

Internet Explorer bug lets hacker control your PC

Microsoft is racing to address a weakness in its popular Web browser that security experts found. The researchers have discovered that hackers have exploited the bug and created a new type of attack. If you're using Internet Explorer and click on the wrong link a hacker could hijack your computer.

This is how it works: Hackers set up a website that installs malware when you visit it. If you're duped into visiting the website while using the Internet Explorer program, malware seeps into your computer and gives a stranger total control and you might not even notice.

That's where the real danger lies. Anyone in control of your computer can spy on everything you do. If it's a PC at work, hackers can reach into anything an employee has access to. It's worse for those using Windows XP, because Microsoft no longer supports that operating system with security patches. To them, Microsoft says: Go upgrade to Windows 7 or 8.1. The U.S. Department of Homeland Security recommends that people ditch Internet Explorer until there's a patch or install special software in the meantime instead. This bug is more omnipresent than it seems. Lots of machines use Windows - - bank ATMs, point of sale systems, restaurant seating tools - and Internet Explorer is their default browser. If hackers manage to send them to a bad website, that machine is now under their control. It won't be easy, but it's possible. This type of attack is particularly nasty, because it affects every version of the Web from IE6 through IE11. That's more than half of the browsers in use right now. This hack is described as a "zero-day." That means that the attack is a unique, never before seen technique - a particularly dangerous vulnerability, since it hasn't yet been patched. The easiest solution is to just ditch Internet Explorer and use another browser like Google Chrome, Mozilla FireFox or Apple Safari because this attack doesn't affect those Web browsers.