



# How to protect your self from Wanacrypt

Wanacrypt is a virus that encrypts your files (Ransomware) and can also spread via your LAN (Worm). Here's how to protect your self against this virus.

Written By: WindowsUser2017

A screenshot of the Wanna Decryptor 2.0 ransomware interface. The window title is "Wana DecryptOr 2.0". The main message is "Oops, your files have been encrypted!".

**What Happened to My Computer?**  
Your important files are encrypted.  
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

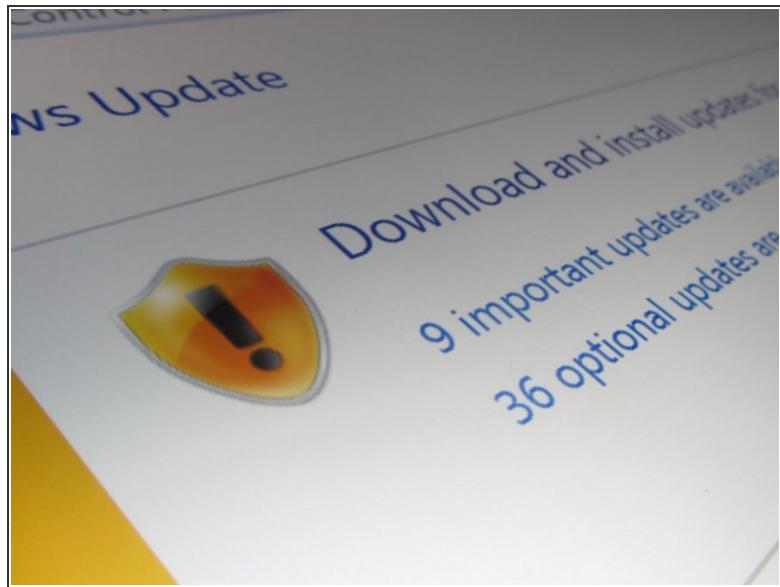
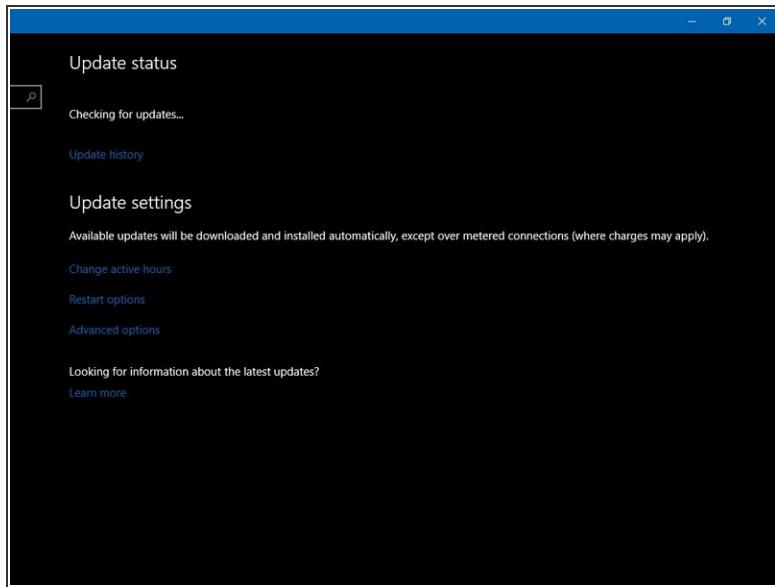
**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CDT, Mon - Fri.

**About bitcoin** **How to buy bitcoins?**

**Contact Us** **Check Payment** **Decrypt**

Send \$300 worth of bitcoin to this address:  
**12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw** **Copy**

## Step 1 — Update your computer (Windows Vista or newer)

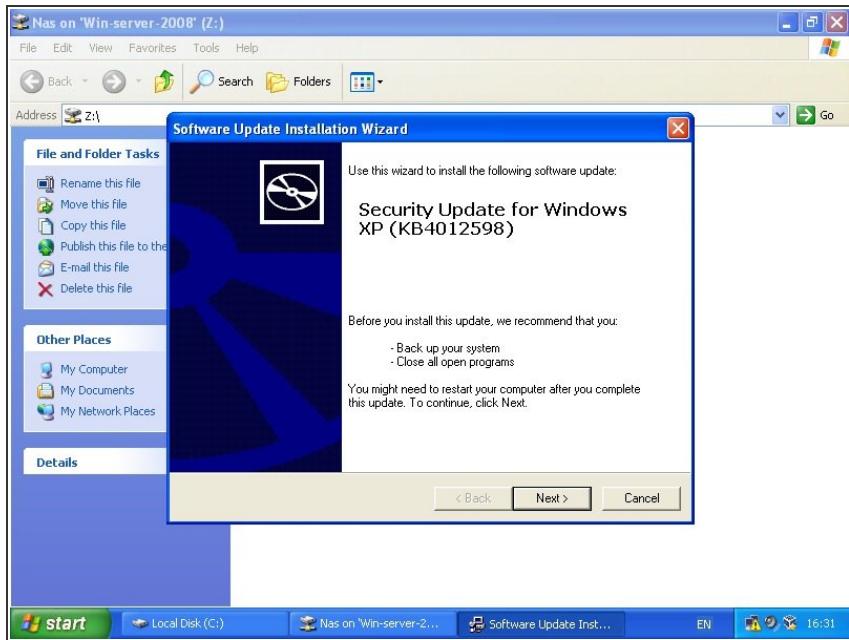


- Update your computer.

*(i)* Microsoft has patched the security flaw that Wanacrypt exploits in March 2017 for computers running Windows Vista or newer.

! Windows Vista support has ended since 11th April 2017

## Step 2 — Update your computer (Windows XP, Server 2003 or 8)



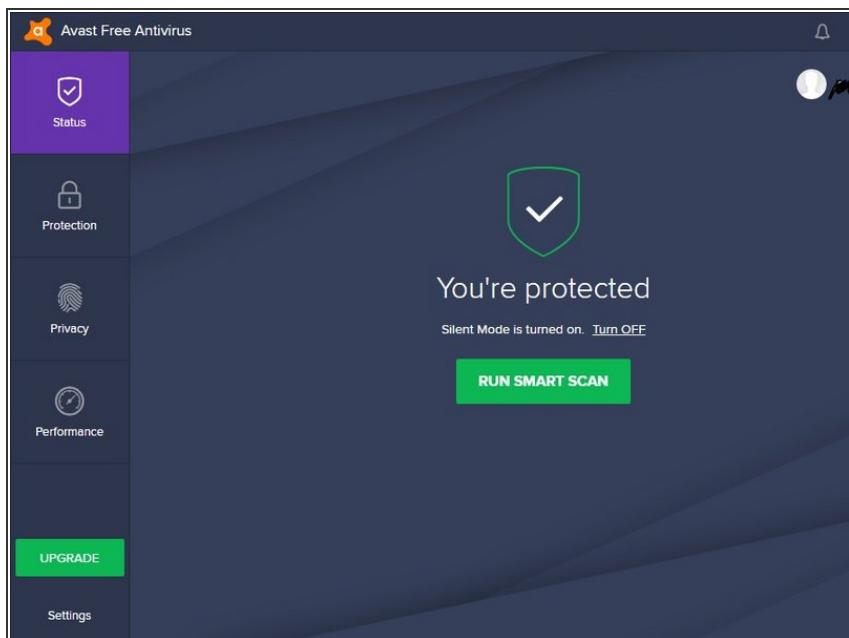
⚠ Windows XP, Server 2003 and 8 support has ended.

- Although Microsoft has ended Windows XP support in 2014, Server 2003 in 2015 and Windows 8 (Not 8.1) in 2016. Microsoft has issued a patch for Windows XP (both 32 and 64 bit), Windows Server 2003 (Both Server 2003 and 2003 R2) and Windows 8.

⚠ Since Windows XP, Server 2003 and 8 support has ended you should upgrade your computer to a newer version of Windows.

- You can download the updates [here](#)

## Step 3 — Anti Virus, Anti Malware



- Keep an up-to-date Antivirus. An Antivirus is very important to protect your self against virus attacks
- You can help your Antivirus by installing an Anti-Malware program such as [Malwarebytes](#) or [Hitman Pro](#)

## Step 4 — Back up, Back up, Back up



- Backup your important files. You can do this by USB flash drive/hard drive.

## Step 5 — Disable SMB 1



- Disable SMB 1 on your computer, you can learn how [here](#)

## Step 6 — What if I'm already infected?



- Sorry but your files are lost forever...  
:(
- ⚠ DON'T pay the ransom as there is no proof that you'll get your files back!
- Disconnect your computer from your network to prevent it from spreading.
- Reinstall Windows, if you need help, [Click here](#)
- ↗ This is where your backup comes into play as the backed up files can be recovered and you can continue working.

This is how to protect your self from Wanacrypt.