

Protect your tech

Scams and threats to avoid, plus new security tools

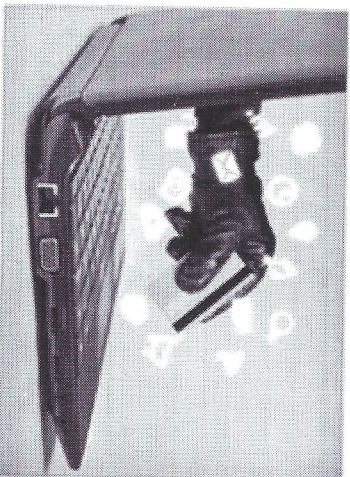
WATCH OUT FOR...

'Ghosting' emails that steal your cash

What's the threat?

Scammers are hacking the email accounts of bank employees so they can impersonate them during financial transactions, tricking customers into sending them money. In these 'ghosting' scams, they intercept email discussions at a crucial point, telling the victim to send their money to a "revised" account.

An Ayrshire farmer, who has remained anonymous, recently lost thousands of pounds. Halfway through negotiating a loan with his bank to buy machinery from a dealer, he received an email supposedly from the bank asking him to send the money to a different account to the one previously given. This email seemed genuine because it came from the address of a bank employee, and contained the correct contact details, plus the usual warnings about fraud.



Soon after, the dealer phoned the farmer to chase the money. Thinking he had already sent it, the farmer contacted his bank, which told him it hadn't processed the payment because he'd stopped replying to their emails. It's unlikely he'll get the money back. Keen to warn others, the farmer contacted the press, saying: "Having

reviewed the emails, the only indication that an intruder had taken over the email conversation with the bank was a very slight change in writing style - something that we simply assumed was a banker typing in a hurry!"

How can you stay safe?

If you're in the middle of a financial transaction, such as remortgaging your home or releasing pension funds, be on high alert for emails asking you to send money to a new account. Phone your bank straight away to check they're authentic.

Security firm Barracuda says it has seen a "significant rise" in the number of phishing emails sent from the hacked accounts of UK organisations - not just banks, but also universities, retailers and IT companies. See some examples on the company's blog: www.barracuda.com/20199.