

What is Spear Phishing? Transcript

What is Spear Phishing?

Spear Phishing is a step up from your average phishing attack. In a Spear Phishing attack the emails are tailored to target a specific individual, organisation or business.

Spear Phishing emails are sophisticated and the attacker has usually done their homework which makes them harder to spot. They may have used social engineering techniques, or may have researched you online. They will often know your interests, which helps them to craft the email with an enticing subject line that will trigger your curiosity.

Cybercriminals may even know the type of email that you regularly receive and when you are likely to receive them. Standard phishing emails usually appear to be from large, well known corporations, such as Google or Amazon.

However, spear phishing emails usually appear to come from an individual within the recipient's own company, or from someone they know personally. This can be enough to lure the unsuspecting individual into trusting the email.

What's the risk?

It only takes one employee to click on a fraudulent link, which will download malware onto your computer. This can have severe consequences for your organisation. The victim of a phishing attack is often asked to provide credentials such as a username, password or credit card payment details.

Cyber criminals can use Spear Phishing to steal commercially sensitive information, cause reputational damage, or even international espionage.