

## **Invoicing & Internet Scams**

### **Invoicing Scam offering 'Free' High Street Vouchers**

A new invoicing scam could lead to firms paying for goods they neither ordered nor need. The scam involves an introductory a telephone call from a London-based firm offering businesses 'free' high street vouchers and a sample of a new cleaning product. Following the call an invoice is sent with the delivered goods, which can include a staff member's name stated on the order. Businesses often make payment without realising the delivery is not legitimate.

Ensure that your order and payment systems are robust enough to spot dirty tricks and antics of this nature. Invoices sometimes slip through the net and businesses pay because they just want to put it down to experience. It's vital staff are briefed about this scam and don't give in and pay. This is the worst kind of scam because it actually questions the integrity of trusted staff who just happen to answer the phone to the deceiving caller.

Unless there is a robust system in place, orders are often accepted as legitimate deliveries with businesses stuck with goods they do not want. The scammer then says that they have taken delivery and should pay, often threatening legal action when the goods in question are overpriced and of questionable quality.

### **European 'Urgent' Invoicing Scam**

On top of this the Advertising Standards Authority have warned businesses to be aware of new scams filtering through from Europe. Several rogue firms in Switzerland, Austria and the Czech Republic have been taking advantage of managers' summer holidays and contacting businesses with 'urgent' invoices that junior employees often mistakenly pay. By doing so, they sign the business up to a contract that binds them to years of payment.

### **Internet 'Scob' Virus**

At the end of June Internet security firms have issued urgent warnings to users of Microsoft's Internet Explorer of a new security flaw, which was highlighted following the outbreak of the 'Scob' virus. Scob remotely installs malicious code, which is then downloaded by anyone using Internet Explorer to visit a series of websites running Microsoft's Internet Information Server. Although the infected sites have been cleaned up, the flaw remains vulnerable to exploitation until it is fixed. Microsoft is currently working on a patch, but in the meantime users are recommended to try a different web browser.

Read Microsoft's advice on this issue by clicking on the following link and remember to upload the patch as soon as Microsoft publishes: [http://www.microsoft.com/security/incident/download\\_ject.msp](http://www.microsoft.com/security/incident/download_ject.msp)

More advice from Microsoft on adjusting your browser settings to maximise security is online here: <http://www.microsoft.com/security/incident/settings.msp>

### **Beware Spyware**

Spyware is the topic of the moment, with businesses becoming more aware of the danger that malicious software poses to their systems' performance and security. However, there are a number of misconceptions about spyware that could lead to potentially dangerous errors, including confusing it with adware and how to combat it most effectively.

A useful guide at the following link should clear up some confusion:

<http://www.sitepronews.com/archives/2004/jun/23.html>

A web resource dealing with spyware, also including guidance on identity theft, can be accessed at:

<http://www.spywareguide.com>