Phishing – a real threat and nothing to do with fish.

By Jamie Grant IT Guru Solutions

Phishing is a scam where criminals try to trick people into giving out private information such as passwords, credit card numbers, social security details and internet banking login details.
The most common tactic used by phishers is to send an email to an individual fraudulently claiming to be from an organisation with which they have a relationship. The person is then asked to click on a link which directs them to a cloned web site that looks exactly like the real organisations and enter the username and password. This is then used to log in and set up direct debits or transfer money.
This has happened to one of my clients. A secretary was looking after the managing directors e-mail while he was on holiday and one of these e-mails came through so she entered the bank details. Within 24 hours a direct debit was set up and £4000 had been removed from the account. They did get it back because it was noticed in the same day. If they hadn't it could have mounted to a great deal of money.
A friend of mine also was effected, not by e-mail but by an innocent looking pop up. He travels a great deal but was a few points off a silver card with British Airways so he booked online for a flight to Paris for an afternoon. After entering his credit card details he got a request to enter his details on the Barclays web site to cut down fraudulent use of credit cards. While he was entering the details a pop-up came up and asked him to confirm the details. This was the problem page and soon after he was getting fraudulent credit card use mainly small amounts of money. This case is on going.
Out of interest he uses an Apple MAC. If he used a PC with an up to date internet explorer then I don't think the pop up would have come up. I also know that all web browsers have similar problems. Firefox has recently issues 15 security warnings for its browser.
There are millions of online transactions that happen every day which people have no problems with, however this type of crime is increasing. There were 16,882 attacks in November of last year.
Common sense should be used and if in doubt don't do it. If they require you to do something they will write to you. Banks and building scocieties will never send you an email with links to their own sites or ask you to confirm security details.

For further information look at http://www.getsafeonline.org/

"Get Safe Online will help you protect yourself against internet threats. The site is sponsored by government and leading businesses working together to provide a free, public service."