Cyber security risk

Remote working and new challenges

Unfortunately in times of uncertainty criminals will try to exploit vulnerability and confusion. As such we are seeing increases in cyber crime particularly utilising common social engineering techniques such as phishing, whaling and ransomware.

What is phishing?

Phishing is when multiple individuals are targeted by a single scam. Typically, a blanket email is sent in the hope that some will reply with sensitive information, transfer funds or open rogue links or attachments.

What is whaling?

Whaling targets a small group of individuals, usually senior executives or individuals who can authorise funds transfer. Typically a hacker will pose as a senior official and request personal information, bank detail changes or a large funds transfer.

What is ransomware?

Ransomware is when hackers gain unauthorised access to a network and system and take it over. They hold an organisation to ransom by blocking system access until a substantial payment is made.

What challenges are organisations facing during Covid that make these threats more of a risk?

- Increased number of people are working from home and outside of normal working hours.
- Employees are using their own home IT infrastructure and in some cases personal email addresses.
- Employees could be printing and downloading commercially sensitive or personal data locally.
- Employees could be less vigilant and distracted given they are not in the office.
- Security on personal equipment and devices may not be as robust as office based infrastructures and networks.
- Cyber criminals are using Covid as a means of luring individuals into accessing sites and links.

What safeguards can organisations put in place against cyber risk?

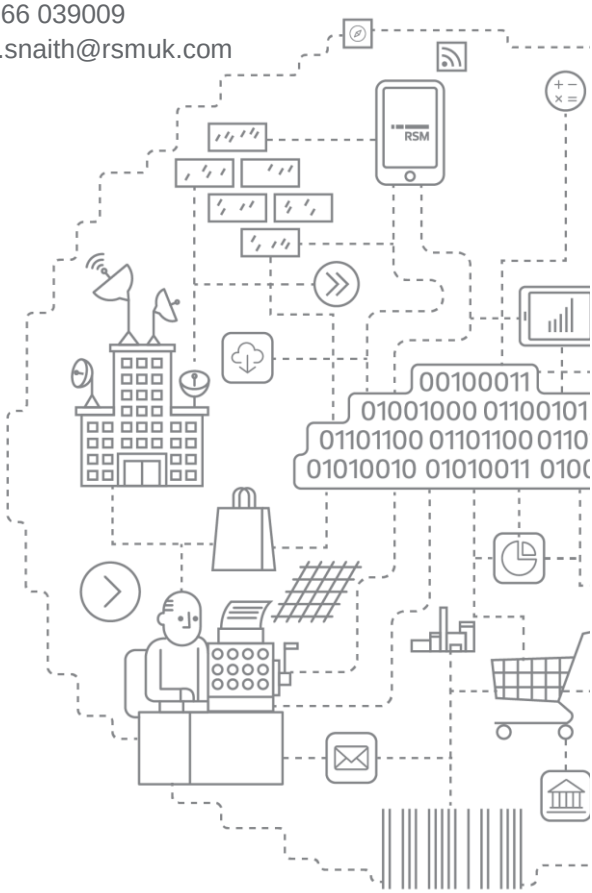
- Awareness and education is key – remind all users / employees of the IT security policy, what it covers and where to find it. This should include how to escalate concerns and incident reporting.
- Ensure all employees have completed the most up to date cyber awareness training. Run remote refresher training sessions.
- Consider running a covert phishing/whaling exercise whilst people are working at home to expose any weaknesses in controls and awareness.
- Ensure all employees are using corporate equipment (laptops, phones, etc) with latest patches and anti-virus updates applied.
- Reiterate that personal or commercially sensitive data should not be printed, downloaded or saved onto unencrypted removable media devices.

- If users find any corporate devices are running slower than normal or application systems not operating as normal they should inform IT immediately.
- Remind users not to open links or download apps onto corporate devices.
- Remind users that when they are on a video conference there is a possibility that someone could be recording the event.
- If employees are utilising home WIFI, ensure it is adequately secured and shipped passwords have been changed.
- Remind users that social media groups between employees should be used professionally as a record/log is maintained of the entire chat history.
- If a data breach is suspected inform IT immediately.

For more information please contact:

Sheila Pancholi
Partner
Technology Risk Assurance
+44 7811 361638
sheila.pancholi@rsmuk.com

Steven Snaith
Partner
Technology Risk Assurance
+44 7966 039009
steven.snaith@rsmuk.com



www.rsmuk.com