

Click here to shield against fraud



FULL FLOOD DATA INCLUDED IN ALL FCI REPORTS!



Signup to our free newsletter

featuring latest articles, partner news & guest blogs

Signup now



Lost £50,000 in property case restates importance to safeguard against email hacking

Chris Langford, 1st July 2015

'Phishing' is a modern day fraud technique which refers to when criminals attempt to acquire sensitive information, such as bank account details. This is done by masquerading as a trustworthy person in an electronic communication.



Vivian Gabb was a recent victim of this particular crime during her property transaction. Her email account had been hacked and every incoming and outgoing message was being monitored. Consequently, the criminals were fully aware, and took full advantage of, the fact she had instructed solicitors to complete her conveyancing transaction. The solicitors were awaiting a £50,000 deposit payment from Mrs Gabb - another facet of information the criminals had gained from her emails.



The fraudsters sent her communications, disguised a follow up email from her solicitors, asking for the £50,000 to be transferred into their account. They claimed the firm had changed their account details.



The email was branded according to her solicitors (Barnes & Partners) style and was sent from a similar looking email domain. It appeared to be identical to their previous correspondence. By the time they discovered the money had gone to a scam artist's account rather than the solicitors, the money had already left the bank account and couldn't be recovered.



Although police are currently investigating the events, Mrs Gabb appears to be in a position to lose her deposit as neither her own bank (Halifax) nor the bank the criminals used (TSB) have offered to refund the money. TSB, despite opening up an account for criminal purposes, have specified they can't release any details of who set up the fraudulent account due to the Data Protection Act 1998.



The internet safety advice website Get Safe Online states that more than half of people in the UK have been a victim of an online crime, and 15% of people have been victims of either attempted or successful hacks of their email account.

Mrs Gabb states Barnes & Partners have told her they aren't responsible as the fraud didn't originate from any issues with their computer security. Notwithstanding, this is not good publicity for the firm and measures should be taken by all solicitors firms to try and protect clients who may not be aware of the growing risk of 'phishing'. Such measures can include:

- Clients should be made aware of the risk, particularly those about to purchase property as they are most at risk due to the size of finances involved
- Clients should be encouraged to confirm account details over the phone or in person before sending large sums of money
- Account details should not be passed over email, particularly unencrypted emails
- Provide clients with their own account on a password protected portal, ensuring all messages and documents remains on the same secure server as opposed to the use of emails
- Ensure all staff are made aware of the risk and comprehensively trained in the appropriate safeguards

Comments

