All the info below was taken from the official SumUp website [SUMUP]

Understanding phishing attacks

Phishing is an online scam technique whereby scammers impersonate legitimate organisations or people in order to access sensitive information. The following tips will help you recognise and avoid phishing scams.

Recognise phishing scams

Consider the language and tone

Scammers exploit their victim’s anxieties by claiming high stakes or an urgent need for action. If you receive an unexpected email, take a moment to consider if the information, context and language make sense.

Check the sender

Scammers may try to obscure the true source of an email. Check the email's details to ensure it came from the correct address or domain. Most companies don't use free-to-sign-up domains such as @yahoo or @gmail

All email contact from SumUp will come from an @sumup email address. Any contact claiming to be SumUp but using a different domain is a hoax.

Check the links

Phishing scams may seek to lure you into clicking a link. Once clicked, a fake website or attachment may load and attempt to steal your information. It is vital not to open unrecognised links.

If unsure of a link's validity, check it by hovering over the link until the destination URL appears in the bottom corner of your screen. Alternatively, right-click the link, select “Copy URL address” and paste it to a separate document.

Scammers constantly change their approach but there are still ways to protect yourself against phishing.

Important:

If you think your personal information may have been compromised, immediately change your passwords and report the incident