

The most common PHISHING techniques

Rapid increases in technology have been hugely beneficial to most people around the world, however this also includes criminals.

Recent research has shown that 45% of UK businesses have experienced a phishing attack in the past two years, but what are the most common forms of attack?

Most phishing attacks come via emails and will generally try to trick you into giving your information to the attacker. Take a look below at the most common forms of Phishing attack.

Invoice Scam



An email from an attacker will normally outline that you owe them money, providing you with an invoice.

You will be asked to click a link which will take you to a web page where you will be asked to enter your bank details, giving your attacker access to your account and funds.

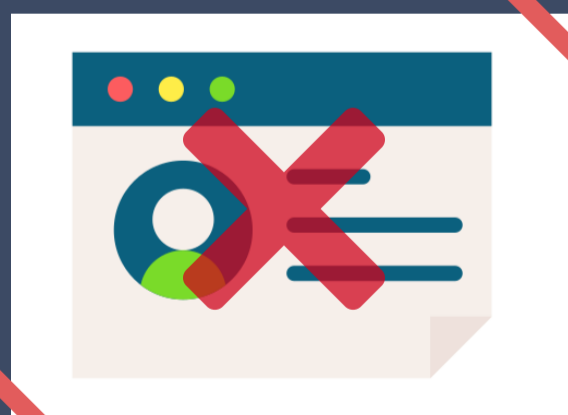
Download scam

Similar to an Invoice Scam, your attacker will send you an email with an attachment, claiming that it holds important information.

However, the attachment will be infected with a virus that will be installed onto your computer, often hijacking your computer into distributing the virus further, or gain access to your sensitive data.



Compromised account scam



An attacker will contact you via email, posing as a third party company, telling you that your account has been hacked.

You will usually be asked to follow a link to reset your details, however, this will be a false link that gives your login information to your attacker.

Payment and delivery scam

A cyber attacker will send you an email impersonating a business claiming that you need to update your details before the delivery can be made.

Of course, this is untrue, and if you follow a link and input your payment details, you will be handing money over to a cyber-criminal.

