WHAT YOU NEED TO KNOW

How a Spear Phishing Attack Works

[music playing]

Text: on screen: This is an example of how criminals planned and carried out a cyber attack. First they researched publicly available information and the company's website.

[An image of the company's website]

Subtitle: From the company website the criminals gathered information about the company culture, its conventions, and the people who work there.

[post it notes appear onscreen and highlights show examples of the language used (culture), the email format (conventions) and the people who work their (two people have the same name and are probably father and daughter)]

Subtitle: They created a fake social media profile and connected with people from the target company.

[Logging into a social media site, writing, and sending, an invitation to the Head of Learning and Development at the target company. Screen shows list of email addresses in a spreadsheet]

Subtitle: The used these connections to build an email list.

The wrote an email which offered the chance to take part in a draw to win £250. The email appeared to be from Jenny Moore the business development manager.

Subtitle: Can you see anything wring with Jenny's email address? It's not Jenny's email address. They used one which looks like hers but there's an 'n' instead of an 'r' i.e. tanget instead or target – very hard to spot.

[The difference in the email address is highlighted]

Subtitle: They used the names and email addresses they'd gathered and sent personalised emails. The tone and style of the website was replicated in the email.

[Highlighted on screen – Dear Lilly, 'teamwork and innovative spirit, £250 Amazon Gift Card, Log into the following link]

Subtitle: To enter the draw, they had to log in and agree to the terms and conditions.

[Screen shows a login page which looks like the company website, but has a slightly different URL using tanget instead of target in part of the address. Video shows Lilly (an employee) logging in]

Subtitle: The sign on page is a copy of the company's page. Like the email, the URL is one letter different from the real one. When Lilly logs in the criminals will have her password.

She's instructed to download the Terms and Conditions and enable macros.

[Word document with enable macros security warning and a content protected sign]

Subtitle: Enabling macros allows the full malware to be downloaded and installed.

[Screen shows Request full malware, loading…, malware installed]

Subtitle: The criminals can now access the network and can do all sorts of damage.

[Three areas appear on screen]

Tactics Criminals Use

- target messages to individuals
- make websites and emails look authentic

Think before you click or tap

Social Media

- evaluate connection requests

- review and update personal privacy settings

Report Phishing
Make sure you know how to recognise and report phishing attempts

[music fades]