

## AVOID THE SCAMS!

Most people believe they won't get taken in by scams - nothing could be further from the truth.

If you have a credit card, mobile phone, access to the internet, even a library card then potentially the sneaky scammer has all the tools needed.

Every day otherwise honest, intelligent, bright people fall victim to unscrupulous, deceitful scammers who'll stop at nothing and the unsuspecting victims don't know a thing - until it's too late.

We hope this issue stops you from falling victim to the scammers.

Kind regards

*The Cerberus Team*

*featured in this issue...*

1. introduction  
*featured above*
2. gone 'phishing'  
*featured opposite*
3. new face! new FREE service  
*featured far right*
4. avoid 'phishing' scams  
*featured right*
5. top 10 scams  
*overleaf*
6. cash machine fraud -  
*how it works*  
*overleaf*

## GONE 'PHISHING'

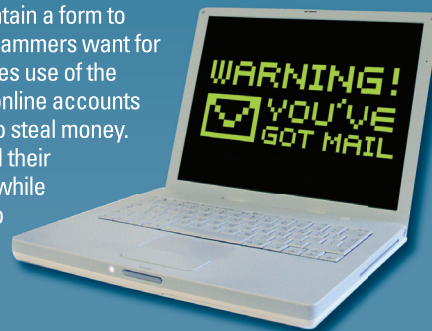
'Phishing', otherwise known as 'identity theft' is when a scammer assumes the identity of a legitimate organisation or web site, via forged e-mails or web pages, with a view to convincing consumers to share their user names, passwords and personal financial information for their own fraudulent use.

Many internet sites have fallen foul of 'Phishing' scams. Some refer to these forgeries as spoof e-mails, perhaps a more consumer friendly term. These spoof e-mails are distributed just like spam to e-mail addresses on the scammers hit list, whether they are a user of that particular site or not. Sites hit by these scams have included:

Yahoo - Microsoft - AOL - eBay - Paypal - Hotmail - Earthlink - Barclays iBank - Citibank - Halifax - NatWest Bank - Nationwide - MSN - Lloyds TSB

Most scams comprise a forged e-mail which urges you to complete an 'essential' procedure and links to a forged web page or site. That 'essential' procedure has included account verification, invalid credit/ debit details, attempted hacking of your account, prize draws and account suspension, to name but a few.

The forged web pages usually contain a form to provide the information that the scammers want for fraudulent use. This usually includes use of the victim's credit/debit card to open online accounts and hijacking of online accounts to steal money. For instance, eBay users have had their accounts hijacked in this manner while the scammers use the accounts to list high value items, receive payments from hopeful buyers but never send the goods.



## 'PHISHING' SCAMS

*don't fall hook line and sinker*

- Regularly log into your online accounts - don't leave it as long as a month before you check each account.
- Scrutinise your bank, credit and debit card statements. Ensure all transactions are legitimate. If suspicious, contact your bank and all card issuers.
- If you must use your financial information online, ensure that you have adequate insurance against fraud.
- Treat all e-mails with suspicion. What you see can be forged, the sender's address or return address can be forged and the e-mail header can also be manipulated to disguise its true origin.
- Never use a link in an e-mail to get to any web page. If you must type the URL directly into your browser's address bar.
- Never send personal or financial information to any one via e-mail.

### A new face! New FREE service!

Neil Walmsley has joined the Cerberus team having recently retired from West Yorkshire Police. With a 30-year career in the force, Neil has gained a wealth of experience with the last 10 years spent in Crime Reduction.

Neil's arrival means the introduction of a new service that will benefit all Cerberus customers.

Each and every customer will receive a visit from Neil at a pre-arranged time. He will assess the risks at your premises and produce a Crime Reduction report, which will be sent to you completely free of charge.



This service is as much for our benefit as yours. As your security provider, we are committed to giving you the best possible support and the aim of this service is to minimise the risk of criminal behaviour and allow us to highlight any weak spots within your premises.

**Neil will be in touch shortly, if he hasn't already, to arrange a suitable time to come and see you. Let us know what you think!**

# top 10 scams

Wise up to the scammers' schemes. Here's some to watch out for.

## 10. PYRAMID SCHEMES

These offer a return on financial investment based on increasing the number of new recruits. Investors are misled about the likely returns and there are never enough people to support the scheme indefinitely.

## 9. NIGERIAN ADVANCE FEE FRAUD

This involves an offer, via letter, e-mail or fax, to share a huge sum of money in return for using the recipient's bank account to transfer money out of the country.

This has been around for years but is still continuing to foil the unsuspecting. The perpetrators often use the bank account details to empty their victim's account.



## 8. INVESTMENT RELATED SCAMS

An unsolicited telephone call offers the opportunity to invest in "soon to be rare" commodities such as shares, fine wines or gem stones.

Often high risk, these may be worth a lot less than you pay. The shares are not quoted on any stock exchange and could be difficult to sell afterwards, while gemstones are said to be stored in secretive Swiss bank vaults, so the investment is never seen.

## 7. PRIZE DRAW MAILINGS

"Prizes" such as holidays can only be claimed in return for administrative fees.

The majority appears to be notification of a prize in an overseas draw or lottery.



## 6. PROPERTY INVESTMENT SCHEMES

Investors attend a free presentation, which aims to persuade them to hand over large amounts of money to enroll on a course promising to make them successful property dealers.

Schemes include buying yet-to-be-built properties at a discounted price or buy-to-let schemes where companies offer to source, renovate and manage properties, claiming good returns from final rental income.

Unfortunately if the properties do exist they are generally near derelict and the tenants non-existent.



## 5. CREDIT SCAMS

Another advance fee fraud where adverts appear in local newspapers offering quick loans regardless of credit history. Respondents are told that their loans have been agreed but they must pay a fee to cover insurance before the funds can be released.

After this "Insurance fee" has been paid, the consumer never hears from the company again and the loan never materializes.

## 4. MATRIX SCHEMES

These are generally promoted via websites offering top of the range electronic gadgets such as free gifts in return for spending around £20 on an inexpensive product, like a mobile phone signal booster.

Consumers who buy this "inexpensive product" then join a waiting list to receive their free gift. The person at the top of the list only receives their gift after a prescribed number of new members join up.

Sadly, the majority of those on the list will never receive their free gift.



## 3. TELEPHONE LOTTERY SCAMS

Many of these scams go under the name of genuine lotteries such as the Canadian Lottery and the El Gordo Spanish lottery. Unsolicited telephone calls inform people that they are being entered into a prize draw.

At a later date they receive a call congratulating them on winning a substantial amount of money in a national lottery but before they can claim their prize they are told they have to send money to pay for administration fees and taxes. Of course, the prize doesn't exist.



## 2. WORK FROM HOME SCAMS

'Business opportunity' and 'work at home' scams are often advertised as paid work from home.

On application, would-be workers are asked for money up-front to pay for materials and after payment, hear nothing. Alternatively, people are asked to invest in a business with little chance of success.

## 1. CASH MACHINE FRAUD

Cash machine fraud describes where the fraud occurs i.e. where the person withdraws money at an ATM and finds their account is compromised.

Although fraud at cash machines in the UK has increased significantly in the last five years, it accounts for less than 10% of total plastic card fraud losses.



## How does it work?

### Card Reading Devices

In the case of 'skimming' at ATMs, a 'skimming' device is attached to the card entry slot and a separate miniature pinhole camera is hidden overlooking the PIN pad. The criminal can then produce a counterfeit card and withdraw money at a cash machine using the legitimate PIN.

Highly sophisticated devices, these look as if they are part of the machine itself. The device may only be placed on the machine for a short period of time whilst the fraudster remains nearby.

### Shoulder Surfing

Criminals take the opportunity to look over the cardholders shoulder to watch the PIN being entered, and then steal the card using distraction techniques or pickpocketing.

### Card Trapping Devices

A device, inserted into a cash machine's card slot, retains the card inside the cash machine. The criminal tricks the victim into re-entering the PIN whilst watching. After the cardholder gives up and leaves, the criminal removes the device with the card, and withdraws the cash.

### Avoid Cash Machine Scams

If you suspect a device has been placed on an ATM, DO NOT ATTEMPT TO MOVE IT. These are expensive devices and suspects may use violence if they think that their valuable commodity is likely to get damaged.

- Instead call the police or contact the bank immediately.
- Do not keep your card and PIN number together.
- Be mindful of people behind you at cash machines.

## JARGON BUSTER

### WHAT IS SKIMMING?

A process where the genuine data on a card's magnetic strip is electronically copied onto another, without the cardholder's knowledge.

- Do not let others see your PIN number.
- When keying in your PIN number try to cover your typing hand.

Source: Office of Fair Trading.