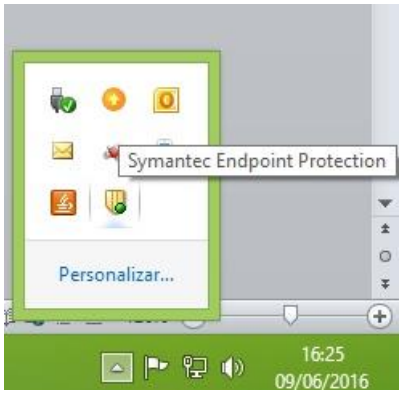
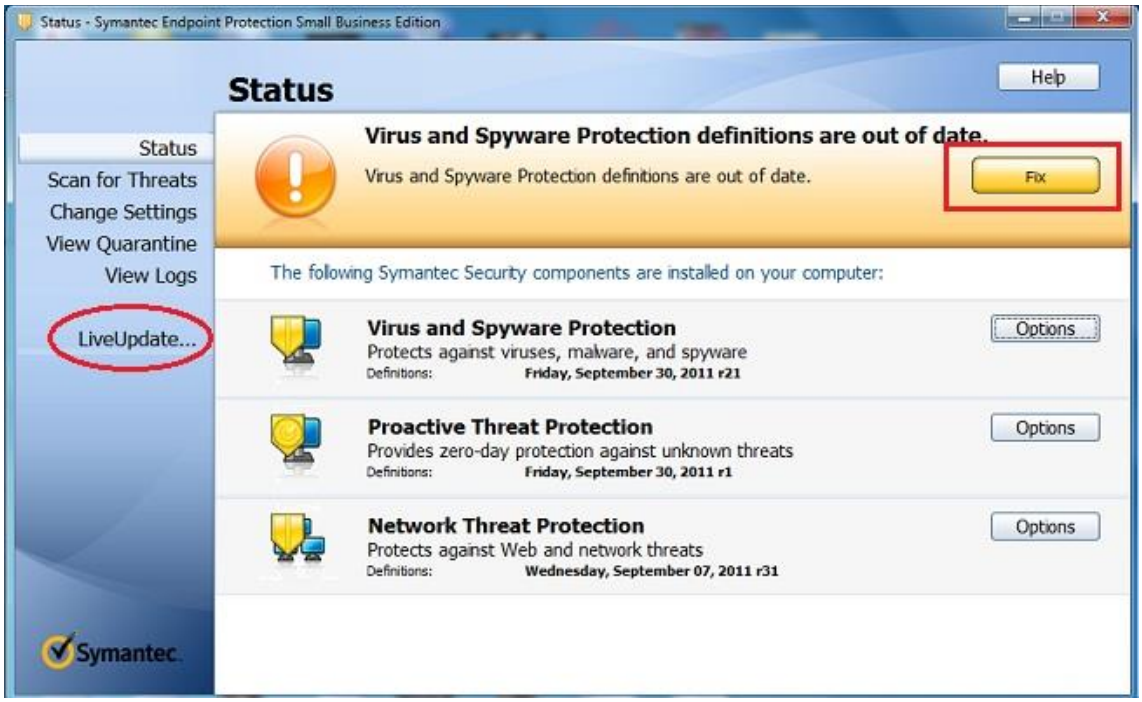
Recomendações mínimas de segurança para os computadores de trabalho da UFABC

1. Verifique diariamente se a vacina do antivírus está atualizada;

Para isso, inicie o programa antivírus localizado na barra de tarefas, ao lado do relógio clicando duas vezes (Windows).



Se a vacina estiver desatualizada, haverá uma mensagem de erro no status do antivírus, conforme a imagem seguinte:



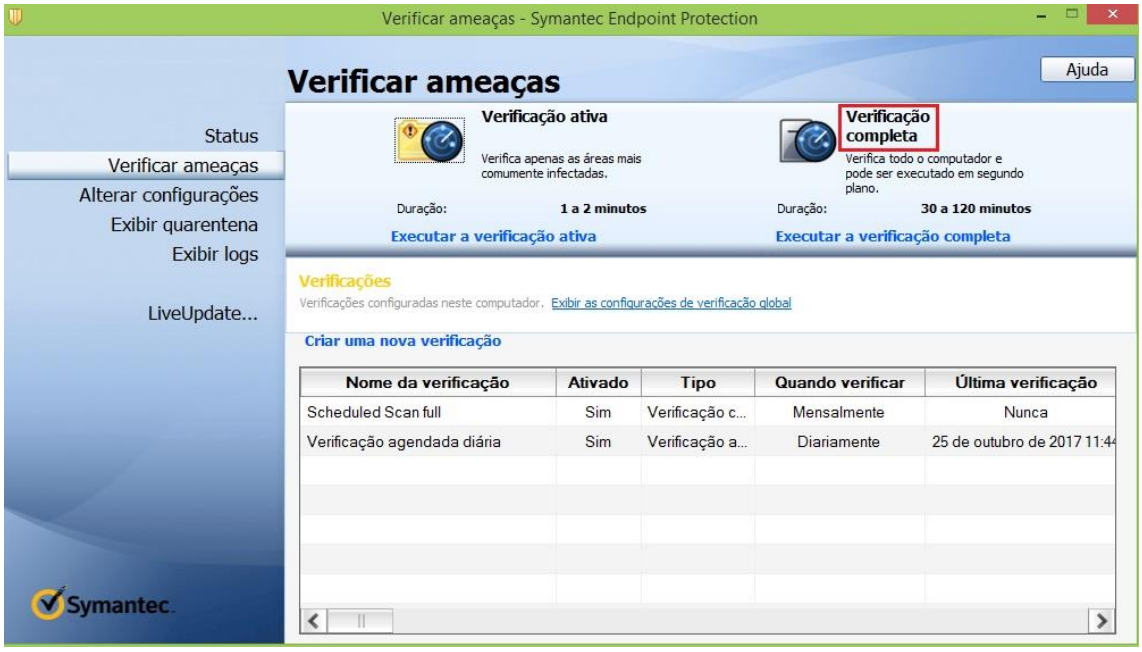
Neste caso, clique em "*Fix*" ou em *"LiveUpdate"* para atualizar as definições de vírus.

O status deverá mudar, conforme demonstra a seguinte imagem:

2. Realize uma verificação completa do antivírus pelo menos uma vez ao mês.

Para isso, clique na guia “Verificar ameaças” (S*can for Threats*), conforme a imagem a seguir:

Depois, clique em verificação completa *(Full Scan)*, conforme a imagem a seguir:



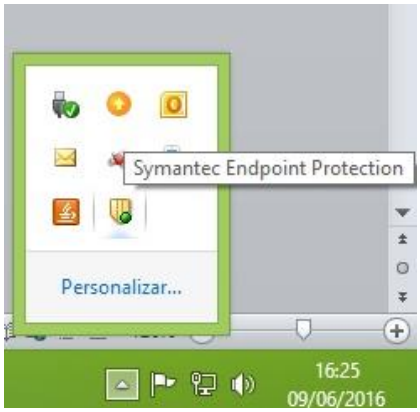
Obs: A verificação ativa (*active scan*) do antivírus é um tipo de verificação "resumida" realizada diariamente.

As verificações completas só funcionam se a verificação do antivírus não tiver sido cancelada pelo usuário. Caso a verificação completa não tenha sido realizada por um longo período, o sistema iniciará a verificação automaticamente.

A verificação completa também poderá ser agendada.

3. Verifique se o antivírus está conectado ao servidor de vacinas ou se está off-line.

Para isso, certifique-se de que há um sinal verde ao lado do ícone do programa antivírus localizado na barra de tarefas do Windows, ao lado do relógio conforme indica a imagem:



Caso ele esteja off-line, não haverá sinal algum, conforme indica a seguinte imagem:

Se o antivírus estiver off-line, solicite o atendimento para solucionar este problema pela central de serviços da UFABC.

Além da central de serviços, você poderá enviar uma mensagem para o seguinte e-mail: abuse@ufabc.edu.br

Outras dicas de segurança:

4. Mantenha o seu sistema operacional sempre atualizado;
5. Não clique em links ou baixe arquivos de e-mails suspeitos ou não reconhecidos como de origem esperada;
6. Não faça downloads de softwares não licenciados;
7. Não faça downloads de softwares de fontes não confiáveis;
8. Siga as normas internas de segurança da informação;
9. Realize o backup dos seus arquivos importantes diariamente ou pelo menos uma vez por semana;
10. Sempre notifique o NTI sobre possíveis incidentes causados por ações de vírus;