



Top Ten Internet / Email scams to be wary of.

1. The Nigerian scam, also known as 419.

It is a desperate cry for help in getting a very large sum of money out of the country. A common variation is a woman in Africa who claimed that her husband had died, and that she wanted to leave millions of pounds of his estate to a good church.

In every variant, the scammer is promising large payments for small unskilled tasks. This scam, like most, is too good to be true. Yet people still fall for this money transfer con game.

2. Advanced fees paid for a guaranteed loan or credit card.

If you are thinking about applying for a "pre-approved" loan or a credit card that charges an up-front fee, ask yourself: "why would a bank do that?"

Remember: reputable credit card companies do charge an annual fee but it is applied to the balance of the card, never at the sign-up. Furthermore, if you legitimately clear your credit balance each month, a legitimate bank will often wave the annual fee.

3. Lottery Scams.

Most of us dream of winning big, quitting our jobs and retiring whilst young enough to enjoy the fine things in life. Chances are you will receive at least one email from someone saying that you did indeed win a huge amount of money. The visions of a dream home, or great holiday, or other expensive goodies you could now afford with ease, could make you forget that you have never ever entered this lottery in the first place.

This scam will usually inform you that you won millions of pounds and congratulate you repeatedly. The catch: before you can collect your "winnings", you must pay the "processing" fee of several thousands of pounds. Stop! The moment the bad guys cash your money, you lose.

AME PARTNERS

Microsoft
GOLD CERTIFIED
Partner

Microsoft
Small Business
Specialist

sage Business Partner

2008
Preferred Partner



LATEST NEWS

* [Samsung 19" Monitor - only £99!](#)

* [Latest Technology – Mobile Pocket Cinema Projector!](#)

* [AME Printer Offer!](#)

* [Out of the office?](#)

CONTACT US

AME Solutions

Sannerville Chase
Exminster
Exeter
Devon

EX6 8AT

4. Phishing emails and phony web pages.

01392 824 022

This is the most widespread Internet and email scam today. "Phishing" is where digital thieves lure you into divulging your password information, through convincing emails and web pages that resemble legitimate credit authorities like eBay or PayPal. They frighten or entice you into visiting a phony web page and entering your user name and password. Commonly, the guise is an urgent need to "confirm your identity". They will even offer you a story of how your account has been attacked by hackers to get you into entering your confidential information.

Info@amesolutions.co.uk

www.amesolutions.co.uk

The email message will require you to click on a link. But instead of leading you to the real login https: site, the link will secretly redirect you to a fake website. You then innocently enter your user name and password. This information is intercepted by the scammers, who later access your account and fleece you for several hundred pounds.

Tip: the beginning of the link address should have https://. Phishing fakes will just have http:// (no "s"). If in doubt, make a contact the company to verify if the email is legitimate. In the meantime, if an email seems suspicious to you, do not trust it. Be sceptical could save you hundreds.

5. Items for sale overpayment scam.

This scam involves an item you might have listed for sale such as a car, van or some other expensive item. The scammer finds your ad and sends you an email offering to pay much more than your asking price. The reason for overpayment is supposedly related to the international fees to ship the car overseas. In return, you are to send him the car and the cash for the difference.

The postal/money order you receive looks real so you deposit it into your account. In a couple of days (or the time it takes to clear) your bank informs you the money order was fake and demands you pay that amount back immediately. In most documented versions of this money order scam, the money order was indeed an authentic document, but it was never authorised by the bank it was stolen from.

6. Employment search overpayment scam.

You have posted your CV, with at least some personal data accessible by potential employers, on a legitimate employment site. You receive a job offer to become a "financial representative" of an overseas company you have never even heard of before. The reason they want to hire you is that this company has problems accepting money from US customers and they need you to handle those payments. You will be paid 5 to 15 percent commission per transaction.

If you apply, you will provide the scammer with your personal data, such as bank account information, so you can "get paid". Instead, you will experience some, or all, of the following:

- Identity theft
- Money stolen from your account
- You may receive fake cheques or money orders for payments which you deposit into your account but must send 85 – 95 percent of that to your "employer".

7. Disaster relief scams.

What do 9-11; Tsunami and Katrina have in common? These are all tragic events where people die; lose their loved ones and/or everything they have. In times like these, good people pull together to help the survivors in any way they can, including online donations. Scammers set up fake charity websites and steal the money donated to the victims of

disasters.

If a donation request comes via email, there is a chance of it being a phishing attempt. Do not click on the link in the email and volunteer your bank account or credit card information. Your best bet is to contact the recognised charity directly via phone or their website.

8. Travel scams.

These scams generally happen during the summer months. You receive an email with the offer to get amazingly low fares to an exotic destination but you must book it today or the offer will expire. If you call, you'll find out the travel is free but the hotel rates are highly overpriced.

Some companies offer you rock-bottom prices but hide certain high fees until you "sign on the dotted line". Others will make you sit through a timeshare pitch at the destination or just take your money and deliver nothing.

Should you decide to cancel, getting your refund is usually a lost cause.

Your best strategy is to book your trip in person, through a reputable travel agency or proven legitimate online service like Expedia.

9. "Make Money Fast" chain emails.

A classic pyramid scheme: you get an email with a list of names, you are asked to send 5 pounds by mail to the person whose name is at the top of the list, add your own name to the bottom, and forward the updated list to another group of other people.

The author of this scam letter painstakingly explains that, if more and more people join this chain, when it's your turn to receive the money, you might even become a millionaire!

Bear in mind that, the list of names is manipulated to keep the top name (the creator of the scam, or his friends) on top, permanently.

As with the previously circulating snail-mail version of this chain, the email edition is just as illegal. Should you choose to participate, you risk being charged with fraud.

10. "Turn Your Computer Into a Money-Making Machine!"

Although this is not a full blown scam, this scheme works as follows: You send someone money for instructions on where to go and what to download and install on your computer to turn it into a money-making machine... for spammers.

At sign-up, you get a unique ID and you have to give them your PayPal account information for the "big money" deposits you'll "soon" be receiving. The program that you are supposed to run, opens multiple advertising windows, repeatedly, thus generating per-click revenue for spammers.

In other scenario, your ID is limited to a certain number of page clicks per day. In order to make any money whatsoever from this scheme, you are pretty much forced to scam the spammers by hiding your real IP address with Internet proxy services such as "findnot", so you can make more page clicks.

**For more information or assistance with any aspect
of your IT requirements please call us on
01392 824022 or email info@amesolutions.co.uk**

Advanced Media Engineering for all your I.T. needs

HEAD OFFICE : Sannerville Chase, Exminster, Exeter, Devon, EX6 8AT

Telephone: 01392 824022 Fax: 01392 824857

Web: www.amesolutions.co.uk

VAT Reg No: 873 8446 80

Registered In England: 4094349

