

Here's a
surprise
you *don't*
need



Don't become a victim
of ransomware



www.getsafeonline.org



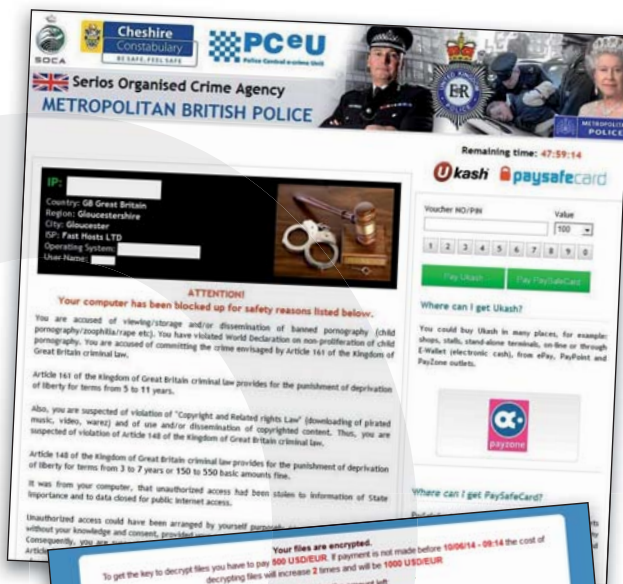
The internet is a wonderful resource for everyone, but unfortunately, it's also become a favourite place for fraudsters. Their sole aim is to steal your money or identity (or both), with no remorse for how much hardship, inconvenience or trauma they cause you.

A particularly nasty type of virus is used by cybercriminals to extort money from their victims. It's called ransomware, and it comes in several different varieties.

Ransomware locks your access to all your files on your computer or mobile device, and pops up a demand for payment to enable you to get back into them.

Sometimes the warning claims to be issued by the police and says that you've been carrying out inappropriate or illegal activity online. Usually it specifies payment in the virtual currency Bitcoin. Once your computer or device is infected it's too late ... it's a very complex process to unlock it, and sometimes it's impossible to do so. Documents, irreplaceable photos, contact lists, emails ... all become inaccessible. And in most cases, paying the ransom is pointless as your files won't be unlocked.

Having updated Internet security software or apps can help, but cybercriminals update their malware so often, that the software doesn't get a chance to catch up. The most common ways that your device gets infected are when you click on attachments in fraudulent emails, or visit infected websites, including adult content sites. It can also result from plugging in infected USB drives or peripherals.



Therefore, it's essential to guard against ransomware before it's too late.

Start by reading these tips:

- Do not reply to, or click on links contained in, unsolicited or spam emails you're not expecting. These may even pose as coming from friends, family or colleagues.
- Visit only websites you know to be reputable.
- Ensure you have effective and updated internet security software / apps and firewall (on a computer) running before you go online.
- Regularly back up all your data, including to a USB-connected device stored remotely from your computer. This is because some ransomware can also infect your cloud-based storage.

If your computer or mobile device gets locked by ransomware:

- To detect and remove ransomware and other malicious software that may be installed on your computer, run a full system scan with an appropriate, up-to-date, security solution.
- If your computer has been locked by ransomware, seek professional advice from a trustworthy source.



Another kind of ransom demand – although not associated with malware – is directed at businesses, who receive an email warning that unless they pay a ransom, their website will be overwhelmed by hits, effectively closing it down.



Visit www.getsafeonline.org, select *Protecting Yourself* and click on *Ransomware*

What to do if you think you've been a victim of Ransomware



Report it to Action Fraud, the UK's national fraud and cyber crime reporting centre by calling **0300 123 20 40** or by visiting www.actionfraud.police.uk

Action Fraud
National Fraud & Cyber Crime Reporting Centre
www.actionfraud.police.uk

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For all the expert advice you need on keeping safe online, visit www.getsafeonline.org



www.getsafeonline.org



OFFICIAL PARTNERS

