HM Revenue & Customs

Issue briefing

Online security

We take the security of our online systems very seriously and the enhancement of our cyber crime capability is just the latest in a series of anti-fraud measures we are taking every day. This briefing sets out our approach to keeping our online systems and customers' information safe.

Protecting our customers from phishing

We recognise that our customers can be innocently caught up in cyber crime attacks known as phishing and they might provide their details to online criminals. There are more than 30,000 new phishing websites established every month, with many millions of phishing emails sent via the internet, as well as other means, such as texts. HMRC's name and brand is used in thousands of phishing attacks – most of which are issued by criminal organisations to offer bogus tax refunds or rebates. They direct customers to false websites designed to dupe them into divulging personal information, such as bank and/or credit card details and sometimes login and password details, including those for online Government services. Bank, credit card and login details can all be used for fraud and personal data for identity theft, so it is important that customers are watchful for this threat.

We heavily publicise the fact that we only ever contact customers who are due a tax refund in writing, yet thousands of our customers still fall prey to phishing scams every year. Our research shows that 58 per cent of HMRC-branded phishing attacks originate from the USA, with only seven per cent coming from the UK. Some of the measures we take to stop this activity include:

- blocking criminals from copying images from our website to create bogus sites. We get 250 of these attempts a day
- creating simple but effective dedicated channels to report the attempted hijack or misuse of passwords or credentials
- dealing with more than 15,000 emails from the public each month related to phishing activity
- deploying an industry-leading anti-phishing service, which has taken down more than 1,000 counterfeit HMRC sites since its launch in 2011, including 228 additional site closures in 2012
- providing security advice to our customers via our genuine website – in January we had more than 55,000 unique visitors to our security pages (see website address at the end).

Tackling fraud

Our systems are not easy to defraud and we are constantly updating our controls and risk-assessment procedures to ensure they are protected from fraud. On top of our anti-phishing measures, our current successful counter-fraud activity includes:

- actively monitoring our systems and repayments for fraud attempts and blocking them
- suspending suspicious payments before they reach the receiving bank
- working with other government departments, law-enforcement agencies and commercial organisations to reduce and tackle the threat from cyber crime across the public and private sectors
- sharing information about known fraudsters and fraud techniques across our systems
- close working with the highest-risk customer groups, such as tax agents, and the publication of security guidance pages on our website (which have had 270,000 views)
- criminal investigation of organised crime groups using cyber crime techniques.

It is also vital that customers protect their passwords and log-in details. Customers should regularly update their computer software and their antivirus and firewalls. This helps protect their computers from viruses and other malicious software that can steal login details and passwords, allowing criminals to login to a customer's account. Where this occurs, we can still prevent fraud as we monitor our systems for unusual or suspicious activity on customer accounts, even where the correct password has been used.

Preventing attacks on our systems

Like many other organisations with a significant online presence, we are the subject of repeated large-scale attacks on our systems from activist groups attempting to disrupt our services, or criminal groups attempting to weaken our security in the hope of stealing sensitive information. We are constantly monitoring and updating our protective controls to stay one step ahead of these cyber threats and have so far succeeded in withstanding these attacks, which mostly originate from abroad. In addition, we have blocked more than 15 million malicious emails during 2011-12 and eight million SPAM emails during the same period.

Catching the cyber criminals

Our criminal investigators and intelligence officers relentlessly pursue those cyber criminals who seek to defraud the taxpayer. We use a range of investigative powers to identify, disrupt and prevent organised criminals from successfully profiting from cyber crime that targets HMRC. We have successfully prosecuted those using cyber crime techniques to try to steal money from HMRC and ultimately deprive the country of the money it needs to fund vital public services. Our digital forensics team provides technical expertise to assist investigators tackling cyber crime and provides the evidence needed to take cyber criminals to court. The ever-changing nature of the internet and the speed which cyber criminals can launch and alter the pattern of these attacks presents considerable challenges for law-enforcement agencies, including HMRC.

Enhanced cyber crime capability

We have increased our capability by recruiting and developing cyber specialists from within HMRC, other government departments, and the private sector to protect the Exchequer from attempted fraud by cyber criminals. The new recruits will build on our existing cyber counter-fraud capability and existing investigation and intelligence work. The enhanced capability is a key part of our Cyber Crime and Security Strategy, and supports the National Cyber Security Strategy launched by the Cabinet Office in November 2011. Recruitment of high-calibre technical experts, analysts and investigators protects HMRC and our customers from fraud, using technology funded by the National Cyber Security Programme.

This capability is providing us with a better awareness of the nature of the threat by using specialist forensic tools to exploit intelligence. Giving expert advice on keeping our services secure, they provide technical expertise to our criminal investigators and present real-time intelligence to our operational risk and security teams.

To find out more

Visit our website at **www.hmrc.gov.uk/security/index.htm**