PHISHING SCAMS: EASY TIPS TO AVOID THEM

PHISHING | \'fi-shin\ | *n.*

1. the fraudulent practice of sending emails purporting to be from reputable sources in order to induce individuals to reveal personal information or transfer sums of money

Phishing emails are built on a simple premise. Hackers access sensitive information – the kind of information that only the victims would know – and then use this to convincingly impersonate a company's CEO or other internal employee, client, customer, or supplier. These emails usually fall into two categories: those targeting data or those targeting money.

The trouble is that phishing scams can look amazingly genuine because they often incorporate real information. Although you might not be able to spot them at first, the good news is that a little extra vigilance will go a long way in preventing the hackers from getting what they want.

DATA

Whenever you receive a request to transfer sensitive data, it's a good idea to first verify the authenticity of the request by speaking to the sender face-to-face or by calling them on a phone number from a separate, trusted source.

TOP TIP

Hackers often include fraudulent phone numbers within phishing emails, which is why it's good to look up the number separately and use that instead of any provided in a text or email.

MONEY

Just like with the requests for data, if you receive an email asking you to transfer funds to a bank account where no previous transfers have been made, it's very important to first verify the authenticity of the request by speaking to the sender face-to-face or by calling them on a phone number from a separate, trusted source.

TOP TIP

Senior management should make it clear to employees that the company will never hold it against them if they do not make a transfer because they are unable to verify the authenticity of the request. This way, employees will be more likely to err on the side of caution when they receive an 'urgent' fund transfer request.