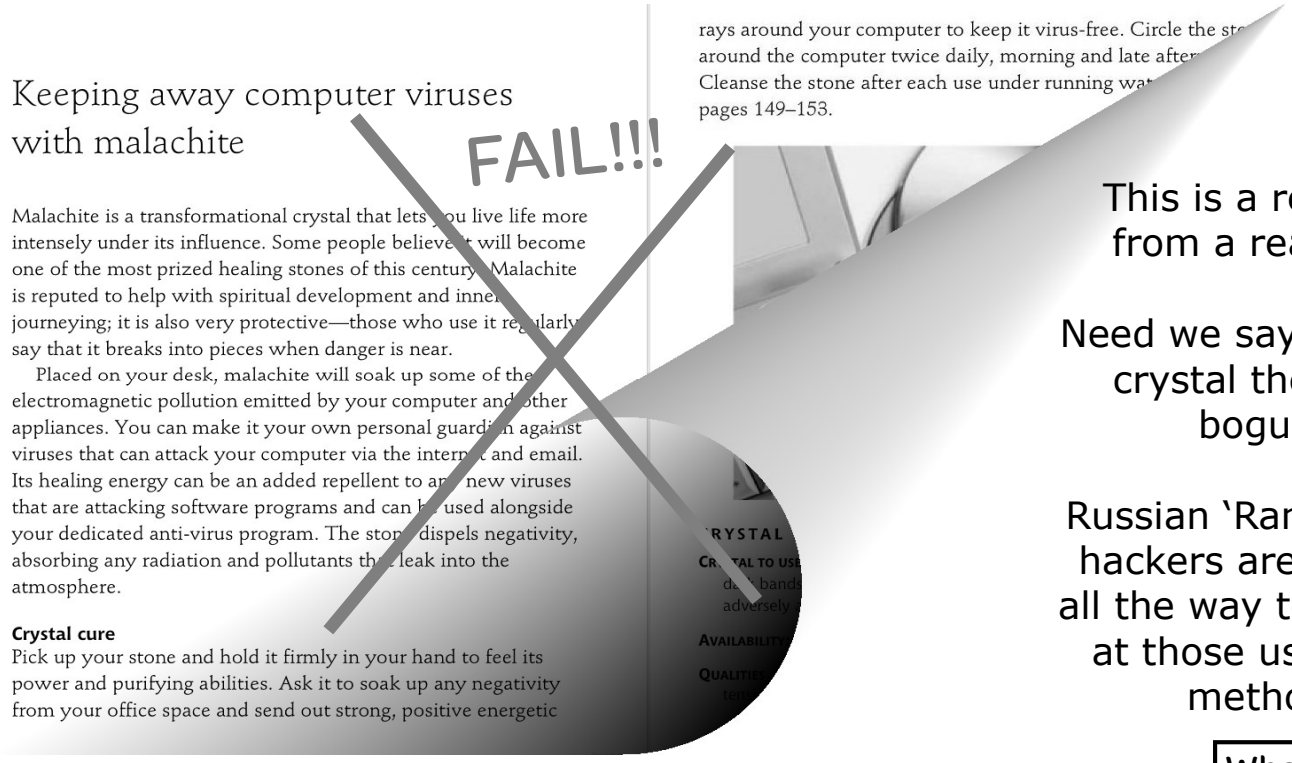
a little CRC...

Northcliffe Community Resource Centre
Tel: 9776 7330
Fax: 9776 7338
PO Box 133, Northcliffe

How to Get Yourself Blackmailed by Criminals: Try Computer Crystal Therapy.



This is a real page from a real book.

Need we say computer crystal therapy is bogus??

Russian 'Ransomware' hackers are laughing all the way to the bank at those using such methods.

What is Ransomware?

'Ransomware' is one of the nastiest computer attacks afoot. Over 20,000 Australian computers are currently affected by just a single ransomware virus called 'CryptoWall' and there are many other types of ransomware attacks active out there.

In some ways it is wrong to call this a 'computer attack' because it is humans who are initiating these attacks. The purpose of ransomware is to hold your computer data to ransom for the profit of criminals who could be living anywhere in the world. While it is generally supposed many of these cybercriminals live in Russia or Asia, they could also be your next door neighbour.

Ransom money is paid using 'Bitcoin' which is a practically untraceable form of online currency. Bitcoin has many legitimate uses but understandably, it gets some negative press for its use in criminal money transfers and tax evasion.

The NCRC recently had a customer who had her computer attacked by 'Ransomware'.

A ransomware attack involves being blackmailed, online, to pay money or otherwise lose all your precious computer data (photos, documents, accounts, scans, music etc).

Ransomware operates via a computer virus which scrambles your hard disk in such a way that only the blackmailing party can unscramble it for you.

It seems that most are being infected by opening email attachments. Even if you recognise the sender of an email, you should know what risks you are taking when you open their attachment. It is far better to play it safe!

In fact there are many different ways your computer could get such a virus, other than email. Even real computer pro's can fall victim.

In the majority of cases those subjected to such an attack will *never* be able to recover their own data. Even if you were to make the bad decision to pay your blackmailer, you have no guarantee that they will recover your data. With these sorts of transactions there are no refunds!

So, **before** you have this problem, make sure you have backups. Do it now, before it's too late. Also, make sure your backups are stored on a disk drives which you generally leave disconnected from your computer.

Even if your data is not precious, 'cleansing' your computer after an infection can't be done with a crystal and could cost you serious $ and time.

What Can I Do?

Back up your personal data on a USB drive. Repeat the process at least once per month.

You can buy a USB drive from the NCRC, at the Post Office or many other places.

NCRC don't recommend you download or install 'backup software'. It's unnecessary. Just copy your files across to your USB drive.

Once the copy has completed 'safely unplug' your USB drive and store it somewhere safe. Don't leave it plugged into the computer.

Help is half-price at the NCRC on Tuesday mornings at the NCRC.

NCRC is proudly supported by...
Government of Western Australia
Department of Regional Development
ROYALTIES FOR REGIONS
Northcliffe Community