

Virus phone scam being run from call centres in India

Britons targeted by cold callers pretending to be from Microsoft phoning to fix a fake computer problem

- [Charles Arthur](#)
- [guardian.co.uk](#), Sunday 18 July 2010 20.48 BST



Beware cold callers – especially those claiming your computer has a virus. Photograph: Corbis

The scam always starts the same way: the phone rings at someone's home, and the caller – usually with an Indian accent – asks for the householder, quoting their name and address before saying "I'm calling for [Microsoft](#). We've had a report from your internet service provider of serious virus problems from your computer."

Dire forecasts are made that if the problem is not solved, the computer will become unusable.

The puzzled owner is then directed to their computer, and asked to open a program called "Windows Event Viewer". Its contents are, to the average user, worrying: they look like a long list of errors, some labelled "critical". "Yes, that's it," says the caller. "Now let me guide you through the steps to fixing it."

The computer owner is directed to a website and told to download a program that hands over remote control of the computer, and the caller "installs" various "fixes" for the problem. And then it's time to pay a fee: £185 for a "subscription" to the "preventative service".

The only catch: there was never anything wrong with the computer, the caller is not working for Microsoft or the internet service provider, and the owner has given a complete stranger access to every piece of data on their machine.

An investigation by the Guardian has established that this scam, which has been going on quietly since 2008 but has abruptly grown in scale this year, is being run from [call centres](#)

based in Kolkata, by teams believed to have access to sales databases from computer and software companies.

Matt, a Londoner who has recently set up his own company, had just arrived home at 7pm when the phone rang and someone with an Indian accent asked for him by name, quoting his address. "It's Windows tech support here," said the caller. "We have reason to believe that there's a problem with your computer. There have been downloads of malware and spyware, and they're slowing down your computer."

He went along with the caller's demands to log into a website and enter a six-digit code into his computer. "I thought it was a new service from [Microsoft] Windows," he said. "I could see them moving the cursor about. It took about half an hour."

The caller could not have obtained Matt's name via HP or PC World, where he bought the machine, because he gave his business address, not his home address, during the purchase.

This suggests that the caller was using the phonebook to find names. Patrick McCarthy, who lives in Dublin, received a call from one of the companies – but they addressed him by the name of the apartment block where he lives instead of his own name, a longstanding error in the Irish phone book.

Often, the victims are inexperienced or elderly, convinced by the apparent authority of the callers and the worrying contents of the Event Viewer. In fact, such "errors" are not indicative of any problems.

Investigators who have spoken to the Guardian on condition of anonymity say that one man, based in the city of Kota in Rajasthan, is behind the centres running the [scams](#).

He has provided fake documentation to a number of payment companies including PayPal and Alertpay, a Montreal-based online payment company, to set up accounts which route money to a bank account in Kota with Axis Bank.

Though people on dozens of web forums have recorded their experiences with the scammers, police and trading standards officers in the UK are powerless to stop them.

UK telephone numbers for contacting the company on the sites are not "geographical" - tied to a location - but instead allocated to voice-over-internet providers.

That means that the calls connect internationally, but cost the scammers almost nothing when anyone calls them.

In the same way, it costs them virtually nothing to make the calls because the international part of the call goes via the internet.

If the payment has been made on a debit card - as many are - there is no hope of reversing the payment. A number of payment organisations used by the scammers have shut down their accounts. PayPal, the eBay-owned credit transfer company, and AlertPay have both taken rapid action against scam sites which used them.

In March, site hosting company Hostgator shut down one of the longest-running sites used for the alleged scam, F1Compstepuk.com, after complaints.

After confirming with Microsoft that the site was not acting for it, Hostgator immediately shut it down. Josh Loe, Hostgator's co-founder, said that following the initial complaint, "we

asked for more information regarding this to confirm. We received a message from a Microsoft representative via this particular person who contacted us first about this. At that time it was enough evidence to close the site and it was done so the same day."

But one investigator who has been tracking the growth of the scam says the challenge is that new sites offering the same fake "service" keep popping up "like mushrooms".

At first the scammers tried desperately to maintain the reputation of their sites, by flooding any forum which garnered enough criticism of their activities with postings claiming that the site helped fix their machine.

But the poor spelling and grammar of the replies – allied to internet addresses which show that the commenters are based in [India](#) – contrasted sharply with that of people in the UK, US and Australia complaining about the attempted scam.

Now they have shifted to creating multiple sites from templates, using stock phrases and photos. However, investigators are sure that the same man - and central operation - is behind all of the schemes. "I don't think that this could really have spread that far. Even if they can see that some of their friends are making money from this, the calls are too similar every time," said one. "It's got to be the same organisation each time."

Microsoft denies any connection with the companies that call people up offering these services.

When contacted about the scams, Microsoft said it was "currently investigating a series of instances in which the business practices of an organisation within the Microsoft Partner Network [that] have given rise to significant concerns from a number of sources. We take matters such as these extremely seriously and will take any action that is appropriate once our investigation is complete."

Three weeks after being contacted by the Guardian, it issued another statement: "We confirm that we have taken action to terminate our relationship with certain partners who are clearly misrepresenting their relationship with us and using our company name in order to facilitate their telephone scam operations."

However, this week, two sites alleged to be involved were still listed as "Microsoft Gold Certified Partners", which Microsoft says means that they must have "demonstrated expertise" and "must employ a minimum number of Microsoft Certified Professionals".

The company has noticed the problem. "Microsoft does not make unsolicited phone calls to help you fix your computer," it [says on its website](#).

"If you receive an unsolicited call from someone claiming to be from Microsoft Tech Support, hang up. We do not make these kinds of calls."

- guardian.co.uk © Guardian News and Media Limited 2011