Change website passwords 'at least every two months'

By Dan Hyde
Consumer Affairs Editor

ONLINE passwords for banking and shopping should be changed "at least every two months" after figures showed the amount of personal data traded by criminals had trebled in two years.

Criminals gathered more information by using fake internet "hot spots" and carefully disguised email and website scams, fraud experts said.

Victims were also guilty of using flimsy passwords or opening attachments and clicking links in emails from strangers, they warned. Peter Wood, of the security consultancy First Base Technologies, said: "The massive increase in illegal trade of personal information on the internet is a result of two factors: the average person doesn't understand how to protect against attacks and criminals are trading hacking skills and techniques in greater and greater numbers."

More than 110 million pieces of data have been traded by criminals this year, according to the information firm Experian. It said this was a 300 per cent rise on the same period in 2012.

Peter Turner, a director at Experian, described the numbers as "startling". He said illegally traded data mostly consisted of login credentials, with username and password combinations accounting for 97 per cent of the sales.

This gave identity fraudsters access to where someone banked or shopped, linked accounts which had passwords saved automatically and any personal information shared over email.

An experiment in London by the Cyber Security Research Institute last month found that in just half an hour hundreds of people logged into a pirate internet hotspot through which criminals could have collected personal data. The hotspot had been disguised as a "free" wifi connection. This was an example of new, sophisticated threats, Experian said.

People should change passwords "at least every two months", Mr Turner said, and use a series of letters and numbers.

Mr Wood warned that email scams had grown into "well-designed cons".

"Most attacks are automated and extremely clever," he said. "Your best protection is to run regularly updated antivirus software, use a personal firewall programme and ensure every programme is up to date."