

Protect Your Tech

Scams and threats to avoid, plus new security tools

WATCH OUT FOR...

'You've been watching porn' scam

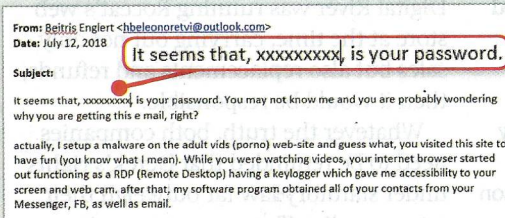
What's the threat?

Criminals are emailing victims their own passwords hoping to trick them into believing they've been filmed on their computer watching porn online.

The 'sextortion' email contains your computer password in the subject line and the opening sentence (see screenshot). It claims to have used this to gain access to your PC, then install malware that captures you doing "nasty things" while watching porn.

It also boasts about gathering "every one of your contacts from your Messenger, Facebook, and email", and threatens to send the video to them ("including relatives, coworkers, and so forth") unless you pay \$1,400 in Bitcoin within 24 hours, which it calls a "fair price for our little secret".

The scammer promises to erase the



video if you pay, adding "this is a non-negotiable offer, so don't waste my time and yours by replying to this email".

How can you stay safe?

You should immediately change the password included in the email. Some victims said the password mentioned in the email was for an old account they no longer use, and had never used on their current PC. Based on this, security experts think the attack draws on passwords and emails contained in a

database stolen in a data breach around 10 years ago.

Action Fraud searched for some of the victims' email addresses on 'Have I been pwned?' (<https://haveibeenpwned.com>), which lets people check whether their online

accounts have been hacked. It found almost all the accounts were at risk. It's feared that the attackers will start using more recent passwords to convince victims the threat is real.

Scams like these get the blood boiling, so you may be tempted to reply to the email, telling the attacker where to go. Instead, seek another way to express your anger. Responding to scams just lets criminals know the email address is active, making it more likely you'll be targeted in future.

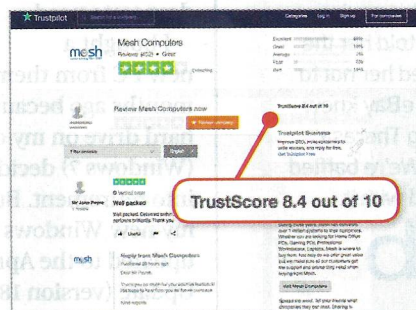
New tools

Trustpilot
<https://uk.trustpilot.com>

Here's something that won't surprise you - there are lots of rogue traders online. An effective way to avoid them is to search for companies on Trustpilot, one of the world's biggest consumer-review sites. This is much easier thanks to a recent redesign that places the search bar front and centre. Type a company name, click Search, and you'll see how many reviews it has, as well as the average rating.

For example, we're glad to see Mesh - makers of our current favourite PC (see page 30) - scores highly: 8.4 out of 10 (www.snipca.com/28555, see screenshot). Other UK manufacturers we recommend regularly, including Palicomp, Wired2Fire and Chillblast, are also popular with customers.

If you don't have a company in mind, it's better to browse the categories



(you'll find the PC firms mentioned above in 'Computer & Accessories'). There's also Craftsman, Electronics, Home & Garden and Legal Services, among others.

Some fake reviews are bound to slip through, but Trustpilot has a dedicated Compliance Team to remove them. If you suspect a review is false, report it via www.snipca.com/28556.



ScamWatch
READERS WARN READERS

Prime scam - a coincidence?

I mistakenly applied for Amazon Prime, but cancelled it within minutes. I was surprised therefore to receive an email a few days later saying my Prime account was being activated. It looked like an excellent copy of an Amazon email. Only when I was asked for my credit-card details did I close the site and as a precaution change my Amazon password. I cannot accept that this was sent coincidentally a few days after I'd signed up for and cancelled a Prime application. I've sent all details to Amazon's fraud department (www.snipca.com/28529).

Tom Sampson



Warn your fellow readers about scams at letters@computeractive.co.uk