making relationships count

SOCIAL ENGINEERING, PHISHING AND CYBER FRAUD FAQ'S

In recent times, Social Engineering, Phishing and Cyber fraud/crime notifications and claims have become prevalent.

DUAL is now offering a coverage enhancement as an Optional Insuring Clause under our Cyber product offering which provides first party cover for the Insured's direct financial loss arising from:

- Social Engineering
- Phishing
- Phreaking
- Cyber Fraud

The Endorsement also provides third party cover in relation to the Insured's legal liability to third parties arising from:

- Social Engineering Fraud
- Phishing
- Cyber Fraud

What is Social Engineering?

Social Engineering is effectively the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

A common example is where a person receives a phishing email which is a clever, authentic-looking email aimed at tricking individuals into disclosing sensitive information or carrying out tasks through deceptive means. They can include malicious links, attachments or redirection to a fake website that requests information. The email looks like it has come from a legitimate sender such as your colleague, organisation, supplier or vendor.

Aren't scam emails blocked by junk mail or firewalls?

Even the most sophisticated email servers will allow some phishing emails to go through, so it's important to check every request for payment or invoice received by email thoroughly before forwarding on for, or organising, payment.

How can you tell if an email is a phishing email?

You can often spot a phishing email from the following:

- The email claims to be sent from a senior executive member of the business

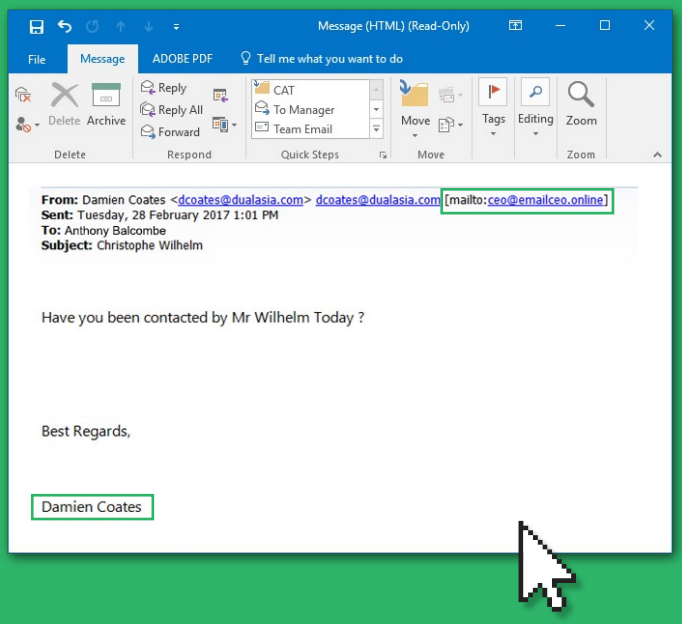
  Example: the Managing Director asking you to pay an invoice

- The content has an urgency to it, or requires urgent action from you

  Example: You must urgently pay this invoice in the next 24 hours

- The return and/ or reply email address are unknown to you, or contain spelling errors. Beware that when using a mobile phone, the return address may not fully display

  Example: email says it's from Damien Coates with return email ceo@emailceo.online



SYDNEY | MELBOURNE | PERTH | BRISBANE
Tel: 1300 769 772 www.dualaustralia.com.au

SOCIAL ENGINEERING FAQ'S

- The content urges you to get in touch with a unknown third party

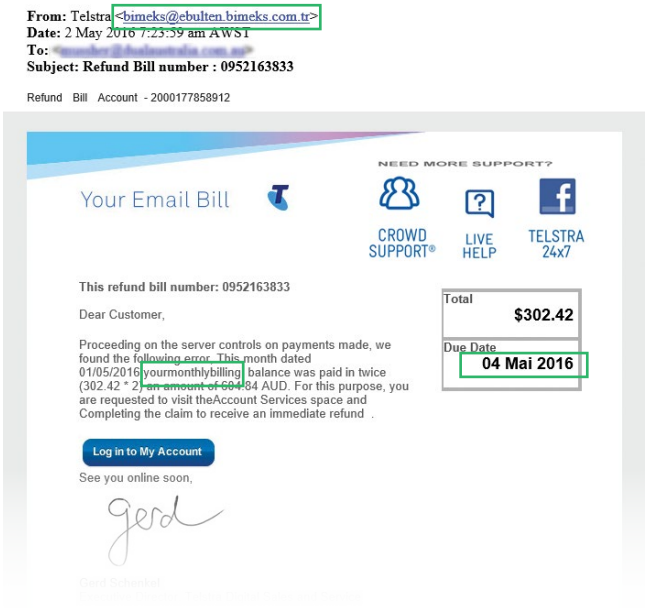
  Example: To arrange payment for a Telstra invoice contact Bimeks

- There are spelling mistakes or formatting errors in the email

  Example: Invoice Date 15th Mai 216, or pleaseclickheretopay

- The content requests sensitive information which you wouldn't normally need to provide to a supplier, or that they should already contain on file

  Example: Please provide your credit card details



From: Telstra <bimeks@ebulten.bimeks.com.tr>
Date: 2 May 2016 7:23:59 am AWST
To: [redacted]
Subject: Refund Bill number : 0952163833

Refund Bill Account - 2000177858912

Your Email Bill

NEED MORE SUPPORT?

CROWD SUPPORT® LIVE HELP TELSTRA 24x7

This refund bill number: 0952163833

Dear Customer,

Proceeding on the server controls on payments made, we found the following error. This month dated 01/05/2016 yourmonthlybilling balance was paid in twice (302.42 * 2 = an amount of 604.84 AUD. For this purpose, you are requested to visit theAccount Services space and Completing the claim to receive an immediate refund .

Total **$302.42**

Due Date **04 Mai 2016**

Log in to My Account

See you online soon,

Gerd

Gerd Schenkel

What can you do if you receive a phishing email?

1. Do not respond or click on any of the links or attachments in the email
2. Forward the email to your IT service provider to confirm
3. Delete the email
4. Block the sender and warn any other recipients

How can you prevent from falling victim to phishing emails or social engineering scams?

1. Check every invoice or email thoroughly against the tips above to ensure you are absolutely confident it is a legitimate request for payment or information before sending on, or organising payment
2. If in doubt, forward the email to your IT service provider to confirm
3. Ensure the Finance Department has the following controls in place that may prevent scam requests for payment from getting through:
   - Verify all new bank accounts by a direct call to the receiving bank to confirm it is a legitimate account, prior to being established in the accounts payable system;
   - Verify all changes to existing bank account details (including routing numbers, account numbers, telephone numbers and contact information), by placing a direct call using only the contact number previously provided by the vendor/supplier before the request was received;
   - Send all confirmations of banking changes requested by the vendor/employee/client to a person independent of the requestor of the change, with any changes being implemented only after the vendor/supplier has the opportunity to challenge them;
   - Ensure there is a review of all changes to banking records by a supervisor or next-level approver before any change to the record is processed;
   - Run exception reports, either automatic, or manually created, showing all changes to the standing data of vendors/suppliers

What is Phreaking?

Phreaking means the unauthorised and malicious use of the telephone system of the Insured which results in unauthorised charges or bandwidth costs which the Insured is legally liable to pay.

What is Cyber Fraud?

Cyber Fraud means an intentional, unauthorised and fraudulent instruction to a financial institution to debit, pay, deliver or transfer money or securities, but was in fact fraudulently transmitted by a third party without the knowledge or consent of the Insured.

What is Direct Financial Loss?

Direct Financial Loss means financial loss suffered by the Insured including:

a. Loss of the Insured's money or securities caused by Social Engineering Fraud or Cyber Fraud provided such loss is not recoverable from any financial institution or any other source;

b. The cost of reimbursing the Insured for its direct financial loss arising from Phishing or Phreaking;

c. Legal Representation Costs; and

d. Public Relations Costs arising from Phishing