Risk Solutions

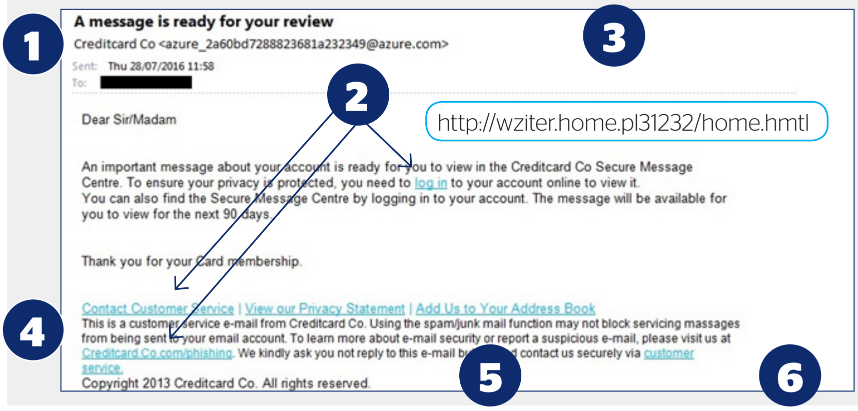
Email Fraud
How to spot a phishing scam

One out of every five UK businesses has suffered a material loss due to a cyber breach and 72% of these breaches are caused by fraudulent emails*. Putting in place procedures to protect against email fraud is essential to protect your data, finances and reputation.

Phishing risk

Hackers utilise business reliance on emails and the anonymity it provides to take advantage of busy employees, as well as play on their natural curiosity, fear or gullibility. By targeting those with access to sensitive information, hackers can breach security to view confidential information or enter a network.

The subsequent impact on a business can be significant; from theft of data or money, to the corruption of data and network failure. Business reputation can also be dented if partner and customer details are stolen, creating a knock-on effect for future prosperity.



A message is ready for your review
Creditcard Co <azure_2a60bd7288823681a232349@azure.com>
Sent: Thu 28/07/2016 11:58
To: [redacted]

Dear Sir/Madam

An important message about your account is ready for you to view in the Creditcard Co Secure Message Centre. To ensure your privacy is protected, you need to log in to your account online to view it.
You can also find the Secure Message Centre by logging in to your account. The message will be available for you to view for the next 90 days.

Thank you for your Card membership.

Contact Customer Service | View our Privacy Statement | Add Us to Your Address Book
This is a customer service e-mail from Creditcard Co. Using the spam/junk mail function may not block servicing massages from being sent to your email account. To learn more about e-mail security or report a suspicious e-mail, please visit us at Creditcard Co.com/phishing. We kindly ask you not reply to this e-mail bu[illegible]d contact us securely via customer service.
Copyright 2013 Creditcard Co. All rights reserved.

WARNING

If you receive an email or message which you suspect may be a phishing scam, do not click on any links or open any attachments until you have checked further with someone else.

Managing email fraud

It is not always easy to spot fraudulent emails, as some look very similar to the real thing. These tips will help your employees to spot the signs:

1. Predict	Are you expecting the email or contact from this organisation? Would this company know your name and normally send an email like this? Watch out for alerts claiming to be from reputable organisations (including compiled alerts and RSS feeds) with links that may contain malware.
2. Hover over the links	Get in the habit of hovering (not clicking) over all the links in the email. They should point to a recognisable domain and differ depending on the function of the link - if not, it may not be legitimate.
3. Inspect the sender's email address	To help check authenticity, always look at the email address the message was sent from. The domain should be recognisable, however it can be 'spoofed' to look authentic. Look for different connectors within the email, e.g. hyphens vs underscores; full stops vs none; and/or subtle spelling errors, such as double vs single letters. Also, watch out for unusual foreign domain extensions, such as .ru, .cn, and .ng.
4. Seek verification	If the email appears to originate from someone you know, verify the authenticity of the request in person or via telephone or email, using the contact details you have on record.
5. Heed your instincts	Most importantly – does everything feel right? Consider whether the 'pleasantries' are incongruous to the nature of the email or person it is supposed to be from.
6. Your security	• Make sure your anti-virus and software patches are always up-to-date; • Consider tighter controls over your firewall/email/web proxy filters; • Adjust your junk email settings to the highest security options.

With one in five businesses being targeted by email scams, ensuring that security procedures are in place and understood by employees must be top priority to safeguard your business assets.

* Department for Culture, Media & Sport. Cyber Security Breaches Survey 2017. April 2017

Made possible
QBE

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 QBEeurope.com
QBE European Operations is a trading name of QBE Insurance (Europe) Limited and QBE Underwriting Limited, both of which are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.