POLICE
SCOTLAND
POILEAS ALBA

Cyber Security Resilience

Guidance for UK organisations

Police Scotland Cybercrime Harm Prevention team
26.11.2024.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Actions to improve cyber security.

The NCSC (National Cyber Security Centre) is continuing in its efforts in advising UK organisations to strengthen their current cyber security controls to mitigate risks from cyber threats.

The cyber threat an organisation faces may vary over time. At any point though, there is a need to strike a balance between the current threat, the measures needed to defend against it, the implications and cost of those defences and the overall risk this presents to the organisation.

There may be times when the cyber threat to an organisation is greater than usual.

Moving towards a heightened cyber awareness can:

- help prioritise necessary cyber security work
- offer a temporary boost to defences
- give organisations the best chance of preventing a cyberattack when it may be more likely, and recovering quickly if it happens

UK organisations are being encouraged to review and where necessary improve their cyber resilience to reduce risk, and to ensure a quick recovery with minimal impact, should they fall victim to a cyber-attack.

Organisations must consider their staff at all levels in terms of raising awareness of the cyber threat and to empower their staff to question suspicious emails and eliminate fear of being criticised for doing so.

As an organisation, do your staff know what a suspicious email looks like i.e. does it include a sense of urgency, unusual request, an element of pressure on the recipient to take some form of action without first questioning the originator or without seeking a second opinion before responding to the request in the email. Awareness is key to prevention.

The following NCSC guidance outlines steps UK organisations can take to improve their cyber security from an increasing cyber threat. Advice covered in the guidance includes patching, improving access controls and testing incident response plans.

Please follow this link to the latest released guidance. Actions to take when the cyber threat is heightened - NCSC.GOV.UK

Further guidance is available via the NCSC website advising how to mitigate risks - 10 Steps to Cyber Security - NCSC.GOV.UK and Small Business Guide: Cyber Security - NCSC.GOV.UK

Information on Cyber Incident Response - Cyber Scotland and Responding To An Incident – Cyber Scotland is also available on the CyberScotland Partnership website.

We have also included this link Maintaining a sustainable strengthened cyber security posture - NCSC.GOV.UK with regard to supporting your staff and frontline users.

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

A further layer of security which all organisations can aspire to is Cyber Essentials. This is an effective, Government backed scheme that will help organisations, whatever their size, against a whole range of the most common cyberattacks. About Cyber Essentials - NCSC.GOV.UK

Police Scotland are also promoting the Police Cyber Alarm (PCA) which is a free resource funded by the Home Office. The PCA helps businesses, who are part of the scheme, to understand and monitor malicious cyber activity.

Members of the scheme benefit from regular reports showing suspicious and potentially malicious attack activity on their firewall and internet gateway.

The report also details how the business is being attacked and from where, in order that they can improve their cyber resilience. You can learn more about the PCA at the following link. Police CyberAlarm

If you have been a victim of crime and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

This information was sent by Police Scotland Cybercrime Harm Prevention team

All information was correct at time of distribution.