for access this computer from the network to*
- > *restrict which users/groups can access a computer for file and print*
- > *sharing. Be careful using the deny access to this computer from the network*
- > *as it overrides the allow user right and remember that administrators are*
- > *also in the users/everyone group.*
- >
- > *-- Have an action plan now for what to do if you discover viruses on your*
- > *network including how to isolate and repair infected computers. The free*
- > *Antivirus in Depth Guide available at the TechNet Security Center can help*

microsoft.public.security: Re: Basic Security Help

- > *you plan such.*
- >
- > -- *Use a firewall at the perimeter to protect your network computers and*
- > *periodically scan it from the outside to make sure it is doing its job as*
- > *configured. The free self scan sites such as <http://scan.sygatetech.com/> can*
- > *be of help.*
- >
- > -- *Make sure that the number of domain administrators is kept to a minimum*
- > *of qualified and trustworthy people and that regular domain users are not*
- > *also "local" administrators unless you have a compelling business reason for*
- > *such. Never allow any domain user to share user accounts or passwords.*
- >
- > -- *Windows 2003 should already have auditing enabled by default in Domain*
- > *Controller Security Policy. Be sure to check the security logs periodically*
- > *looking for unauthorized account management events and suspicious failed*
- > *logon attempts.*
- >
- > -- *Never logon to a domain workstation computer that is not a secure admin*
- > *workstation as a domain administrator as you risk capture of your*
- > *credentials or their exploitation by malware/hacker.*
- >
- > -- *Disable non essential services on domain computers. Use the Microsoft*
- > *Baseline Security Analyzer to help with such as it can scan your network*
- > *computers and also report other vulnerabilities such as missing critical*
- > *security updates.*
- >
- > -- *Physically protect to some degree your domain controllers and any other*
- > *critical domain computers with sensitive information.*
- >
- > -- *Don't underestimate the impact of social engineering on network security.*
- > *Helpful users often gladly give access or passwords to those that ask for*
- > *such nicely posing to be part of the IT staff or a big boss. Training,*
- > *strict procedures, and awareness is the best defense against such.*
- >
- > -- *Don't tolerate unauthorized computers or Wireless Access Points on your*
- > *network that may be poorly secured or even infected with malware. This*
- > *mainly can be employee laptops. Have a written computer use policy that the*
- > *employee/user signs and understands the consequences.*
- >
- > -- *Use Group and security policy to uniformly manage security and*
- > *configuration of your domain computers. One good example would be to force*
- > *computers to lock their desktop after a period of idle time. The free Group*
- > *Policy Management Console can make that task much easier.*
- >
- > -- *Backups are a must part of securing a network. For domain controllers be*
- > *sure to backup the "System State" on a regular basis as that is where your*
- > *Group Policy and other Active Directory objects such as users, groups, and*
- > *computers are stored. Have a disaster recovery plan and try it out sometime*
- > *on a test network so that you know what to do if the real deal happens.*
- >
- > -- *If you want to try and change security policy settings such as security*

microsoft.public.security: Re: Basic Security Help

- > *options it is best to test out the changes on a test computer in a test*
- > *Organizational Unit.*
- >
- > *That should be a start but maybe it is not what you expected. Securing a*
- > *network is much more than some registry tweaks and modifying ntfs*
- > *permissions. Be sure to read the Windows 2003 Server Security guide and the*
- > *Threats and Countermeasures Guide that are available at TechNet Security*
- > *Center. --- Steve*
- >
- > *<http://www.microsoft.com/technet/security/tools/mbsahome.mspx> --- MBSA*
- > *<http://www.microsoft.com/windowsserver2003/gpmc/default.mspx> --- GPMC*
- > *<http://www.microsoft.com/smallbusiness/support/computer-security.mspx> --*
- > *Small business security guidance center*
- > *<http://www.microsoft.com/technet/security/default.mspx> --- TechNet Security*
- > *Center*
- >
- >
- > *"Eddie" <Eddie@discussions.microsoft.com> wrote in message*
- > *news:350C21EF-AFDE-4912-8045-1649B9270462@microsoft.com...*
- > > *I have a windows 2003 single domain in native mode. All of my workstations*
- > > *are windows 2000 pro or xp pro. all of my windows servers are 2003. I want*
- > > *to*
- > > *lock down security but I am affraid of causing problems. any articals i*
- > > *can*
- > > *read. also any advise would be great.*
- >
- >
- >