Boas práticas para a criação de contas de usuário - Parte 1

2. Use pelo menos duas contas (conta normal e conta de administrador)
Você não deve fazer login todos os dias com uma conta de administrador local ou com acesso privilegiado (Admin de Domínio).

Em vez disso, crie duas contas, uma conta normal sem direitos de administrador e uma conta privilegiada que é usada apenas para tarefas administrativas.

MAS
Não coloque sua conta secundária no grupo Admins. Do Domínio, pelo menos permanentemente.

Em vez disso, siga o modelo administrativo de menos privilégios. Basicamente, isso significa que todos os usuários devem fazer logon com uma conta que tenha as permissões mínimas para concluir seu trabalho.

Você pode ler em outros artigos e fóruns para colocar sua conta secundária no grupo Admins. Do Domínio.

Esta **não é uma prática recomendada da Microsoft** e eu desaconselho. Novamente, temporário está OK, mas precisa ser removido assim que o trabalho seja concluído.
Você deve usar uma conta normal que não seja de administrador para as tarefas do dia a dia, como verificar e-mail, navegar na Internet, sistema de tíquetes e assim por diante. Você só usaria a conta privilegiada quando precisasse realizar tarefas administrativas, como criar um usuário no Active Directory, fazer login em um servidor, adicionar um registro DNS, etc.

Observe esses dois cenários.

- Cenário 1 - Equipe de TI com direitos de domínio

Steve faz login em seu computador com uma conta privilegiada, verifica seu e-mail e, inadvertidamente, baixa um vírus. Como Steve é membro do grupo DA, o vírus tem direitos totais sobre seu computador, todos os servidores, todos os arquivos e todo o domínio. Isso pode causar sérios danos e resultar na queda de sistemas críticos.

Agora, considere o mesmo cenário, mas desta vez Steve está conectado com sua conta normal de não administrador.

- Cenário 2 - Equipe de TI com direitos regulares

Steve verifica seu e-mail e, inadvertidamente, baixa um vírus. O vírus tem acesso limitado ao computador e nenhum acesso ao domínio ou a outros servidores. Isso causaria danos mínimos e evitaria que o vírus se propagasse pela rede.

Simplesmente usando uma conta normal, você pode aumentar a segurança e evitar causar danos graves.

É muito fácil delegar tarefas administrativas sem conceder direitos de administrador de domínio à equipe. Aqui estão algumas tarefas comuns que podem ser delegadas a uma conta de administrador secundária.

- Direitos para usuários e computadores do Active Directory
- DNS
- DHCP
- Direitos de administrador local em servidores
- Política de grupo
- Troca
- Direitos de administrador local em estações de trabalho
- Administração Vsphere ou Hyper-v

Algumas organizações usam mais de duas contas e usam uma abordagem em camadas. Isso é definitivamente mais seguro, mas pode ser um inconveniente para alguns.

- Conta normal
- Conta para administração de servidor
- Conta para administração de rede
- Conta para administração de estação de trabalho

Ao usar duas contas e implementar o modelo com menos privilégios administrativos, você reduzirá muito os riscos de segurança e evitará situações como o cenário 1.