

Prevention of IT related tax fraud: Advice for Tax Agents and Advisers

This guidance is being issued in response to recent fraudulent activity.

Some recent attempted frauds have been via tax agents' systems. The claims have all been submitted using valid log in details and passwords, requesting payment to a third party bank account. Only a few agents have been affected so far and HMRC is working with them and the police to tackle the problem. Investigations to date have confirmed that there has been no breach of HMRC's security systems, so a priority is to identify how the criminals obtained the information. The main risk involves the stealing of identity or access details.

Please take the necessary time to read and implement this advice where relevant to you and your business.

A. Online security - making your online experience as secure as possible

Electronic communication and transactions are a key part of HM Revenue & Customs (HMRC) business. The advantages that online transactions provide can, however, also give rise to the risk of fraud - individuals claiming to be someone they are not, and obtaining information and misappropriating funds to which they are not entitled. Good security is therefore essential at both ends of a transaction. HMRC, in common with all responsible providers of online services, is committed to data security and tax agents also need to make sure that systems and processes are secure and regularly reviewed.

HMRC continuously monitors systems and customer records to guard against fraudulent activity. The methods fraudsters use to obtain the information they want are constantly changing and becoming increasingly sophisticated, so HMRC provides regular updates on the type of scams it is aware of (see Section G). The main risk involves the stealing of either identity or access details.

Please do everything you can to ensure that your HMRC log in details and passwords for accessing HMRC systems and your own systems are kept secure and are updated regularly. Any suspicious activity should be reported to HMRC immediately. (see Section F)

B. Why is Online Security important to HMRC, Tax Agents and their clients?

The use of online services to handle clients' tax affairs continues to grow, due in part to mandatory requirements, but also because of the speed and accuracy they offer. The log in details and passwords that you use provide access to your entire registered client base, so it is vitally important that these are protected.

Online services enable agents to create and update client information, at times generating repayments of tax. If agents' confidential credentials fall into the wrong hands, fraudsters have the ability to generate spurious tax repayments and direct them to third parties without the knowledge of HMRC, the agent or the client until after the fraud has been perpetrated. These credentials can be obtained through physical access in an agent's office, sight of passwords displayed on workstations or notice boards, inappropriate disclosure through "phishing" emails or the unintentional downloading of malicious software that can be used to record confidential information remotely.

Such frauds can lead to financial losses for agents, their clients or HMRC, as well as affecting the client/agent relationship. There is also the potential to undermine clients' confidence in the ability to communicate or transact business with HMRC or their agent by email or online.

C. What HMRC does to protect the online tax system

HMRC takes online security very seriously. Here are just some of the measures HMRC takes to protect you and your clients' data:

Firewall protection

HMRC uses firewall protection as a very effective high security barrier around its systems and your data. This detects many attempts at unauthorised entry.

Security certificates

Any page of the HMRC website that contains sensitive information is protected by a technology known as SSL (Secure Sockets Layer). This encrypts the data you send to HMRC via the Internet. When you log into HMRC's Online Services you are always protected - and this is shown by the padlock in the bottom right hand corner of your Internet browser.

Secure sign-in

HMRC's Online Services are only available to customers who register their details. Every time you log in, you must enter your Agent User ID and Password before you can access your services.

Time-out

After 15 minutes of inactivity within HMRC's Online Services, you are automatically logged out. So if you've forgotten to log out, no one will be able to access your services once your computer has been inactive for 15 minutes. Simply log in again to continue. It's good practice to always log out if you are leaving your computer unattended (even in your own office) to prevent unauthorised access. When finally leaving the HMRC site, it's also good practice to close your Internet browser.

Further measures

HMRC will continue to monitor its security measures and update and enhance them as necessary.

D. Steps to protect your system online

Dependent on the size of your practice and the type of clients you deal with, you will already have in place normal business procedures to prevent unauthorised access to or use of data. However, HMRC recommends that the minimum level of security for any business using e-services should include:

Anti-virus software

Make sure all your computer systems have appropriate anti-virus software, that it is continually updated, and that all hard drives are periodically scanned to check the contents of the files on your computers against the information it holds about known viruses.

Personal firewall

Make sure all your computer systems which connect to the internet have appropriate firewall protection to block any unauthorised connections being made to your computers.

Anti-spyware software

Make sure all your computer systems have appropriate anti-spyware software, that it is continually updated, and that all hard drives are periodically scanned to check for known spyware and other malware. Malicious software on your computers can track what you do, potentially weakening other security measures you have in place, such as changing passwords. Identifying and tackling such software is therefore essential in reducing the likelihood of criminals gaining access to your online credentials.

Keep your software up-to-date

Make sure the software on your computers, particularly the operating system and Internet browser, is up-to-date. Make sure you download and install updates regularly.

Keep your password secure and change it regularly

It is vital to keep log in details and passwords secure. Do not pass them on to other staff unless it is absolutely necessary for their job and ensure they follow the same secure procedures. There are also basic steps that can be taken in any office environment to minimise the risk of inadvertent disclosure of identities and passwords. These include:

- A. Change your password regularly and consider an additional password change if you have personnel changes;
- B. If exceptionally you have to tell someone the password, only release it to those who need to know it for business reasons. Keep a record so you can track access if you become aware of any suspicious activity;
- C. If the password does need to be written down or stored, make sure it is physically secure so that it is only available to those who need it: do not display it on workstations or notice boards;
- D. Do not save passwords on a computer being sent for repairs to a third party; and
- E. Never give your passwords to anyone over the phone. If asked for your password by someone purporting to be from HMRC, please report this to the Online Services Helpdesk immediately. HMRC staff have been instructed never to ask for passwords.

Wireless networks

To minimise the possibility of unauthorised access, wireless networks require additional layers of security, which your IT consultant may be able to assist you with, such as:

- A. Service Set identifiers (SSIDs) (the name you give your network) should have a name that has no apparent connection with you, your business or your address, to avoid connection with you;
- B. Encryption between the router and computers is advisable;
- C. MAC addresses associated with individual computers can be added to wireless router configurations so that only permitted computers can access the router;

- D. Adding an administrative layer, such as a username and password ensures that only computers with those details can access the wireless network;
- E. The on/off switch can disable the router during periods when not used; And
- F. If you have a wired network, you should disable the wireless functionality of any routers that have this.

E. Frauds and Scam emails (phishing)

HMRC wants to make sure you can recognise a fraudulent email if you receive one. If you have received an email that you consider to be fraudulent, please forward it to HMRC at phishing@hmrc.gsi.gov.uk. HMRC cannot reply to every email, but it does investigate and take such matters very seriously.

To help you spot a scam email, HMRC has compiled a list of key points to look out for:

- Disclosing personal information - HMRC will **never ask** you to disclose personal information such as your PIN or your passwords, or your bank details. Never disclose this information to anyone.
- The padlock - when you log in to HMRC Online Services you are always in a 'secure session' - which is shown by the padlock or an unbroken key in the bottom right hand corner of your web browser. The beginning of HMRC's address will change from 'http' to 'https' when a secure connection is made.
- Your name - fraudulent emails are not normally addressed to you personally; they can have missing addressee details or contain something vague such as 'Dear valued customer'.
- The sender - HM Revenue & Customs (HMRC) was formed on 18th April 2005 following the merger of Inland Revenue and HM Customs and Excise departments. Those former departmental names no longer exist. Recent fraud attempts have used [fake departmental names](#), and purported to be sent from [HMRC Board Members](#).
- Links within the email - the email may include a link that you are asked to follow to take you to a website. When a mouse hovers over a link it will often show the underlying URL. If this is different to the one typed in the email do not click on it. Following the link could take you to a site that might look genuine but is most probably a fake, and merely clicking on the link could download malicious software to your computer systems. Always check the site shown in the address bar and if you have any concerns at all, go in via the HMRC website at www.hmrc.gov.uk.

F. What to do if you receive a scam email

HMRC would never contact you asking you to disclose personal information. If you have received an email requesting personal information or payment of tax, or suggesting that you are due a tax rebate, please take the following action:

- do not click on any links included in the email;
- send it to phishing@hmrc.gsi.gov.uk then delete it;
- if you suspect that your security may have been compromised, run your anti-virus and anti-spyware software applications to check your hard drives for infections; and
- review the advice featured on [Get Safe Online \(Opens new window\)](#) on rectifying common online security problems.

G. Useful HMRC links

To help users of online services stay secure, HMRC provides regular updates on its website.

- [Current security messages](#)
- [HMRC-related scam examples](#)

In addition, anyone signing up to use online services has to agree to abide by the terms and conditions. These include a number of provisions that relate to security and the use of the services.

- [Online services terms and conditions](#)

H. Useful external links

You may find these links useful, however they are not under HMRC control and we are not responsible for their content.

- [Get safe online \(Opens new window\)](#)
- [Bank safe online \(Opens new window\)](#)
- [Office of Fair Trading \(Opens new window\)](#)
- [Consumer Direct \(Opens new window\)](#)
- [Identity-theft.org.uk \(Opens new window\)](#)
- [APACS \(Opens new window\)](#)

August 2009