Spear Phishing

Spear phishing is when a malicious actor spends time before the phishing attack to gather information about their specific target, to make the email more effective. By tailoring the email to the target, it makes it more convincing. It increases the chances of the recipient clicking on the email and entering their credentials, or opening an attachment. This type of attack requires planning and good use of open-source intelligence (OSINT) sources to gather information. The attacker will look for websites that the target uses, any hobbies or interests they have, and even record family members, colleagues, or friends. All of this information can be used to create highly effective emails that seem legitimate. Let's cover a few examples.

Other phishing email techniques can be used, such as typosquatting or sender spoofing, to make the email sender appear legitimate, and if the attacker is trying to entice the target to visit a malicious website, the typo squat domain works to mimic the real name of a legitimate site, making it harder to spot at a glance that it's fake. (We'll cover both of these techniques in the next few lessons).

EXAMPLE WALKTHROUGH

An attacker wants to send a spear phishing email to an employee at Dickson United in order to get them to open a malicious attachment, which will create a backdoor and allow the malicious actor to remotely connect into the target's corporate laptop or desktop.

The attacker finds the employee on LinkedIn and notes down their colleagues. The actor then performs a reverse-image search on the profile picture and finds their Facebook account. From there, they are able to collect information about their interests and friends as they haven't set up privacy settings properly.

They then craft an email designed specifically for the target using information related to the subject so they are more likely to engage with the email. Spear-phishing emails can also include social engineering tactics such as impersonation to make the email even more believable. This type of phishing attacks are very popular with advanced malicious actors, and you'll see that this technique is responsible for lots of data breaches.