CUSTOMER GUIDE

Spear-Phishing Attack Types Explained

Avoid becoming the next victim of spear-phishing

Email continues to be the most popular cyber-attack surface. Research shows that 91% of cyberattacks starts with an email, of which, 80% reported are spear-phishing attacks. **Here is a list of the most popular spear-phishing attack types – explained.**

Employee impersonation

The attacker assumes the identity of the victim, such as an upper level employee, assuming a position of trust with the victim. Exploiting this trust, the attacker can gain access to important corporate information or convince the victim to perform a task, like a bank transfer to a malicious account.

Scamming

With email scamming, cybercriminals use fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information.

Blackmail

Online blackmailing is very similar to traditional blackmailing. The attacker will demand a large sum of payment to the victim, claiming they will reveal embarrassing information about them if the payment is not made.

Domain impersonation

The attacker intentionally misspells the 'from' address or the web address, altering it slightly in order to fool the victim. The target might respond to a nefarious request, thinking the request is coming from someone they trust.

Service phishing

The attacker impersonates a well-known service, like a bank or internet service provider, and asks the victim to click the embedded link to log into their account. The victim's login credentials are then stolen by the attacker.

Examples

Employee impersonation
The attacker impersonates an upper level employee and requests the victim to purchase various gift cards. They then instruct the victim to send the activation codes to the attacker.

Scamming
The infamous "Nigerian Prince" scam, we've all seen, which is like robo-calls but in an email format.

Blackmail
The attacker pretends to have taken access to the victim's email box, computer, or other files/property, and threatens to release damaging material (such as inappropriate pictures) in exchange for payment through crypto currency.

Domain impersonation
sgcmidlands.co.uk vs scgmidlands.co.uk

Service phishing
The attacker mimics a bank with an urgent request to the victim to log in to their account to read an urgent message.

Contact us:
0330 333 0001
info@scgmidlands.co.uk
www.scgmidlands.co.uk