《CCTV9英语新闻：互联网心脏出血震惊IT业》

CCTV9英语新闻：互联网心脏出血震惊IT业

??,?????“?????????????,??????????????????4?8??????XP?????????

Recently, a cyber security bug dubbed "Heartbleed" was exposed and shocked the whole Internet industry. It happened on April 8th, the same day Microsoft stopped its Windows XP service. Experts warn the bug could put the privacy of billions of Internet users at risk.

It's a bug on the OpenSSL, a crucial channel to transmit virtually all your private information, including you emails and credit card numbers.

Experts call it "Heartbleed". They say it's hitting the IT industry just like an earthquake.

Leading Internet companies in China have taken steps to thwart it. But not all were quick to react.

"Big companies value security very much and they were quick to react. But some may think it's not much of a big issue, so it could take some time before they fix it," said Dong Fang, an Internet expert.

Some industry insiders suggest users should change passwords in case they were already hacked. But does it really work in this case?

"You can change your passwords only when you are sure that the website doesn't have a loophole. Because if it does, and you change your password, it could still be leaked," Dong said.

For users, changing passwords seems the only thing they could do, provided that the website has already fixed the bug. But how can we know that? CCTV took a look at a number of big and small sites, and found none of them provide such information.

"We don't have this. Because we fixed it when we spotted it. There was no damage from the bug," said Jiang Yi at Paoku.com.cn.

"I haven't thought about it yet. We couldn't sort out this issue ourselves, let alone users," said Li Jifeng at Aiduanzi.cn.

JD.com, one of China's three leading business-to-customer retailers, said it had fixed the problem and no theft of credit card numbers had been reported so far. But on its official website, we too failed to find any risk alert.

"We will fix it as soon as we spot it. There's nothing we can warn the public about as of now. JD.com should have no problem with its website," said a publicity staff at JD.com.

So far, except some sleepless nights for internet programers, no damage seems to have been done.

But it doesn't undermine the urgency of the issue. Experts say, some hackers may be already on the move, and a surge in such attacks could happen any time soon.