MFSA
MALTA FINANCIAL SERVICES AUTHORITY
Notabile Road, Attard BKR14
Tel +356 2144 1155 Fax +356 2144 1188

# Media Release

**Issued: 12 October 2004**
**For immediate release**

## "Phishing" – Email users urged to beware of a new type of internet scam

In these last few days, the Malta Financial Services Authority (MFSA) has received a number of reports from the general public regarding what appears to be a new wave of spam emails which seem to originate from international financial entities such as bank or credit card companies. These emails urge customers to submit personal information about themselves or to "verify" information that was previously provided when their account was established. Those tricked into providing their details run the risk of losing money from their account or even misuse of their personal details.

This troubling new internet phenomenon is called "phishing" as fraudsters are trying to hook potential victims from a sea of internet users. When fraudsters go on "phishing" expeditions, they lure their targets into a false sense of security by hijacking the familiar, trusted logos of established, legitimate companies. A typical phishing scam starts with a fraudster sending out millions of emails that appear to come from a respected financial services provider.

From the e-mails reported to MFSA, it is evident that these fraudsters are capable of designing e-mails and websites to look like those of the organisation being copied. As a result, it is hard to tell whether the email received is from a genuine organisation or from a fraudster. Rather than create from scratch a hoax company, the fraudster might use a legitimate company's name and incorporate the "look and feel" of its website (including the colour scheme and graphics) into the "phishy" email.

Users should not be fooled ? if there is suspicion that the email is not authentic, the organisation concerned should be contacted for the purposes of verifying the authenticity of its communication.

The MFSA urges the public to be extremely cautious and not to rush into responding to any type of e-mail with urgent requests for personal information.

Persons wishing to obtain additional information about this scam are invited to contact the MFSA's Consumer Complaints Manager (telephone: 80074924, direct: 25485313, email address: consumerinfo@mfsa.com.mt).

**Further information:**

1. Typically phishy emails are not personalised. However, this may not exclude emails which might either include the name of the organisation being copied or contain the names of officials who actually work with the organisation (or both) in the "from:" line.

2. In common phishing scams, emails might include information that seeks to upset or stimulate the user to respond without delay (such as a warning that failure to respond will result in the user's account being deactivated).

3. These phishy emails might also include a convenient link to a seemingly legitimate website where a user is asked to enter information which the fraudster wants to steal. The page will be designed to look like other pages from the real/legitimate website. In some cases, the page might also contain links lead to select pages of the legitimate website — such as the real company's actual privacy policy or legal disclaimer.

4. The best way one can protect himself from phishers is to understand what legitimate financial service providers will and will not do. Most importantly, legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as email. Therefore, users should not rush into responding to any type of e-mail with urgent requests for personal information. Moreover, before sending any personal information, a user should always ensure that he is using a secure website.

5. Users should never use links within an email to get to a company's website. It is always safer to type the internet address of the site the user would like to visit in the address bar at the top of the browser.

6. As many of these scams are spam, e-mail users should have reliable anti-virus and anti-spam software installed and up to date with the latest virus/spam filters.

7. It is also advisable for users to regularly reconcile their bank and credit account statements as this will help in detecting fraud quickly.

*Issued by the Information Office, Malta Financial Services Authority*