



Too good to be true

There are enough web users who click on web links or respond to emails promising something for nothing to make it worth the scammers' efforts to keep sending them. Wendy Brewer looks at some common online hoaxes and sounds a cautionary note

The internet is a fantastic marketing medium and offers a virtual shop front to businesses of every type and size. But it's also open to abuse, most notably in the form of unsolicited mail and viral marketing for products of dubious provenance and of unverifiable efficacy. While their exact form and what they are pushing varies, the approach is often all too familiar.

Nigerian nuisance

Despite its reputation as the most prevalent email scam in history, every year thousands of people are still duped into falling for the promise of quick riches offered by so-called Nigerian spam mail.

The emails, known in Nigeria as the 419 scam after the country's penal code for that crime, usually tell the

story of a government official or wealthy businessman who has squirrelled away money and needs help to get it out of the country.

The recipient is promised a share of the stash - usually between 10 and 30 percent - for their help. The sender asks the recipient for their bank details in order to transfer the money, and in some cases will request additional funds to cover transfer costs and legal fees.

The scale of the scam is impossible to calculate. In the UK, thousands of emails are reported every year, but this represents only a tiny percentage of the total number sent. Recognising the continuing problem, the Nigerian High Commission in the UK has set up a website (www.nigerianfraudwatch.org) where people can register the receipt of these messages. If you receive a Nigerian email, report it then delete it.

Windows assault

In 2003, spammers found a new security vulnerability in Microsoft's Windows Messenger service, the pop-up network administration tool which notifies users when printing. Unlike with traditional email, spam messages appear on the desktop without the need for user interaction, making them impossible to stop unless the service is disabled.

One of the most publicised assaults of 2003 concerned auction site eBay's online payment service, PayPal. Spammers sent out mass messages warning users their accounts were due to expire. The message contained a link for customers to click on to update records such as credit card numbers. "We would never ask customers to reveal such personal details in such an impersonal way," said eBay's spokesman.

This stance was echoed by other targeted companies, which advised customers to ignore the messages. After a flood of complaints from users, Microsoft has made the decision to turn off the Messenger service by default in its second XP service pack due out later this year.

Until then, you can switch off WMS in XP by going to Start, Control Panel and double-clicking on Administrative Tools. Double-click Services, scroll down and select Messenger. In the Startup Type dialog choose Disable and, under Service Status click Stop then hit ok.

Credit card fraud

Credit card fraud is as much of a problem for online shoppers as those on the high street. Scammers use all sorts of underhand measures to encourage people to reveal card details from sending fraudulent emails to creating bogus websites offering goods that don't exist.

Fortunately, all credit card users are insured against fraud and will be reimbursed by their credit card company for anything over £100. However, debit cards offer no such guarantee. "If something looks too good to be true, doesn't feel right or seems suspicious then avoid it," said a spokesman at the Consumers Association.

Promises, promises

We've all been inundated with emails and pop-up adverts offering us the opportunity to earn truck loads of money working from home or to purchase an honours degree at the touch of a button. Hundreds of trusting consumers are still falling for such scams, which include all-too-common bogus product offers.

One *PC Advisor* reader was duped into purchasing Norton AntiVirus software after receiving a too-good-to-be-true offer. Unfortunately, after the software failed to arrive he contacted Symantec which had no record of his purchase. As it turned out, the company that had made the offer never actually existed.

As a goodwill gesture in this instance, Symantec sent our reader a copy of the software free of charge. But he was one of the lucky ones.

When purchasing any product or service, regardless of the great deal you think you're getting, it's essential to do a little background research. Look at the company's

history or contact the product manufacturer for verification that the offer is genuine and that you're buying from a reputable reseller.

Pyramid selling

Nothing to do with flogging the tombs of the Ancient Egyptians, this common swindle ropes in people to sell goods or services to their friends and family on the promise of high commissions. Pyramid selling is illegal in the UK but that doesn't stop it happening, especially online where retailers target users through emails.

The products sold are usually overpriced and of poor quality. Manufacturers use the relationship of trust between the seller and buyer to shift products and services that would otherwise be impossible to sell.

The next person in the chain is promised cash back if they can then sell the goods on or sign up another friend to the service. And so it goes on down the pyramid. It is unlikely that people will make much, if indeed any, money, and sellers may face a barrage of angry relatives who agreed to buy the product on the seller's say-so.

Pyramid selling has its roots in multilevel marketing, another style of chain selling which isn't illegal. The key difference is that multilevel marketing involves quality goods being sold to end users, rather than friends and family, and at reasonable cost instead of inflated prices.

Staying safe

The internet's anonymity and speed allows conmen to send emails out at unprecedented rates, focusing on specific countries, areas or topics at one time. As consumers, we need to be aware of what's out there and how to avoid it.

Our advice is buy goods only from reputable vendors and don't take up any offer without checking its validity first, particularly if it's the best deal you've ever seen. ☒

What's your password?

Hackers use myriad innovative ways to worm passwords out of online users. In many instances people are quick to reveal them if promised a reward. A survey conducted by IT assurance firm NCC across 150 IT experts showed just how willing people are to divulge their passwords. Almost all of those questioned gave out their network access codes at the end of a survey about computer security.

NCC estimates around half of passwords can be accessed in less than three minutes, with many people opting for obvious choices such as family names, book titles or dates of birth. Fraudsters have also sent out emails urging people to update their passwords or confirm them by clicking a bogus URL.

It sounds pretty obvious but as a rule of thumb, passwords should only be given out to those who need to know them, they should be changed regularly and users should choose different passwords for each application to make life harder for hackers.

The borrowers

Under the HCI scheme, employers can charge staff for home-loan of the firm's IT equipment, while securing themselves a tax break into the bargain. Now IT companies are helping make it an even more tempting proposition, says Wendy Brewer

Recognising that a happy workforce is a productive workforce, the Department of Trade and Industry has published a new set of guidelines for employers on home computing initiatives (HCI), reminding them of an existing £500 tax exemption on loaned computers.

The tax break was originally introduced by the 1999 Finance Act, but a lack of interest in the scheme encouraged chip-maker Intel to establish the HCI Alliance back in 2003. The group, which now boasts BT and Microsoft among its members, has pledged funds and resources to help the government promote the scheme.

HCI explained

Under HCI, employers are entitled to loan out equipment for a set period - agreed between themselves and staff members - to a value, per employee, of £2,500 if the kit is owned by the company, or £500 per year if it has been hired. These costs are completely free from tax and National Insurance payments.

Two key providers in the HCI scheme are Evesham and Mesh, who offer packages from around £4 per week, deducting the money monthly from the employee's bank account.

All IT equipment can be loaned under the scheme, including PCs, laptops, printers, fax machines and scanners. The idea is to improve employees' working lives by giving them access to up-to-date equipment in and out of the office, and at the same time providing them with help and advice on-tap.

There are two ways to approach HCI: with company-owned PCs or with leased PCs. With the former, the initial expenditure should qualify for capital allowances at 25 percent of the reducing balance rate. Leasing



costs will generally be deductible as an expense in computing from the business profits.

Loan period

There is no defined period of time across which the scheme must run and employers do not need to notify the Inland Revenue when the scheme is in place, but certain rules must be followed in order to qualify for the tax exemption.

First, the salary sacrifice scheme, through which employers recoup their costs, must be defined from the outset. If the employee has the ability to return the equipment at any time and revert back to their original salary, then the IR may deem the scheme ineffective.

The HCI period must also be agreed in writing before a loan starts.

Mine, all mine

At the end of the agreed period, the employee may purchase the machine at the discretion of the employer or simply return it to the company. If it is purchased, then the employee must pay the market rate to avoid incurring benefit-in-kind tax charges. ☒

What's on offer

Hardsoft.co.uk

For a monthly fee of £27.45, Hardsoft.co.uk will loan a Compaq P4 2.66GHz PC with 80GB hard disk, 18in LCD, 56K modem, Windows XP Professional and Epson Stylus Photo C84 colour inkjet printer. This works out to £329.40 per year - well below the £500 limit.

The cost of the scheme is deducted from the employee's gross wages in a practice known as 'salary sacrifice'. Deductions must not cause gross salaries to fall below minimum wage.

Evesham

A basic package from Evesham provides an Intel Celeron 2.6GHz Evolution C2600 PC with 15in TFT monitor and three-year onsite warranty for £3.69 per week. Again, this is paid direct from the employee's bank account.

All PCs, providing they are kept at one registered address, are supplied with lifetime access to customer service helplines.

Mesh

Mesh offers an Elite M800, 3GHz Pentium 4 PC with 512MB DDR RAM and Windows XP preinstalled for £703 inc VAT - £70 off the normal price.

There's a three-year warranty and access to free customer service for the lifetime of the machine. For an employee, this equates to a direct debit of £19.52 per month for 36 months. Mesh also offers a range of services for larger organisations.