

Cyber Attack

Risk overview





Risk

Cyber attack

Risk Lead	Lincolnshire Police
Risk Descriptor	<p>We live in a digital focused world where individuals, businesses, charities and our government all rely on digital technology and online capability to deliver essential services. As a result any sector of our economy and society that uses IT networks and systems is vulnerable to the threat.</p> <p>Cyber criminals exploit weaknesses in online systems, usually for financial gain. They use technology to commit crimes, such as hacking to steal data, and can use the same technology to increase the scale and reach of other crimes such as carrying out fraudulent financial transactions.</p>
How Prepared Are You?	
How to prepare for the risk	<p>Keep your personal information protected – use strong and different passwords for your online accounts. Keep your passwords to yourself and do not share them.</p> <p>Don't leave your devices unattended without locking them.</p> <p>Turn on 2-Factor Authentication (2FA) for all your online accounts – this gives you additional protection. This makes it even more difficult for cyber criminals to access your accounts.</p> <p>Back up your data – make your data recoverable in the event that your IT equipment is compromised. Ensure backups are regularly maintained on a separate device or in the cloud.</p> <p>Always update your devices – these regular updates contain security updates and your accounts and data remain vulnerable without them.</p> <p>Remain vigilant against phishing scams – be cautious when clicking on links. Do not give out private information (such as bank details or passwords), reply to text messages, download attachments or click on any links in emails if you're not sure they're genuine.</p>
How to respond to the risk	<p>See the National Cyber Security Centre's website for information and advice on:</p> <ul style="list-style-type: none"> • dealing with common cyber problems • protecting data and devices <p>https://www.ncsc.gov.uk/section/advice-guidance/all-topics</p> <p>Cyber crimes to organisations and charities can be reported to Action Fraud at https://www.actionfraud.police.uk/ or on 0300 123 2040.</p>

	<p>They can also be reported to the police, or Crimestoppers on 0800 555 111 or http://www.crimestoppers-uk.org/</p> <p>Suspicious emails</p> <p>Forward the email to report@phishing.gov.uk The National Cyber Security Centre (NCSC) will investigate it.</p> <p>Text message</p> <p>Forward the text message to 7726 – it’s free. This will report the message to your mobile phone provider.</p> <p>Adverts</p> <p>Report scam or misleading adverts to the Advertising Standards Authority. You can report adverts found online, including in search engines, websites or on social media. https://www.asa.org.uk/make-a-complaint.html</p> <p>You can report a scam or misleading adverts to Google if you find them in Google search results, or to Microsoft if you find them in Bing search results.</p>
<p>How to recover from the risk</p>	<p>If you think you’ve been a victim of an online scam or fraud</p> <p>Contact Action Fraud via their website or 0300 123 2040 if you think you’ve lost money or been hacked because of an online scam or fraud.</p>
<p>How prepared is your family?</p>	<p>Following the 6 steps to better cyber security will ensure members of your family are best protected from a cyber-attack.</p> <ol style="list-style-type: none"> 1. Use strong passwords for online accounts 2. Do not share you password with anyone 3. Utilise a password manager 4. Turn on 2-Factor Authentication (2FA) for all your online accounts 5. Install the latest software and app updates 6. Back up your data onto a separate device or cloud service <p>Make a cyber action plan via the following link- Stay protected online with a Cyber Action Plan - NCSC.GOV.UK</p>
<p>What can you do to support your Community?</p>	<p>Make a cyber action plan via the following link- Stay protected online with a Cyber Action Plan - NCSC.GOV.UK</p> <p>Lincolnshire Police also offers free cyber-security training presentations for business staff and members of the community. If you</p>

	<p>would like to arrange a presentation, please email protectbookings@lincs.police.uk</p>
<p>How Prepared is your business?</p>	<p>See the National Cyber Security Centre's website for information and advice on:</p> <ul style="list-style-type: none"> • dealing with common cyber problems • protecting data and devices <p>Cyber crimes to organisations and charities can be reported to Action Fraud at https://www.actionfraud.police.uk/ or on 0300 123 2040.</p> <p>They can also be reported to the police, or Crimestoppers on 0800 555 111 or http://www.crimestoppers-uk.org/</p> <p>NCSC's Cyber Aware campaign provides information on the steps individuals and small businesses can take to protect themselves online.</p> <p>Make a cyber action plan via the following link- Stay protected online with a Cyber Action Plan - NCSC.GOV.UK</p> <p>Lincolnshire Police also offers free cyber-security training presentations for business staff and members of the community. If you would like to arrange a presentation, please email protectbookings@lincs.police.uk</p> <p>Businesses can also visit the East Midlands Cyber Resilience Centre for support and help to protect businesses across the region against cyber crime.</p> <p>The Cyber Resilience Centre for the East Midlands (emcrc.co.uk)</p>
<p>What are the Lincolnshire Resilience Forum doing to prepare for this risk?</p>	<p>The LRF work together to:</p> <ul style="list-style-type: none"> • Collectively develop and maintain a multi-agency Cyber Group and Cyber Response Plan. • Activate to assess the impact across interdependent partner organisations and coordinate support to enable service delivery.

For further information please see the LRF website: www.lincolnshireresilienceforum.org