Ethical hackers collaborate with Defence to strengthen cyber security

Bug Bounty programmes provide safe environments for experts to identify areas where security can be improved. The identification of real vulnerabilities by ethical hackers is rewarded and Defence cyber teams are working with the ethical hacking community whose expertise has been extremely valuable in finding and remediating vulnerabilities – ensuring better security across Defence's networks and 750,000 devices.

In the Integrated Review published earlier this year, the government committed to a more robust position on security and resilience, ensuring that lives and livelihoods are protected from those who may wish to do us harm. This challenge is part of wider plans to ensure transparency and collaborate with partners to improve national security.

MOD will continue to make use of the Bug Bounty expertise, in addition to other capabilities available to ensure cyber security and resilience. MOD cyber security efforts reinforce the UK Government strategy for cross-department resilience and security, lessons learned by Defence are shared with partners.

Minister for the Armed Forces James Heappey said:

> Bug bounty is an exciting new capability for the Ministry of Defence. Our cyber teams are collaborating with the ethical hacking community to identify and fix vulnerabilities in our systems, ensuring we're more resilient and better protected.
>
> This work will contribute to better cyber and information security for the UK.

Participants praised Defence for its openness and willingness to embrace new tools and capabilities to secure cyber systems. Programmes like this are industry best practice and used by governments and organisations across the world to defend against possible cyber-attacks.

Christine Maxwell, Ministry of Defence Chief Information Security Officer said:

> The Ministry of Defence has embraced a strategy of securing by design, with transparency being integral for identifying areas for improvement in the development process.

> It is important for us to continue to push the boundaries with our digital and cyber development to attract personnel with skills, energy and commitment. Working with the ethical hacking community allows us to build out our bench of tech talent and bring more diverse perspectives to protect and defend our assets. Understanding where our vulnerabilities are and working with the wider ethical hacking community to identify and fix them is an essential step in reducing cyber risk and improving resilience.

CEO of HackerOne, Marten Mickos said:

> Governments worldwide are waking up to the fact that they can’t secure their immense digital environments with traditional security tools anymore.

> Having a formalised process to accept vulnerabilities from third parties is widely considered best practice globally, with the U.S government making it mandatory for their federal civilian agencies this year. The U.K MoD is leading the way in the U.K government with forward-thinking and collaborative solutions to securing its digital assets and I predict we will see more government agencies follow its example.