Business Emergency Resilience Group Are you Cyber ready?

3 simple steps

1. Know the basics

Cyber attacks
hacks your computer to steal data or damage computer software

Online Fraud
steals your identity to make fraudulent purchases

Phishing, Spear Phishing, Whaling
tricks your clients online and installs malicious software (malware)

Trojans and viruses
installs malware onto your computer remotely via email or websites

Spyware
eavesdrops on your computer to steal your passwords

2. Protect your business

Install a firewall and anti-virus and online security software

Be aware of computer scams, unsolicited emails, fraudulent links and email attachments

Keep passwords safe, secure and regularly changed
use a mix of letters, numbers and special characters

Only visit secure websites
Donated by the prefix 'https' and locked padlock or unbroken key symbol

Obtain appropriate level of cyber insurance cover

Run regular backups and computer restore exercises

3. Know how to recover

Determine if the cyber threat is legitimate and the extent of cyber attack
use professional IT support and know who to contact for immediate help

Contain the cyber attack

Repair your computer system quickly to avoid further attacks

Communicate to your staff and customers
safeguards your reputation

"In our hyper-connected and digitally dependent world, BERG creates a unique collaboration between the public and private sectors. By encouraging greater business and community resilience, BERG helps business owners prepare for, respond to and recover more quickly from emergencies, including from cyber threats."

Mike Still, Chair, BERG

Find out more: www.bitc.org.uk/berg

www.getsafeonline.org
www.cyberstreetwise.com
https://www.cert.gov.uk/
www.actionfraud.police.uk
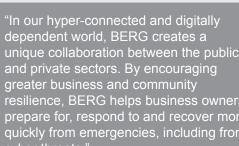www.financialfraudaction.org.uk
http://www.cpni.gov.uk/
http://www.globalservices.bt.com/uk/en/point-of-view/disrupting-cyber-crime

#BERGResilience
Business Emergency Resilience Group

Business Emergency Resilience Group Are you Cyber ready?

10 simple questions

PLAN AHEAD

		Y	N
1.	**Do you have someone responsible for cyber-crime?** Know who to contact for help including your IT Helpdesk		
2.	**Do you use an internet provider offering a high level of cyber security?**		
3.	**Do you screen prospective employees for cyber risk?** Review previous employer references and disclosure checks		
4.	**Do you have a good basic security culture amongst staff?** Regularly changed passwords, unshared and unique passwords, auto-lock function on computers; safely stored sensitive materials		
5.	**Do you know and look after your people?** Insider threats can be linked to overwork, individual grievances, poor colleague relationships, absenteeism, anti-social behaviours, financial or other welfare issues		
6.	**Do you regularly audit?** Regular overt and covert auditing of commercial and financial processes improves security		
7.	**Do you have protective security controls?** Simple systems to restrict introduction or removal of electronic data		
8.	**Are you aware of current cyber threats and emerging scams?** CERT-UK and Cross-sector Safety and Security Communications provide helpful updates		
9.	**Do you run regular backups and restore exercises?** On-line training packages on threats, mitigations and the evolving nature of cyber-crime		
10.	**Do you have cyber insurance?**		

Find out more: www.bitc.org.uk/berg

www.getsafeonline.org

www.cyberstreetwise.com

https://www.cert.gov.uk/

www.actionfraud.police.uk

www.financialfraudaction.org.uk

http://www.cpni.gov.uk/

http://www.globalservices.bt.com/uk/en/point-of-view/disrupting-cyber-crime

🐦 **#BERGResilience**

in **Business Emergency Resilience Group**

"Asking BERG's 10 simple questions and following the advice will help keep your business safe and provide security against the variety of on-line threats. Being aware of your vulnerability and questioning your Cyber attack readiness are important steps."

Allan Burnett, Operations Director, SecuriGroup