CLAIMS FIRST

# EMAIL ACCOUNT BREACHES ALERT

## Experiencing a loss can be a devastating experience. However big or small, our priority is to resolve your claims as quickly as possible, but we'll also help you avoid potential losses by analysing our data and sharing our market leading insights.

Over the last few months, we have seen a dramatic increase in cyber claims notifications relating to compromises of email accounts, in which hackers have gained access to sensitive information including bank details. Some urgent actions and precautions can mitigate this threat.

Often the compromise starts with a phishing email containing a link directing the recipient to a bogus login screen. As soon as the victim enters the account details, they are captured by the hacker who then has the necessary information to log in to the victim's email account. The perpetrator is then able to send and receive emails from the victim's email address and access all of the information in the victim's email inbox.

## Recent examples

**The following recent examples of cyber claims notifications all resulted from hackers gaining access to employees' email accounts after phishing attacks:**

- A hacker used the employee's email account to send an email purportedly from the treasury team approving client's funds to be sent to bank accounts controlled by the hackers.
- A hacker set up an auto-forward function allowing a bogus email to be sent purporting to come from a senior member of their finance team in relation to a payment and requesting a client's fee-letter. This was discovered by the Insured but the hacker had access to sensitive information and the potential consequences are clearly of concern.
- An employee had been using their work email to arrange a personal financial transaction. A hacker accessed the employee's account and replaced a genuine email which contained bank account details with a new email attaching different account details, the account being one which was controlled by the hackers. The employee lost substantial personal funds as he sent his money to the hacker's bank account.

**Our claims experience suggests that most of these matters notified to us could have been avoided if two factor authentication was in place. The requirement for a secondary password would have prevented unauthorised access to the account.**

## We strongly recommend the following actions:

As a matter of priority, alert all staff about this type of hack. (The most vulnerable users are remote users who use web access to connect to their email inboxes).

Ensure staff are trained about the threat of phishing emails, with refresher courses to reinforce previous sessions followed by testing to strengthen understanding and retention. (AIG offers end-user training service, including phishing testing to CyberEdge and ProfessionalEdge policyholders).

Highlight to employees that in phishing emails, the sender's email address is not genuine and should always be checked. For example, instead of being from "joe.bloggs@aig.com", the email comes from "joe.bloggs@aig1.com". The modification to the email address may be minor but it makes all the difference.

Hovering your mouse over a link in the phishing email may display a bogus URL that the hacker wants the victim to click on.

If in doubt, always contact the email sender for verification that the email received is real. This should be done by telephone rather than email.

Two factor authentication for email accounts should be enabled (especially for Microsoft Office 365). This is not the default setting so has to be specifically changed. Two factor authentication is a two-step verification process that requires a password and a username and most importantly, a password that only the user has access to (for example a physical token which generates a code).

Priority should be given to ensuring that two factor authentication is in place for senior managers and those working in the finance team who handle financial transactions/ sensitive data.

**To register for cyber risk training visit www-105.aig.com/cyberriskconsulting**



GBL00002920 0818