



POLICE
SCOTLAND
POILEAS ALBA

Cyber Security Resilience

Tensions in Ukraine; Cyber Security Guidance for UK Organisations

Police Scotland Cybercrime Harm Prevention team

19/04/2023

OFFICIAL



Heightened threat of state-aligned groups against western critical national infrastructure

Our colleagues at the National Cyber Security Centre (NCSC), the UKs' technical authority on cyber security, have issued an alert to critical national infrastructure (CNI) organisations warning of an emerging threat from state-aligned groups and we would also suggest all organisations take cognisance of this alert.

[NCSC warns of emerging threat to critical national... - NCSC.GOV.UK](#)

This is a direct follow on from previously issued guidance from the NCSC, which we shared, to assist UK organisations bolster their cyber defences in response to the situation in and around Ukraine, when they urged UK organisations to prepare for an extended period of heightened cyber threat in relation to the Russia-Ukraine conflict.

The NCSC – a part of GCHQ – warn in the alert that some groups have stated an intent to launch 'destructive and disruptive attacks' and that CNI organisations are strongly encouraged to follow the steps outlined in the NCSCs' heightened threat guidance to strengthen their defences,

[Actions to take when the cyber threat is heightened - NCSC.GOV.UK](#)

The guidance sets out an eleven point plan for sustaining a strengthened cyber security posture when systems, processes and the workforce remain under pressure and also focusing on staff welfare as a direct contributor to maintaining an organisations' resilience.

The NCSC assess the cyber threat to the UK, as a result of the conflict, remaining as heightened and organisations are urged to not let their guard down and to consult the new guidance to prepare for longer-term resilience.

We would also like to highlight other NCSC guidance and resources to help organisations improve their longer-term resilience, including the [10 Steps to Cyber Security](#) and [Cyber Security Toolkit for Boards](#).

OFFICIAL

OFFICIAL

Also included is the following link to Cyber Essentials and we strongly encourage you to consider this resource as a fundamental in your cyber security.

[About Cyber Essentials - NCSC.GOV.UK](#)

The NCSC further support your resilience and continuity, both on a personal and business level with their;

[Stay protected online with a Cyber Action Plan - NCSC.GOV.UK](#)

and this will take a couple of minutes of your time and is free. The outcome will be an action plan for you or your business, with suggestions to strengthen your cyber security and resilience.

Further information and guidance for specific sectors are available through the NCSC website

- Small Medium Enterprises - [Small business guide](#)
- General public - www.cyberaware.gov.uk
- For all - [Secure system administration - NCSC.GOV.UK](#)

Our team are sponsors for CiSP applications and the following link will provide you with further guidance on joining and the benefits of membership. [About CISP - NCSC.GOV.UK](#)

We also have additional resources which you can access at [Incident Response – Cyber Scotland](#) within the Cyber Scotland Partnership which is, a collaboration of key strategic stakeholders, focused on improving cyber resilience for all across Scotland.

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

Police Scotland Cybercrime Harm Prevention team

PPCWCyberHarmPrevention@scotland.police.uk

All information was correct at time of distribution. 19/04/2023.

OFFICIAL