NCi TECHNOLOGIES

Spear Phishing: How to Keep Your Organisation Off the Hook

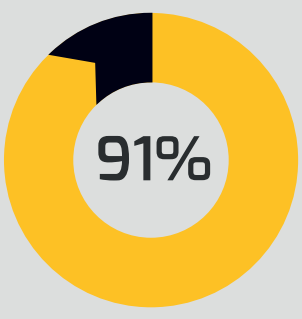
WHAT IS SPEAR PHISHING?

Spear phishing is a phishing method that uses social engineering to target specific individuals or groups. A spear phishing email will appear to be sent from a trusted source or a person of authority that the victim knows, possibly within their own organisation. A typical spear phishing attack will seek to steal personal data using malware as an attachment or using links to a phishing webpage. The attacker's goal is to gain access to your organisation's systems and networks for malicious purposes.

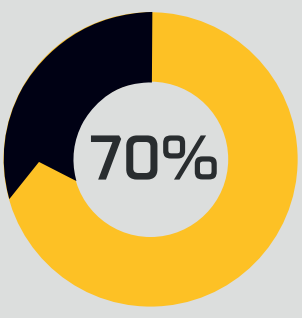
HOW DOES SPEAR PHISHING WORK?

1. Attacker gathers information on an intended victim within the target company
2. Attacker distributes email with malicious links or attachments to the targeted victim
3. Victim receives the spear phishing email in their inbox, opens it and opens attachment or clicks link
4. Attachment or link to website executes malware giving attackers access to victim's network and systems

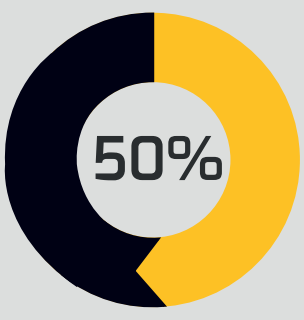
MUST KNOW SPEAR PHISHING STATISTICS



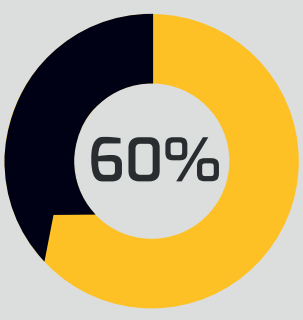
of cyberattacks begin with a spear phishing email[1]



of people open spear phishing emails[2]



of people click on the links within a spear phishing email[2]



of organisations lost data after a successful phishing attack[3]

9 WAYS TO SPOT A SPEAR PHISHING ATTACK

If you fall for a spear phishing email the effects could be devastating for your organisation, but don't despair! Here are nine ways you can spot a potential spear phishing attack.

01	Uses an unfamiliar tone	02	Contains grammar or spelling errors
03	There are inconsistencies in the email address, links, and domain names	04	Creates a sense of urgency
05	Includes suspicious attachments	06	Asks an unusual request
07	The email is short and vague	08	You did not initiate the conversation
09	It requests personal details		

STOP YOUR ORGANISATION GETTING HOOKED

Your organisation and its employees can make it harder for cyber criminals to execute a successful spear phishing attack by implementing the following steps:

01 **Limit** the amount of personal information shared online

02 **Do not click** on suspicious links in emails

03 **Confirm** email requests using a separate form of communication

04 **Analyse** your inbound email history to determine how to improve security

05 Implement an **outside audit** to expose any cybersecurity vulnerabilities

06 **Update** security software and advanced threat protection

07 Implement **cybersecurity awareness training** that includes simulated spear phishing attacks

1. KnowBe4 2022 – 91% of Cyberattacks Begin with a Spear Phishing Email | 2. Fireeye 2022 – Best Defense Against Spear Phishing
3. Tessian 2022 – Must-know Phishing Statistics: Updated 2022

ncitech.co.uk | 01326 379 497 | sales@ncitech.co.uk