Cyber-Attack!

How to handle the situation should you become a victim.

What would you do if your business was the victim of cyber-attack? How would you handle the situation? The BBC's Technology correspondent Mark Ward recently published a great article describing what it could be like to be a victim of a rogue cyber-attack.

Our team at Dragon IS have delved into the scenario as described in the Blink Wink's head office and highlighted our own Do's and Don'ts of the case, how the individuals should have acted and where the mistakes were made.

Event in the '***Blink Wink's***' case study	**Do's**	**Don'ts**
Tuesday 8.30 am: Tony Lewis discovers the initial email with the threat.	Verify whether the email is a hoax or not. Contact the Security Officer.	PANIC
Doug Hughes, Security officer, asks if it's one of their customers. Tony doesn't know yet.	Validate data purported to be breached or stolen.	
Doug asks when the threat email was received.	Establish when the actual breach took place – it may be weeks prior as in this case when a phishing email was received with a log-in page.	Don't believe that the threat email is the time of the breach.
A second email with a ransom demand is received.		Never pay a ransom. Never respond to the email.
Doug calls Blink Wink's legal counsel.	Follow your Data Breach Policy/ procedure and ensure everyone knows their role/responsibility. Seek legal counsel. Inform Information Commissioner's Office (ICO). Contact the police about the crime. Inform your cyber insurance company.	

Please see next page for more...

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com

Event in the '*Blink Wink's*' case study	Do's	Don'ts
Doug has now confirmed that the data is genuine and it comes from their website.	Determine the source of the breach - website in this case. Contain the breach - shut down the website in this case. Repair/restore the data - make repairs to the website in this case.	Never delay getting to the source of the breach. Time is critical, as you don't want any further loss of data.
Sandra Ellis has drafted a public statement, but the team can't agree on the wording.	Call your cyber insurance company to ask for guidance and leverage their PR capabilities. Inform all affected customers about the breach (ICO requires notification within 72 hours of you becoming aware).	Refrain from writing a press release without input from your legal team/insurance provider.
Malware has been found in an email with an attachment and Tony clicked on it.	Make sure all systems are protected from viruses, malware and hacking. Audit your systems regularly.	Never click or access any email / attachment that is suspicious or that you can't verify the origin of.
Grace returns to informing the ICO. She explains they will need to say what they did to mitigate the problem.	Journal all steps taken during the incident. You might need this when reporting to the ICO, or for press release purposes.	
Tony explains why they hadn't got the latest threat detection software.	Make sure you perform an internal root cause analysis and use this information to change/update your policies/practices moving forward.	Never underestimate the threat. Don't become complacent. Audit security software and hardware frequently.
They found a phishing email had been received two months ago that linked to a lookalike log-in page for their cloud provider. That's how they got in.	Educate your staff so they can identify threats and encourage them to notify IT immediately.	

You can read the original article in full here:
https://www.bbc.co.uk/news/technology-44482380#

Want To Know More?

If you'd like Dragon IS to help you with your IT security strategy, please contact us today.

CONTACT US

For proven, trusted IT systems support to keep your business trading profitably

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com