Cyber Security Alert

Hacktivists target UK Organisations

Police Scotland Cyber and Fraud Unit.

30.01.2026

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

New Guidance: The NCSC encourages local government and critical infrastructure operators to harden their ‘denial of service’ (DoS) defences.

The cyber threats organisations face will vary over time, especially as criminals surreptitiously take advantage of advances in technology.

There may be times when the cyber threat to an organisation is greater than usual, such as moving to heightened state of alert and preparation for this is key.

This change in focus will;

- help prioritise necessary cyber security work i.e. review of Business continuity and incident response plans.
- offer a boost to defences.
- give organisations the best chance of preventing a cyber-attack and recovering quickly if it happens.

From the perspective of a business operating model, there will be a need for organisations to strike a balance between their risk appetite to the current cyber threat, the measures needed to defend against it, the implications and cost of those defences and the overall risk to the organisation.

The NCSC (National Cyber Security Centre) is currently advising UK organisations to strengthen their current cyber security controls to mitigate risks associated with a move to heightened cyber threat level.

This change in focus relates to Pro-Russia hacktivist DDOS attacks - NCSC.GOV.UK which highlights the potential use of less sophisticated, lower impact attacks against critical infrastructure entities.

Organisations, particularly local government authorities and operators of critical national infrastructure, are being encouraged to review their defences and improve their cyber resilience by preparing and being able to respond to cyber-attacks with a focus to harden their ‘denial of service’ (DoS) defences.

The Heightened cyber threat - NCSC.GOV.UK guidance provide access to a collection of supporting guidance materials which will support organisations to review and improve their cyber security.

Further guidance is available via the NCSC website advising how to mitigate risks for both medium to large organisations and small organisations.

Organisations are also encouraged to register for NCSC's Early Warning Service, which provides notifications of malicious activity, incidents, and security issues. To find out more information about this free service and how to register please follow this link. Early Warning - NCSC.GOV.UK

We have also taken the opportunity to include Top tips for staying secure online - NCSC.GOV.UK guidance from our colleagues at the NCSC.

Information on Creating a Cyber Response Plan and Dealing with a Cyber Attack is also available on the CyberScotland Portal.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.