22 October 2003

PRESS RELEASE

FOLLOWING NEW EMAIL SCAM THE NATIONAL HI-TECH CRIME UNIT AND UK BANKING INDUSTRY JOIN FORCES TO HELP CONSUMERS STAY SAFE ONLINE

Today (22 October) the National Hi-Tech Crime Unit (NHTCU), APACS (the Association for Payment Clearing Services) and the BBA (British Bankers' Association) issued a checklist for UK consumers to help protect themselves against the Internet fraudster. The advice coincides with a two-tiered email scam that has emerged over the past two months.

The first part of the scam involves emails being sent to UK consumers claiming to be from UK banks, asking them to "re-register" or "reactivate" their accounts at a replica bank website. Should people provide their password details, the criminals are potentially able to transfer money out of their accounts.

Typically, the fraudsters behind these fake sites are located outside the UK and, as they are unable to transfer money directly out of their victims' online account overseas, they need a UK intermediary. Over the past few weeks, in order to achieve this, the fraudsters have been attempting a second "funds transfer" email scam. This involves spam emails being sent to people offering them the chance to make some easy money by acting as a UK agent to a business overseas. They are asked to receive funds into their account and send them on overseas, less a certain commission. If someone agrees to do so, their account is used as part of the scam to send on stolen funds to the fraudsters overseas.

Although all the early indications are that very few people have been successfully duped by these scams - and the likelihood of falling victim to any type of Internet fraud is very low - the banking industry is fully committed to keeping the Internet safe for its customers and is publishing this new checklist to make people aware of the need to treat the emails they receive with caution.

Detective Chief Superintendent Len Hynds at the NHTCU says of the new scam: "*We know that many of these 'funds transfer scams' involve the proceeds of fraud and consumers who participate in these schemes are likely to become embroiled in a police investigation. The message* is - don't allow yourself to be duped*. Remember, if an unsolicited money-making offer looks too good to be true, then it probably is*."

David Lennox, Director, Fraud & Physical Security at the BBA comments: "*The threats in the online world are the same as in the offline world. While these types of fraud have always been with us, the Internet is now being used as the preferred medium for attempting to carry them out*".

Sandra Quinn, Director of Corporate Communications at APACS, adds: "*There is no reason why the Internet shouldn't be safe and used with confidence but our message is* - don't relax your guard when online*. Be more suspicious of an email than you would of someone knocking on your door requesting information because it is harder for you to ask the sender to prove they are who they say they are*."

Tips for staying safe online

Know who you are dealing with - Always access Internet banking by typing the bank's address into your web browser. Never go to a website from a link in an email and enter personal details. If in doubt, contact the bank separately on an advertised number.

Keep passwords and PINS safe - Always be wary of unsolicited emails or calls asking you to disclose any personal details or card numbers. Keep this information secret. Be wary of disclosing any personal information to someone you don't know. Your bank and the police would never contact you to ask you to disclose PINs or all your password information.

Keep hold of your cash! - Don't be conned by convincing emails offering you the chance to make some easy money. If it looks too good to be true, it probably is! Be especially wary of unsolicited emails from outside the UK - it will be much harder to prove they are who they say they are.

Keep your PC secure - Use up-to-date anti-virus software and a personal firewall and, if your computer uses the Microsoft Windows operating system, keep it updated from the Microsoft website. Be extra careful if using Internet cafes or any PC which is not your own and over which you have no control.

Check your bank's website - If in doubt, a good place to get help and guidance on how to stay safe online is your bank's website. Check regularly for specific information and guidance on protecting your PC and yourself online.

Check your statement - If you notice anything irregular on your account contact your bank immediately.

Notes to editors

- APACS' research (September 2003) shows a five-fold increase in banking online user numbers over the past three years, taking the total number of active users in the UK to over 11 million.
- Fund transfer scams – most recently fraudsters have been sending spam emails with fake job offers and advertising dummy jobs on recruitment websites to lure consumers to act as their UK agent in fraudulent money transfer schemes.
- Spoof emails and websites (often called "phishing") have been used by fraudsters all over the world to attempt identity theft, plastic card and Internet banking fraud. Spam emails are sent randomly to potential victims' addresses - not obtained as a result of security breaches at banks or companies they are doing business with. Typically, an email claiming to be from a bank contains a link to a fake copy of the bank's real website, often hosted overseas. This fake site will closely mimic the real site and will try to dupe the consumer into disclosing financial or personal information such as credit card numbers or passwords. Banks continue to monitor the Internet and work with the National Hi-Tech Crime Unit and foreign law enforcement agencies to get dummy websites shut down.

Media contacts:

NHTCU - Louise Brown, Office Manager - 0870 241 0549 / louise.brown@nhtcu.org

BBA - Brian Capon, Head of Media Relations - 020 7216 8810 / brian.capon@bba.org.uk

APACS - Jemma Smith, Communications Manager - 020 7711 6340 / jemma.smith@apacs.org.uk

See www.apacs.org.uk or www.cardwatch.org.uk for further information.

ENDS