

SCAM ALERT!

Beware of unsolicited phone calls from suspects who claim to be calling from legitimate IT companies. The scammer will allege that your computer is infected and in need of urgent repair. The victim will be guided to allow remote access to their computer for the fake technician to assess the issue.

DO NOT GIVE THEM ACCESS!

They could potentially infect your PC with a Cryptolocker virus which renders your device unusable and requires payment to be removed. They also have the ability to steal your personal information.

If you believe you have been the target of this scam or similar, you can report to your local Police Station or online via:

<https://www.acorn.gov.au/>

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
04/04/2017
6:00pm

Time left

07:54:04

Next >>