Agent Engagement Strategy Group

Briefing: VAT Phishing Attack

Author: Roger Murphy (VAT Systems Lead, Indirect Tax)

Summary: There is evidence that a number of agents were targeted by a sophisticated email "phishing" scam.

The fraud involved identity theft via malicious software (mainly disguised in 'phishing' emails) sent to some tax agents. It was designed to extract the secure login details of customer accounts to enable the fraudsters to submit bogus VAT repayment claims.

Sophisticated malicious software can evade even the latest security controls in some cases, targeting the login credentials for a variety of financial services. These can be very challenging to detect. IT security can be a technically challenging area: By ensuring computer updates are applied and your web browser/security software is up to date, you can mitigate the vast majority of threats, but sadly not all. Please continue to maintain your vigilance in this regard.

HMRC employs an array of measures to ensure the integrity of our systems and data. These include intrusion detection and prevention systems, transactional monitoring and extensive, rigorous audit trails to support this activity. We take security very seriously and continuously monitor systems and customer records to guard against fraudulent activity. We have robust processes both to prevent attempted fraud and to investigate and prosecute those behind this activity. For obvious reasons the details of these processes cannot be made public but they involve both automatic risk assessment and manual reviews.

We understand that despite best efforts to protect your systems, these events may still sometimes occur. We also recognise that data held by HMRC and tax agents could be exploited by identity thieves. This is why HMRC will continue to invest in digital security to ensure such activity can be detected and stopped promptly. It is also why we feel it is important to notify victims and work with them to raise their awareness of any potential further misuse of their data.

What Agents need to do

If you have not already done so, please make sure that your anti-virus, anti-spyware and firewall software is fully up to date. You should then carry out a full computer scan using your software to make sure your computer is clear of computer viruses.

Please also review who has access to the computer or network that is used to access our systems. You should make sure confidential data such as your password and credentials are secure and not shared with others. For more information, please go to our agent security pages **www.hmrc.gov.uk/security/agents.htm**

We strongly recommend that you change the passwords you use for all government transactions or services, including ours, at least once every three months.

What we have done

- We have identified the customer accounts changed by the fraudulent attack and we have written* to each agent’s affected clients separately as well as the relevant agents (*****letters were sent out w/c 16th December 2013 onwards)
- We have cleansed the affected customer accounts and returned them to their ‘pre-attack’ status
- We have ensured there is no financial loss to customers and no disruption to the HMRC Agent Online Service
- We have introduced additional security measures to guard against a repeat attack of this nature.

What can be done in general to guard against further attack?

There may be things you can do to identify other fraudulent activity and prevent it happening again. You can get more information and advice from

- the National Fraud Authority’s ‘Action Fraud’ website: **www.identitytheft.org.uk**
- the UK’s fraud prevention service’s ‘Credit Industry Fraud Avoidance System’ website: **www.cifas.org.uk** (or 0330 100 0180, 8.00am to 6.00pm Monday to Friday);
- CIFAS also provides a Protective Registration Service to help people protect their details from being misused. You can phone them on **0330 100 0180**, 8.00am to 6.00pm Monday to Friday.
- ‘Get Safe Online’ - this website provides practical advice on how to protect against online fraud, identity theft, and viruses: **www.getsafeonline.org.**