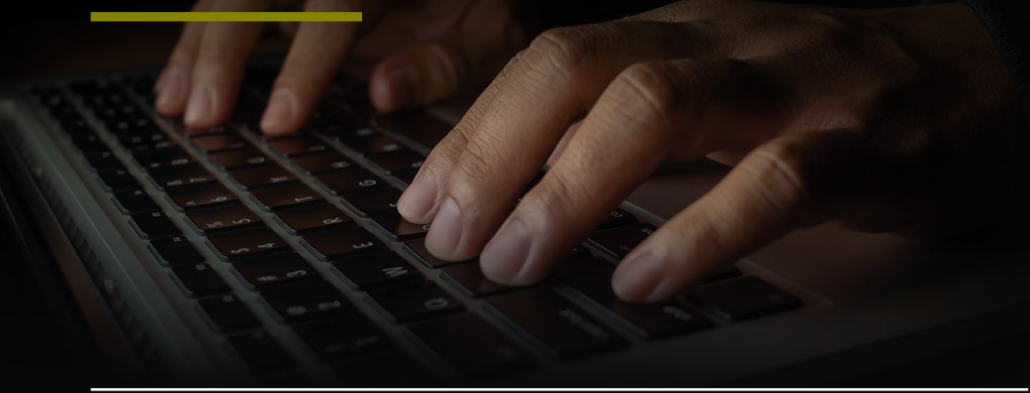


SPEARPHISHING ATTACK




Mark the hacker is able to research **email addresses and personal information** from social media groups for school parents.



A well-crafted email is sent to Simon, one of the parents in the group.

→ Spearphishing time ←



 **The email address has been 'spoofed'** to look like the address used by the school's fee payment department.



!!!
Too good to be true

The email offers a fee discount for early payment and a link is included.

Mark has created a website **that looks very similar to the school's**.



The discount was too good to ignore, **so Simon transfers the money**.

The real payment request comes from the school a week later!



 ecclesiastical
It was a lie



Simon realises that he might have been the **victim of a scam**.

Simon immediately calls his bank, but as he voluntarily sent the money **there's little they can do**.




It has all gone! 

Simon has now lost the term's fees for his children and **has to find the extra money**.



HOW TO MANAGE THE RISK

 **The email address** that appears in the 'from' field of an email **is not a guarantee** that the email came from the person or organisation it says it did... **check**.

Call any known sources by phone, to check they are bona fide, **if they are asking for money to be transferred**.

