

Important Links

www.actionfraud.police.uk – report cybercrime and fraud to police.

www.NCSC.gov.uk – National cyber security centre (Active Cyber Defence)

<https://www.cyberalarm.police.uk/> – Free network traffic monitoring

www.nomoreransom.org – Free Ransomware decryption keys

www.haveibeenpwnd.com – check if your email or phone number has been exposed in a data breach

www.emcrc.co.uk – East Midlands cyber resilience centre

www.eastmidlandscybersecure.co.uk – Our website full of free cyber security news and advice

www.eastmidlandscybersecure.co.uk/incident-response - Incident response plans guidance



NCSC_A5 Response NCSC_A5_Small_Busin
and Recovery Guide_vess_Guide_v4_OCT20.r

Important Information

Never click links in emails from unknown sources as it could be a phishing email

Report ransomware attacks/attempts immediately to Action Fraud.

If you discover yours or another business email has been compromised, Change the passwords immediately and contact Action Fraud.

Have an effective incident response plan in place:

- Advise not to pay
- Disconnect infect devices from wider network
- Change mentioned passwords & check accounts compromised
- Advise not to communicate with the criminal
- Ensure backup is free from malware

Have strong policies in place so that changes in invoice and other financial information is ratified

Never transfer money or invoices on behalf of someone else without first checking with them directly using another form of contact such as a work phone.

Keep all your devices updated and protected using anti-virus

Keep your backups updated regularly, consider a 3-2-1 back up policy: 3 separate backups, 2 file formats and 1 offsite

Make sure Access control is handled appropriately and employees only have the permissions necessary to perform their job.

Use strong passwords with three random words e.g. WaterPhilosophyZebra!72

Enable Two Factor Authentication for email and social media accounts.

Consider using NCSC active cyber defence services e.g. Exercise in a box, Early warning, Logging made easy, Vulnerability disclosure toolkit, Suspicious Email Reporting Service.

Reduce your exposure to Cyber Attacks:

- Secure Boundary firewalls and internet gateways

- Consider Malware protection/ security monitoring
- Consider your patch management
- Consider Whitelisting and Execution control
- Secure your configuration
- Consider your policies and access controls
- Ensure you have user training, education, and awareness culture
- Know your security incident management

Important Contacts

Report email phishing attempts to report@phishing.gov.uk

Report SMS phishing attempts by forwarding the message to 7726 [spells spam on the keyboard]

Report cybercrime and fraud to Action Fraud by calling 0300 123 2040 or visit www.actionfraud.police.uk

Join CISP and join a network for sharing cyber security information and advice by going to www.ncsc.gov.uk/section/keep-up-to-date/cisp-organisation