

John Hookham looks at the current crop of cons, frauds and tricks floating around the web.

# Phishing, pharming and other scams

THROUGHOUT HISTORY, confidence tricksters and their scams have always existed. In the age of the internet the old classics are alive and well and new ones have been invented. And despite warnings that con men and fraudsters out there are after your money, millions of normal computer users and many businesses still fall victim to cyber crimes.

Some scams are easy to avoid and some are fairly obvious, but others are more subtle, some are downright fiendish and a few are quite simply despicable – preying on the most vulnerable and often desperate members of society.

## Phishing

Approximately 40% of all emails that circulate the globe can be classified as junk. They include adverts for fake watches, body enhancements, dating agencies and the like, but increasingly they include fake emails from what appear on the surface to be well-known financial institutions – the bank security update.

These include UK companies such as the Halifax building society or Llyods [sic] but, given the nature of the internet, most of the emails impersonate American banks.

The story is fairly consistent – there has been a software security update at the bank and it is mandatory for you to log on and update your details.

This will include your account number and password, date of birth, mother's maiden name, etc – after all, your security is their prime concern and they need to ensure their (the criminals') records are correct.

No financial institution, bank or building society anywhere in the world will ever ask you to enter or update personal and/or account details via an email request.

These bogus emails may use the bank's logo and if you log on to the website it will look identical to the bank's website, but behind the scenes you will be supplying information to [www.takeallofyourmoney.com](http://www.takeallofyourmoney.com).

## Key logging

This bank security update scam will be seen by most people for what it is – a fairly crude attempt to get you to type your details into a bogus website. The savvy computer user is not going to be conned by this sledgehammer approach, but

they may well be tempted to open up the email and 'have a look at it' anyway.

This action can allow a key-logging program to be installed on your PC and is the next level of sophistication used to obtain your personal details.

The small piece of malicious software waits patiently until you visit your online bank and then the software simply sends your details back to the [Takeallofyourmoney](http://Takeallofyourmoney) website.

It works by keeping a log of all the keystrokes that you have entered, including account numbers, passwords, etc. This is a subtle and devious method of stealing data, as the user will be unaware that anything untoward is happening – until, that is, money disappears from their account.

To protect yourself or employees, you need to install anti-virus software and keep it up-to-date and install either a corporate or personal firewall.

## Pharming

Adept con men can also mix-and-match scams and techniques – and pharming is one method they use.

The first technique again involves secretly installing software on a user's PC. The program patiently waits for you to log on to one of a number of popular and well-known retail sites and then technique number two takes over and sends you to a 'doppelganger'



**John Hookham: protect yourself at all times**

site – it looks like the retail site, acts like the retail site but is a fake, set up to collect your credit card details.

Other undesirable programs that can sit unnoticed on your PC include ‘spyware’ – software that is primed to collect personal details; or ‘dialler’ software that is designed to connect you to premium cost phone lines.

Installing ‘spyware’ detection programs will help you to remove these types of malicious and not so malicious programs from your PC.

### A friend in need

In the 80s, company officials often received letters from bogus lawyers who needed to use British companies to help them extradite monies from deceased clients – normally ex-Nigerian or other African country government ministers.

The money was deposited in a secret account and you could not tell anyone about this opportunity – there are lots of dishonest people out there who would try and steal the money.

In return for some of your official company headed paper and the use of a bank account, you or your company would retain 10% of the fund value, which was always around \$5 million, netting you half a million dollars.

Today these snail-mail letters have been replaced by email, but the story remains more or less the same; deceased client or father, money with a security company, all taxes have been paid, it’s not illegal, \$5 million in the account, for your help you will receive the normal 10%...

Without wishing to be offensive – why do you deserve this great honour? If someone approached you in the street with an offer like this, you would run a mile, so do the same in cyberspace.

### Beauty contest

In the game of *Monopoly*, the Chance cards let you win a beauty competition, but on the

internet it’s a substantial sum of money in a lottery or prize draw.

In the real world there is an extremely small chance of you actually winning either a beauty competition or the lottery. But the high-priority email will say you will have won over £100,000 on a foreign lottery, normally from either Canada or Australia or maybe even Spain (it’s never from Zimbabwe or Nigeria – see ‘A friend in need’ above).

The lottery’s official authorised agent will of course help you to get your win processed. In return you will just need to cover the fees and taxes that have to be paid in order for the money to be released.

If you do succumb, and pay the first small upfront fee (what’s £1,000 when you will collect £100,000?) there will be some other problem that requires a further payment. This process will continue until you stop paying.

The prize draw is a more recent phenomenon and is usually fronted by a multinational company – not the real company of course, but one pretending to be the household name.

Your email address will have been selected from millions on the internet as part of a four-part selection process. This massive company’s promotional event means that you will not only win money but in addition you will receive one of the company’s flagship products – typically a top-of-the-range car.

Your winning voucher will need to be registered with your appointed agent, but there has been some computer mix-up so you mustn’t tell anyone about your good fortune, as they may try and steal your winnings.

Naturally your appointed agent only has a mobile phone number and as the promotion is international, there will be some fees to be paid so that your winning voucher can be processed: make your cheque payable to...

### Start-ups

For many companies, it is now common practice to advertise jobs on their websites and for job applications and CVs to be accepted via the internet. This includes government agencies, companies in the FTSE 100 and many well-respected international giants such as IBM.

The job and recruitment agencies have not been slow in getting individuals to enter their CVs online and embracing this new technology – and neither have the con men.

A basic assumption made by the con artists is that most people at some time will have registered their details with an online recruitment company. So typically the email will start by saying: “Having received your details from a recruitment agency (unspecified), you are

**People do not realise that the company email is a fake**

going to be offered a chance to obtain the job you have always wanted – an opportunity to join ‘the business’.”

This is, according to the email, a real job that will give you financial independence. The sender, who will also be your mentor, joined ‘the business’ and now works two or three hours a day, has had four foreign holidays in the last year and this week has taken delivery of the latest BMW or TVR. He or she even makes money while they sleep, such is the power of ‘the business’.

You will be directed for more information to the accompanying website [www.givememoney.com](http://www.givememoney.com). The website will have pictures of tropical beaches, yachts, houses and happy smiling people. This

is, you are told, a legitimate and ethical business opportunity, giving you the chance to have the fantastic lifestyle that most people can only dream about...just send some money.

If you don’t bite immediately and send off your joining fee, follow-up emails will try to entice you – “I’m just about to go for holiday number five, that’s the freedom that ‘the business’ can give you, John – join now, before it’s too late”.

### Spear-phishing

So who do you trust? Your boss? Somewhat surprisingly, it is often easy to get a list of email addresses from a company, including the director of IT and the head of finance.

So-called ‘spear phishing’ attacks use these email addresses to create fake internal company emails to ask employees for confidential or personal information.

The email will look as if it is from within the company, the name is correct; all you need to do is to reply confirming your bank details for the next salary run or supply the updated sales prospect list.

But the information will not go to your boss, it will go to the hacker. This approach – spear-phishing – is used to target individuals when their defences are down and they do not realise the internal company email request is a fake.

In conclusion, at the start of a boxing match the referee tells the combatants to ‘protect yourself at all times’.

This advice equally applies to your PCs, dealings over the web and with email. We know tricksters, con men and criminals exist in the physical world, but they are even more prevalent in the virtual world that is the internet.

● *John Hookham is a director of management consulting and marketing services company Adrelia Ltd. Tel: 020 7286 7073. Email: [john.hookham@adrelia.com](mailto:john.hookham@adrelia.com). Website: [www.adrelia.com](http://www.adrelia.com).*