Spotlight on Digital Security Working Group

Briefings

03 February 2026

The Digital Security Working Group was initially formed by HMRC in May 2025 in response to an increase in unauthorised access attempts on HMRC agent digital services, which is some cases enabled fraudulent filings to be made.

In the first half of the year, professional bodies received a significant number of concerns from members who were struggling to navigate agent account suspensions and, in some cases, dealing with the consequences of fraudulent filings. ATT and CIOT, along with other professional bodies, raised these concerns with HMRC.

To facilitate collaborative discussions on key current issues, HMRC established the Digital Security Working Group. Membership of the group includes HMRC, ATT, CIOT, LITRG and other professional bodies. The priorities of the working group are:

- raising awareness of preventative measures that agents can take to enhance online security; and
- making improvements to the process for reinstating agent accounts following unauthorised access attempts.

This group initially met on a monthly basis, with meetings now arranged every six to eight weeks as required. The group has been undertaking a range of activities:

Transparent and collaborative sharing of experiences: Professional bodies have been able to pool examples of the difficulties faced by agents when navigating agent account suspensions and share these with HMRC, including cases involving fraudulent filings. This has helped to highlight changes that could be made to communications issued by HMRC during the account suspension process, as well as potential improvements to HMRC processes and call handler guidance. HMRC has been open and transparent about the challenges it has faced in responding to agent account hacks and has provided insight into measures being developed to improve security.

HMRC communications and guidance: The group has worked collaboratively to identify what guidance would be most helpful to agents in protecting themselves against malevolent activity, and how best to communicate this information. HMRC is also due to publish agent-specific guidance, which will be accessible from the Agent Handbook once published. In addition, HMRC has published an article in Agent Update 135 on how to protect agent accounts from phishing scams.

Multi-factor authentication: The group has been working with HMRC and other stakeholders to explore the potential introduction of multi-factor authentication as an option to enhance security for agent online services, particularly for agents who do not have the proprietary security infrastructure available to larger firms. While there are a number of complexities to address in implementing multi-factor authentication, the group will continue to work with HMRC as this project progresses.

We continue to welcome feedback on unauthorised access attempts to HMRC digital services to inform ongoing discussions with HMRC.

Please send any feedback to us at:
CIOT: technical@ciot.org.uk
ATT: atttechnical@att.org.uk