



Latest phishing scams to look out for – April 2016

HMRC

Email posing to be HM Revenue & Customs (HMRC) claims that you are eligible to receive a tax refund. The e-mail states that in order to receive your refund you need to click a link to create a government Gateway Account. However, the email is not from HMRC and the claim that you can click a link to get a tax refund is false. This email is a phishing scam created to steal your personal information. If you are unsure about any correspondence you receive it is best to contact HMRC as they don't usually contact via e-mail.

APPLE ITUNES

Email posing to be from Apple iTunes Store says that your order has been placed and tells you that if you did not authorise the purchase, you should click a 'cancel' link. The email is not from Apple and is a phishing scam created to try and get you to share your Apple ID and other personal information.

UEFA

Email purporting to be from European football governing body UEFA claims that you have won £760,000 in the UEFA Euro 2016 online e-draw. It isn't from UEFA. The email is an advance fee scam created in order to trick you into sending money and personal information.

FACEBOOK ADS TEAM

Warning message pretending to be from the Facebook Ads Team says that your account has been found in violation of terms of service and will be closed for safety reasons. The message is not from Facebook and your account is not going to be closed. The message is designed to access your login details and personal information.

DISNEY CRUISES

'Disney Cruises' Facebook Page claims that you can win a cruise with them if you click. This is a false page designed to trick users into subscribing to highly priced SMS 'services' or calling premium rate phone numbers.

PAYPAL

Email designed to look like PayPal claims that your account has been limited because some information in the account is missing or incorrect. It is a phishing scam created to steal your login details and personal information.

If you suspect something 'phishy' about an e-mail it's best to contact the company directly if you hold an account with them, using their legitimate contact details and not those in the e-mail.